Informatiebeveiliging en privacy, gemeenten Eersel, Oirschot en Reusel-De Mierden

Onderzoeksrapport

Rekenkamercommissie Kempengemeenten

7 juni 2019

Inhoudsopgave

1 Inleiding

Onder andere door de toegenomen taken in het sociaal domein beheren en verwerken gemeenten meer en meer persoonlijke en gevoelige data. Gemeenten zijn daarbij kwetsbaar gebleken, zoals onder andere blijkt uit datalekken bij gemeenten en recente onderzoeken van rekenkamer(commissie)s. Wat gebeurt er bijvoorbeeld als die informatie op straat komt te liggen? Of als de digitale dienstverlening aan burgers niet meer mogelijk is? Naast financiële, juridische en technische gevolgen kunnen deze crises het imago van de gemeente en de privacy van burgers aantasten.

Beveiliging van informatie is een must voor gemeenten, gelet op de toename van de hoeveelheid aan vertrouwelijke data in informatiesystemen. De Algemene Verordening Gegevensbescherming (AVG, ook bekend als General Data Protection Regulation, GDPR) schrijft voor dat passende maatregelen getroffen moeten worden om persoonsgegevens te beveiligen, in het belang van de burger en de gemeente zelf. De Autoriteit Persoonsgegevens registreerde in de eerste helft van 2018 8.898 datalekken, tegenover 10.009 in heel 2017. De overheid is verantwoordelijk voor 17% van de datalekken, bijna 1.500 in de eerste helft van 2018, tegenover 2.000 in 2017. De toename van het aantal geregistreerde datalekken is uiteraard te 'danken' aan de aandacht die de AVG heeft gegenereerd.

De taak van gemeenten is complex en de praktijk is nog in ontwikkeling, met name in het sociaal domein. Informatiebeveiliging wordt soms alleen als een technisch vraagstuk benaderd. De ervaring leert dat men het technisch nog zo goed voor elkaar kan hebben, wat op zich te organiseren is, de cruciale factor in beveiliging is houding en gedrag van de menselijke actor.

1.1 Leeswijzer

In hoofdstuk 3 gaan we in op de beleidsmatige context van gemeenten met betrekking tot informatiebeveiliging en privacy. Ook worden de doelstelling van het onderzoek en de onderzoeksvragen die in het onderzoek centraal staan gepresenteerd. In hoofdstuk 4 behandelen we de gehanteerde onderzoeksaanpak om de vragen te beantwoorden. Hoofdstuk 5 bevat de bevindingen, geordend aan de hand van de onderzoeksvragen. Tot slot bevat hoofdstuk 6 de conclusies en aanbevelingen.

In de bijlagen is achtereenvolgens een verklarende woordenlijst opgenomen, de bestudeerde documenten en geïnterviewde bestuurders en ambtenaren en de normen, gekoppeld aan de onderzoeksvragen.

2 Doelstelling en onderzoeksvragen

2.1 Context

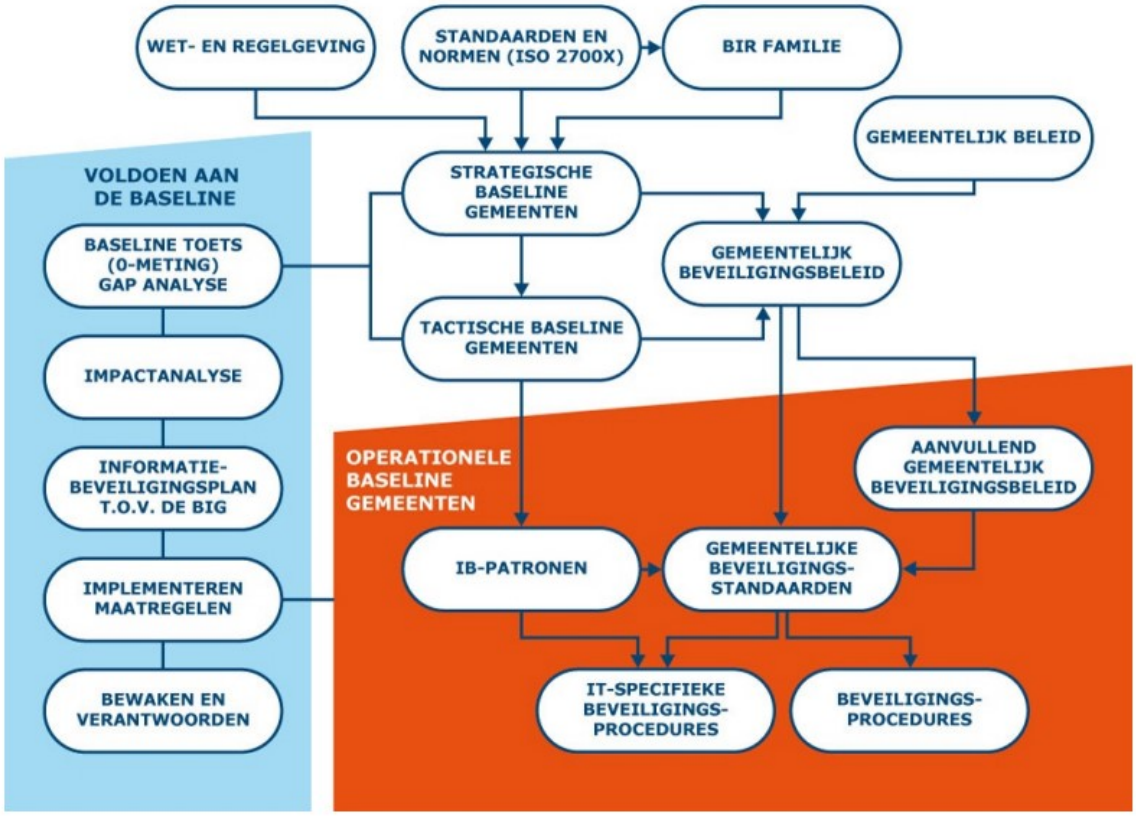
Informatiebeveiliging

Gemeenten hebben in 2013 afgesproken te voldoen aan de maatregelen uit de Baseline Informatiebeveiliging Gemeenten (BIG). Daar is geen deadline voor gesteld, verwacht wordt dat gemeenten daar naar toe werken. De BIG bestaat uit een strategische variant, met richtlijnen over de inrichting van het beleid en de verantwoordelijkheden die belegd moeten worden bij bestuur en management, ook governance genoemd. De BIG kent ook een tactische variant, met een grote hoeveelheid maatregelen die gemeenten op basis van een risicoanalyse kunnen nemen om aan het minimumniveau van de BIG te voldoen.

In de BIG is afgesproken is dat het informatiebeveiligingsbeleid twee- of driejaarlijks wordt geüpdatet, met behulp van een GAP-analyse. Dat wil zeggen een assessment in hoeverre de beveiligingssituatie van de gemeente van de gewenste situatie afwijkt. Daarnaast kan de gemeente eigen beveiligingsbeleid formuleren. Op basis daarvan wordt jaarlijks een informatiebeveiligingsplan opgesteld voor de te nemen maatregelen. Afgesproken is dat het lijnmanagement bij de analyses en de maatregelen betrokken wordt. In onderstaand schema is de huidige context van het gemeentelijk informatiebeveiligingsbeleid weergegeven.

De BIG wordt in 2020 geüpdatet met de BIO (Baseline Informatiebeveiliging Overheid). Deze is onder andere meer gericht op risicomanagement. Medio 2019 wordt op basis van de Eenduidige normatiek single information audit (ENSIA) gerapporteerd. Deze systematiek gaat de verticale verantwoording richting landelijke toezichthouders en de horizontale verantwoording richting de gemeenteraad op informatiebeveiliging en privacy vormgeven. De richtlijnen uit de BIO en de rapportagevereisten van ENSIA worden in 2020 op elkaar afgestemd.

Figuur 1. Context Baseline Informatiebeveiliging Gemeenten (BIG).



Bron: Informatiebeveiligingsdienst Gemeenten (IBD)

Context gegevensbescherming

Voor de bescherming van persoonsgegevens is op 25 mei 2016 de opvolger van de Wet Bescherming Persoonsgegevens van kracht geworden, de Algemene Verordening Gegevensbescherming (AVG). Daarmee is de privacywetgeving in de gehele EU geharmoniseerd. Overheden en bedrijven kregen tot 25 mei 2018 de tijd zich daarop voor te bereiden. Ongeveer 80-85% van de maatregelen zijn dezelfde als onder de WBP. Nieuw is onder andere dat gemeenten een functionaris gegevensbescherming (FG) als adviseur en controleur moeten aanstellen. Verder zijn gemeenten verplicht een privacyverklaring te publiceren, waarin zij in begrijpelijke taal uitleggen hoe zij omgaan met persoonsgegevens. Verder moeten zij een verwerkingsregister opstellen, waarin zij alle processen waarin persoonsgegevens worden verwerkt opnemen, en verwerkersovereenkomsten afsluiten met partijen die gegevens voor of namens de gemeente verwerken. En gemeenten moeten op bijzonder privacygevoelige processen data protection impact assessments (dpia) uitvoeren, om op voorhand de risico's te inventariseren die de verwerking van persoonsgegevens met zich mee brengt.

2.2 Centrale onderzoeksvraag

De centrale onderzoeksvraag luidt:

> *Zijn (bijzondere) persoonsgegevens en andere bijzondere gevoelige informatie in veilige handen bij de gemeenten Eersel, Oirschot en Reusel-De Mierden?*

De centrale vraag wordt beantwoord aan de hand van de onderzoeksvragen zoals opgenomen in onderstaande tabel 1.

Tabel 1. Onderzoeksvragen in het kader van onderzoek informatiebeveiliging.

A. Beleid en kaderstelling
1. Welke kaders en richtlijnen hebben raad en college met elkaar afgesproken ten aanzien van informatiebeveiliging? Hoe is de kwaliteit van deze kaders en richtlijnen?
2. Hebben de gemeenten een goed beeld van de belangrijkste risico's op het gebied van informatiebeveiliging en in het bijzonder de bescherming van (bijzondere) persoonsgegevens en andere gevoelige informatie?
B. Uitvoering
3. Hebben de gemeenten adequate maatregelen genomen om de (bijzondere) persoons-gegevens en andere gevoelige informatie die zij in beheer hebben te beschermen tegen de belangrijkste veiligheidsrisico's? Bij deze vraag worden zowel processen, organisatie, afspraken als houding & gedrag bedoeld.
4. Is het mogelijk om oneigenlijk toegang te krijgen tot (bijzondere) persoonsgegevens en andere gevoelige informatie die de gemeenten in beheer hebben? Zo ja, wat zijn de mogelijke consequenties?
C. Bestuurlijk proces
5. In welke mate is de raad in de gelegenheid zijn kaderstellende en controlerende rol waar te maken?
6. Hoe is de informatievoorziening aan de raad?

Voor de normen bij deze onderzoeksvragen verwijzen we naar bijlage 3.

3 Aanpak

De onderzoeksvragen worden beantwoord door middel van een analyse van documenten in deskresearch en interviewverslagen. De documenten bevatten beleid en rapportages van de gemeenten Eersel, Oirschot en Reusel-De Mierden en het Shared Service Centre (SSC) op informatiebeveiliging en privacy. Het SSC is onderdeel van de samenwerking die de Kempengemeenten hebben in de Gemeenschappelijke Regeling Samenwerking Kempengemeenten (GRSK). De documenten die zijn bestudeerd zijn in bijlage 2 opgenomen, evenals de functies van de in totaal 16 bestuurders en functionarissen van de gemeenten, SSC en GRSK die zijn geïnterviewd. De deskresearch vond plaats in de periode september-oktober 2018. De interviews zijn in november-december 2018 afgenomen.

Daarnaast zijn in de periode augustus-september 2018 zogenoemde penetratie- of pen-testen uitgevoerd. Deze zijn uitgevoerd door CybersecurIT BV, een bedrijf dat hierin is gespecialiseerd. Doel is om de algehele gesteldheid van de gemeenten op het gebied van digitale veiligheid te testen. De secretarissen van de gemeenten Eersel, Oirschot en Reusel-De Mierden en de manager van het SSC zijn in juni 2018 op de hoogte gesteld van het voornemen pen-testen uit te voeren. Alle vijf gemeenten die op automatisering samenwerken in Kempenverband, en het SSC, hebben een vrijwaringsverklaring getekend om de pen-testen te kunnen laten uitvoeren. Deze testen bestonden uit een technische test op (sub)domeinen en e-mailadressen van de gemeenten, inlooptesten en het versturen van phishing e-mails naar medewerkers. Daarbij is de nodige zorgvuldigheid in acht genomen om geen schade of ongewenste uitval te veroorzaken.

De rekenkamercommissie heeft het concept-rapport vastgesteld op 23 januari 2019. De feitencheck in het kader van de ambtelijke hoor & wederhoor vond plaats in januari-februari 2019. Na bijstelling naar aanleiding van de hoor & wederhoor is het definitieve rapport aangevuld met conclusies en aanbevelingen, door de rekenkamercommissie vastgesteld op 1 april 2019, voor de bestuurlijke reactie aangeboden aan de colleges.

4 Bevindingen

In dit hoofdstuk worden de bevindingen per onderzoeksvraag weergegeven.

4.1 Welke kaders en richtlijnen hebben raad en college met elkaar afgesproken ten aanzien van informatiebeveiliging? Hoe is de kwaliteit van deze kaders en richtlijnen?

In 2014 hebben de gemeenten Eersel, Oirschot en Reusel-De Mierden in Kempenverband met 2 andere gemeenten het informatiebeveiligingsbeleid vastgesteld. Dat is relatief vroeg. Gemeenten hebben in 2013 in VNG-verband afgesproken informatiebeveiliging volgens de richtlijnen van de Baseline Informatiebeveiliging Gemeenten (BIG) op te stellen. Het Shared Service Centre de Kempen (SSC), onderdeel van de Gemeenschappelijke regeling Samenwerkende Kempengemeenten (GRSK), had daarin volgens de respondenten het voortouw.

Het informatiebeveiligingsbeleid geldt de Kempengemeenten en de GRSK. Naar aanleiding van het beleid is een GAP-analyse uitgevoerd ten opzichte van de BIG-maatregelen. Op basis daarvan is begin 2015 een Informatiebeveiligingsplan opgesteld, met daarin een prioritering van de maatregelen op basis van een risicoanalyse. Daarin zijn geaccepteerde en niet-geaccepteerde risico's gedefinieerd, en maatregelen opgenomen in het informatiebeveiligingsplan.

Op onderdelen zijn sinds 2014 verbeterplannen opgesteld, zoals op de DigID-aansluitingen en SUWInet voor werk en inkomen. De informatiebeveiligingsplannen bij de gemeenten zijn na 2014 niet jaarlijks bijgesteld en het informatiebeveiligingsbeleid zou na maximaal 3 jaar bijgesteld moeten worden, zoals de BIG voorschrijft. Zeker met het oog op turbulente ontwikkelingen in de sfeer van (dreigingen op) informatiebeveiliging. Wel heeft het SSC de afgelopen jaren, naar aanleiding van audits en assessments op automatisering en applicaties verbeterplannen opgesteld en uitgevoerd. Daarnaast hebben gemeenten op onderdelen verbeterplannen opgesteld en uitgevoerd, zoals naar aanleiding van de DigID-audit over 2017.

Pas eind 2018 is in Kempenverband, met ondersteuning van SSC en BMC een nieuw informatiebeveiligingsbeleid opgesteld. Ten tijde van de interviews is dit beleid door de colleges van de drie gemeenten vastgesteld.

De kaders van de BIG zijn leidend voor de inrichting van informatiebeveiliging. 2019 is een overgangsjaar van de BIG naar de Baseline Informatiebeveiliging Overheid (BIO).[1] Bij de vaststelling van het beleid is daar voor zover dat kan rekening mee gehouden. Na de vaststelling van het beleid moet begin 2019 een GAP- en een risicoanalyse opgesteld worden, met het oog op de BIG- en BIO-maatregelen. Daaruit moet dan een jaarplan met prioritering van activiteiten op informatiebeveiliging volgen.

De Kempengemeenten werken op Informatie en automatisering samen in het SSC. 80% van de infrastructuur op ICT is dezelfde voor de deelnemende gemeenten, zoals de basisadministraties die zijn ondergebracht in het SSC. Grootste deel van het beleid is dan ook generiek. Er zijn accentverschillen op bijvoorbeeld het inregelen van de applicaties bij de

[1] De BIO is onder andere meer risicogericht en kent veel minder maatregelen dan de BIG (60% minder), maar deze zijn wel verplicht in tegenstelling tot de maatregelen uit de BIG.

individuele gemeenten. Het SSC heeft met name op de technische kant, de automatiseringskant, het initiatief in de samenwerking. Gemeenten hebben het voortouw op de i-kant en informatiebeveiliging. Het SSC ondersteunt de beleidsvorming daarop. De chief information security officer (CISO) was tot nu toe nergens ingevuld, niet bij de individuele gemeenten noch bij het SSC. De CISO wordt door de IBD van groot belang geacht voor de implementatie van de BIG. Met het nieuwe informatiebeveiligingsbeleid is besloten deze functie op gemeenteniveau in te vullen en is er niet voor gekozen deze bij het SSC of GRSK te beleggen. Hierin is een verschil te constateren met het beleid bij de Kempengemeenten op privacy en bescherming van persoonsgegevens. De voor overheden verplichte functionaris gegevensbescherming (FG) is bij het samenwerkingsverband GRSK gepositioneerd. Niet bij het SSC in de lijn, want de FG heeft een advies- en controlefunctie en rapporteert aan afdelingshoofden bedrijfsvoering, en directeur GRSK en kan gevraagd en ongevraagd secretarissen en colleges adviseren.

Op informatiebeveiliging zijn verschillende onderdelen in beleid geformuleerd, voor het merendeel opgezet en ondersteund vanuit het SSC als het om gezamenlijk beleid op automatisering gaat. Zoals wachtwoordenbeleid, patchmanagement en 'choose your own device' (CYOD) en werken op afstand. Bij de gemeenten zelf ligt de fysieke beveiliging. De open uitstraling en toegankelijkheid voor de burgers die gemeentehuizen nastreven moet in relatie staan tot beveiligingseisen. De beleidsonderdelen die daarop spelen zijn onder andere clean desk policy, toegangsbeleid van de gebouwen en sleutelbeheer. Dit zijn beleidsonderdelen die regelmatig gecheckt, geüpdatet en gehandhaafd moeten worden, hetgeen ook incidenteel gebeurt. Het wachtwoordenbeleid voor de medewerkers is aan een update toe en de fysieke toegankelijkheid is een aandachtspunt, zo bleek uit de pen-testen die zijn uitgevoerd (zie §54).

Op privacy hebben de Kempengemeenten samengewerkt om te voldoen aan de minimumeisen van de AVG per 25-5-2018, ondersteund door de GRSK. Zoals de aanwijzing van een functionaris gegevensbescherming, publicatie van een privacyverklaring over hoe de gemeente omgaat met (bijzondere) persoonsgegevens en een meldprocedure voor datalekken. Voor daarna stelde de Autoriteit Persoonsgegevens dat er een activiteitenplan moest liggen voor de overige eisen, zoals een verwerkingsregister met alle verwerkingen van persoonsgegevens door of namens de gemeente, assessments op privacyaspecten op hoog gevoelige verwerkingsprocessen enz. Er is voor de verdere implementatie van de AVG een activiteitenplan voor 2019 opgesteld, op stimuleren van bewustwording, verwerkingsregister completeren en verwerkersovereenkomsten afsluiten en privacy impact assessments (pia's, ook bekend als data protection impact assesments, dpia's) uitvoeren. De FG is hierbij als adviseur en uiteindelijk controleur betrokken.

4.2 Hebben de gemeenten een goed beeld van de belangrijkste risico’s op het gebied van informatiebeveiliging en in het bijzonder de bescherming van (bijzondere) persoonsgegevens en andere gevoelige informatie?

De laatste GAP- en risicoanalyse zijn eind 2014 uitgevoerd, daarna niet meer. Naar aanleiding van het nieuwe informatiebeveiligingsbeleid dat eind 2018 is vastgesteld, moeten deze analyses opnieuw worden uitgevoerd. Bij de GAP-analyse die begin 2019 op de rol staat wordt het lijnmanagement betrokken. Een up-to-date inzicht in de risico's zal dan moeten leiden tot een lijst met risico's die beredeneerd geaccepteerd worden en risico's die

op korte of langere termijn aangepakt dienen te worden. Op basis van die analyse kunnen geactualiseerde prioriteiten worden gesteld.

Tussen 2014 en 2018 zijn op onderdelen beleids- en verbeterplannen opgesteld. Mede naar aanleiding van de verbeterpunten die voortkwamen uit assessments en (zelf)evaluaties op beleidsonderdelen, zoals de DigID-aansluitingen. Of naar aanleiding van externe beleids-ontwikkelingen, zoals de AVG of de Eenduidige normatiek single information audit (ENSIA).

Voor de aansluiting op de Informatiebeveiligingsdienst gemeenten (IBD zijn vier stappen noodzakelijk:

1+2. aanwijzing van de algemene en vertrouwde contactpersonen (algemene contactpersonen en vertrouwede contactpersonen voor de informatiebeveiliging, respectievelijk ACIB en VCIB)
3. uploaden van de in gebruik zijnde url's en ip-adressen
4. uploaden 'foto' van de in gebruik zijnde hard- en software

De gemeenten hebben, in samenspraak met het SSC, de vier stappen gezet voor de volledige aansluiting op de IBD. Daarmee verzekeren ze zich van meldingen van de op hun situatie van toepassing zijnde beveiligingsrisico's en kwetsbaarheden en worden ze geïnformeerd op te installeren 'patches' zoals beveiligingsupdates van de software.

Het SSC laat jaarlijks een audit in het kader van een 'third party memorandum' (TPM) uitvoeren op procedures en werkwijzen en krijgt daarmee over risico's gerapporteerd. Op basis daarvan worden activiteitenplannen opgesteld. Tevens laat het SSC pen-testen uitvoeren. Het ene jaar ligt de nadruk op testen van de (technische) systemen door een externe partij. Het andere jaar ligt de nadruk op testen van de 'awareness' bij medewerkers door met behulp van social engineering door onder andere phishing mails te sturen naar de medewerkers van de gemeenten. Het SSC stelt voor de gerapporteerde kwetsbaarheden verbeterplannen op.

Verder worden de applicaties getest in het kader van de jaarlijks verplichte assessments, audits en (zelf)evaluaties, zoals de BRP, SUWInet, DigID. Deze worden intern gerapporteerd aan management en colleges en extern naar de landelijke instanties. Ook hier komen zwaktes ten opzichte van de normen naar voren die in verbeterplannen geadresseerd moeten worden. Over het algemeen worden de assessments gehaald en moet er soms marginaal een verbeteractie worden uitgevoerd. De testen worden als een opgave ervaren, daar ze tijdrovend zijn en er nog geen integraal informatiemanagementsysteem, een zogenoemd 'information security management system' (ISMS), aanwezig is om hierin te ondersteunen. Bij de meeste gemeenten is dat alleen voor burgerzaken geïnstalleerd en moet apart over de verschillende applicaties gerapporteerd worden. Er loopt een aanbestedingsprocedure voor een integraal ISMS, dat waarschijnlijk in 2019 zal worden geïnstalleerd.

Niet alleen op digitaal, maar ook op fysiek gebied moet aandacht aan beveiliging worden besteed. Daar zijn met name interne procedures voor opgesteld, zoals de clean desk policy of de beveiliging van de toegang tot de gebouwen door middel van badges/toegangspassen. De fysieke beveiliging is een aandachtspunt bij alle drie gemeenten, zo blijkt uit de pen-testen (zie §5.4).

Voor de 2^{e} helft van 2018 stonden in het kader van de implementatie van AVG-maatregelen de zogenoemde privacy impact assessments (pia's) op de rol. Hiermee worden de risico's

van de verwerking van (bijzondere) persoonsgegevens in hoog gevoelige verwerkingsprocessen in kaart gebracht. Er zijn nog geen pia's aangetroffen. Op basis van het verwerkingsregister kan geprioriteerd worden op welke processen met hoge privacy gevoeligheid assessments uitgevoerd moeten worden. De assessments zullen door de privacyofficers van de gemeenten worden uitgevoerd en door de FG vanuit de GRSK als adviseur ondersteund.

Respondenten geven aan dat de gemeenten nog niet volledig 'in control' zijn op de verwerking van persoonsgegevens. Grotendeels vanwege de onvolledigheid van het verwerkingsregister en de pia's. Dat geldt de interne en met name externe verwerkingsprocessen, die namens de gemeenten worden uitgevoerd. Met de grote marktpartijen zijn verwerkersovereenkomsten gesloten, met afspraken over de veilige verwerking van de data. Zo heeft het SSC externe gegevenskoppelingen met PINK en SIM, die zijn afgedekt in verwerkersovereenkomsten die AVG-proof zijn. Het grootste risico zit in de verwerking van bijzondere persoonsgegevens van kwetsbare groepen burgers door kleinere partijen in bijvoorbeeld de jeugdzorg. Zo wordt erkend door een aantal respondenten.

Aandacht ('awareness')

Volgens de meeste respondenten is er tegenwoordig aandacht bij college en management van de gemeenten voor informatiebeveiliging en privacy. Mede door de implementatie van de AVG in 2018 en ENSIA voor 2019. Een aantal merkt op dat dit sterker en pro-actiever mag. Vanuit de gemeenteraden worden hierover volgens de respondenten over het algemeen weinig vragen gesteld. Een aantal respondenten gaat ervan uit dat raadsleden klaarblijkelijk vinden de onderwerpen goed belegd zijn bij de colleges.

Aan bewustwording van risico's bij medewerkers wordt aandacht besteed. Informatiemanagers, privacyfunctionarissen en FG gaan bij college en afdelingsoverleggen langs met presentaties. Op algemene bijeenkomsten, zoals het maandelijkse ontmoetingscafé in Eersel of workshops in Reusel-De Mierden, worden de belangrijkste ontwikkelingen op informatiebeveiliging en privacy besproken. Aangegeven wordt dat men ook voorzichtig moet zijn met aandacht hiervoor vragen, er kan ook vermoeidheid bij de medewerkers optreden. Incidenten helpen dan weer om de aandacht scherp te krijgen, zie ook §5.4.

Bij de afdeling burgerzaken van de gemeenten was deze awareness op gegevensbescherming en informatieveiligheid al aanwezig. De medewerkers werken al langer met persoonsgegevens van burgers. Respondenten merken op dat de aandacht hiervoor bij andere afdelingen groeit. Men komt met vragen naar de privacyfunctionaris en men spreekt elkaar aan op risicovol gedrag. Geconstateerd wordt dat de medewerkers ermee bezig zijn, hoewel de meeste respondenten ervan uitgaan dat niet iedere medewerker precies weet wat een datalek is. Hier moet continu aandacht aan besteed worden, en de cultuurverandering kan en moet volgens een enkele respondent sneller. Zo zit het volgens respondenten niet in de cultuur om onbekenden, die zich op een niet voor publiek toegankelijke plek bevinden, aan te spreken of zij wel toegang mogen hebben binnen de gemeente.. Een tweetal gemeentehuizen herbergt dienstverlening voor risicogroepen, zoals het Centrum voor Jeugd en Gezin (CJG), en daar zijn medewerkers meer gewend alert te reageren.

4.3 Hebben de gemeenten adequate maatregelen genomen om de (bijzondere) persoonsgegevens en andere gevoelige informatie die zij in beheer hebben te beschermen tegen de belangrijkste veiligheidsrisico's? Bij deze vraag worden zowel processen, organisatie, afspraken als houding & gedrag bedoeld.

Beleid is in het algemeen en op onderdelen geformuleerd, zoals in de vorige paragrafen is bevonden. Zoals in §5.1 is geconstateerd wordt aandacht besteed aan de 'awareness' bij medewerkers, en zijn de gemeenten van plan daar continu aandacht aan te besteden. Om elkaar onderling te voeden en activiteiten af te stemmen hebben de privacyofficers en de FG eens per maand overleg en heeft de Beheergroep Informatieveiligheid met de functionarissen voor informatiebeveiliging van de gemeenten, binnenkort CISO's, en de coördinator van het SSC tweewekelijks in Kempenverband een overleg. Samen met de FG en coördinator van het SSC. Het bewustzijn bij medewerkers op risico's wordt daar ook geagendeerd.

Het SSC is niet in de lead in deze overleggen. Het overleg over informatiebeveiliging functioneerde al lang, maar zonder duidelijke voorzitter. Volgens een enkele respondent was dat ook de reden dat de aanpassing van het informatiebeveiligingsbeleid te lang op zich heeft laten wachten. Met de komst van de AVG en met name ENSIA op informatiebeveiliging is de urgentie gevoeld tot meer overleg en is meer structuur en doelgerichtheid in de overleggen gekomen. Momenteel functioneert het overleg onder wisselend voorzitterschap van één van de gemeenten.Vanaf begin 2018 functioneert het overleg met een vaste voorzitter.

Het SSC geeft aan dat deze vanuit de automatiseringskant een aantal initiatieven opgepakt heeft, omdat er naar eigen inschatting niet mee gewacht kon worden Zo is beveiligd e-mailverkeer opgezet, door middel van Cryptshare. Ondanks het feit dat het een (kleine) extra handeling vergt, wordt dit volgens de meeste respondenten wel gebruikt. In Eersel wordt gemeld dat, als informatie onbeveiligd binnen komt, de medewerker meteen contact opneemt met de afzender om herhaling in de toekomst te voorkomen.

Voor andere zaken is het SSC afhankelijk van de snelheid van de individuele gemeenten, en bepaalt het traagste tempo de maat. Zo wordt vanuit het SSC het beleid voor devices uitgerold, maar niet overal gelijk in de Kempengemeenten. In het algemeen is in Kempenverband afgesproken dat een meerderheid van drie gemeenten de gezamenlijke inspanningen bepaalt. Een enkele gemeente laat de eigen medewerkers (en raadsleden) hun eigen mobiele apparaat en software gebruiken, ook voor de gemeentelijke informatie. Dat brengt risico's met zich mee, als de 'devices' niet beschikken over adequate beveiliging, Het beleid gaat uit van 'range' van apparaten die door het SSC ter beschikking worden gesteld die voorzien zijn van beveiliging.

Er is nog geen integraal managementsysteem op informatiebeveiliging (ISMS) geïnstalleerd (zie §5.2) en dat vormt een risico op inefficiëntie. Bijgevolg is het ISMS ook niet gekoppeld aan de PDCA-cyclus, zodat niet gestructureerd acties toegewezen kunnen worden op de leerpunten uit de managementrapportages op informatiebeveiliging.

Uit de deskresearch en de interviews komt naar voren dat de autorisaties van medewerkers op de applicaties, en met name de mutaties daarop, een verbeterpunt vormen. Voor de medewerkers in vaste dienst verloopt het aan- en afmelden van medewerkers in overleg met P&O, dat binnen de GRSK is gepositioneerd. Een nieuw account voor applicaties aanvragen

gaat door middel van een door SSC verstrekt aanvraagformulier via de het contactpersoon SSC of MT naar het SSC. Het SSC regelt de technische autorisatie op een applicatie. De specifieke toegangsrechten van de medewerker binnen de applicatie worden door de functioneel beheerders van de gemeenten bepaald. De uitdiensttreding zou de omgekeerde weg moeten volgen, maar deze wordt volgens respondenten niet altijd conform de regels afgelegd. Bij functiewijzigingen is dat ook niet altijd het geval. Daardoor kan het voorkomen dat iemand die uit dienst is of van functie gewijzigd is, onterecht nog over zijn/haar oude autorisaties beschikt en toegang kan hebben tot informatie waartoe hij/zij niet gerechtigd is. Behalve bij burgerzaken en SUWInet, daar wordt in het assessment op de correcte procedure voor autorisaties gecheckt. Bij andere applicaties worden de autorisaties aan personen toegekend en niet functiegericht. Eens per jaar zet het SSC de autorisaties op een rij en rapporteert dat aan de gemeenten, daarmee kunnen deze gecheckt en verbeterd worden. Dat bergt het risico in zich dat autorisaties maximaal een jaar lang onterecht kunnen doorlopen. Tevens is het een risico op inefficiëntie, omdat ieder account op applicaties de gemeenten geld kost.

Externe medewerkers vormen een ander vraagstuk met betrekking tot autorisaties. De externen worden niet bij P&O aangemeld, daar deze meestal op gemeentelijke projectmiddelen worden aangesteld. Hierbij moeten de afdelingsmanagers zelf de autorisaties bij SSC aanvragen en ook weer afmelden bij vertrek. Dat gaat niet altijd goed.

De procedures met autorisaties heeft de aandacht van het management en gaat opgepakt worden, volgens respondenten. Onder andere door autorisaties op functie toe te kennen, en niet meer op personen. Zo zou in plaats van achteraf te controleren het aan de voorkant dicht geregeld gaan worden.

Functiescheiding is in kleine(re) gemeenten een lastig thema in verband met autorisaties. In een van de audits kwam dit naar voren. Wat voorkomen moet worden is dat een beheerder op applicaties gebruikersrechten heeft. Zo kan hij/zij zichzelf geen rechten toekennen om bij data te kunnen komen, om deze vervolgens in te zien of aan te passen. In kleine afdelingen is dat lastig te organiseren, wanneer er te weinig medewerkers zijn om de verschillende functierollen in te vullen. In Reusel-De Mierden wordt dat opgevangen door een extra audit door de FG en informatiemanager, een check op de logging wie al dan niet terecht toegang heeft gekregen tot gegevens en extra parafen die voor handelingen gezet moeten worden. Een andere oplossing kan zijn door een persoon meerdere functiegerichte autorisaties toe te kennen. Dan kan via de logging gecheckt worden welke functie toegang heeft gekregen tot gegevens. Dat is op dit moment niet mogelijk door de persoonsgerichte toekenning van autorisaties.

Overigens is de logging, het registreren van handelingen in een applicatie, alleen op een beperkt aantal applicaties mogelijk, zoals het Document Management Systeem (Corsa), het klantcontactsysteem en bij burgerzaken. Implementatie van logging staat op de agenda, maar heeft volgens een enkele respondent geen prioriteit. Voor de logging op het gehele systeem ontbreekt vooralsnog ook de servercapaciteit bij het SSC. Daarmee vervalt de mogelijkheid om via een check op de logging te monitoren en mogelijk te handhaven op onrechtmatige handelingen.

Op technisch gebied zijn er volgens de meeste respondenten voldoende middelen om informatiebeveiliging te organiseren, mede door de schaalvoordelen die het SSC biedt. De technische veiligheid blijkt ook grotendeels uit de pen-testen die zijn uitgevoerd door de

rekenkamercommissie (zie §5.4) Het SSC houdt in een Handboek Operations de verschillende procedures en werkwijzen, met toewijzing van verantwoordelijkheden aan SSC en gemeenten. SSC stelt jaarlijks een zogenoemd Third Party Memorandum (TPM) op, laat pen-testen uitvoeren door externe partijen en stelt op basis daarvan verbeterplannen op. De beveiliging van de infrastructuur gaat uit van een zero-trust beleid. Dat wil zeggen dat de servers gecompartimenteerd zijn, opgedeeld in stukken, waartussen firewalls verdacht dataverkeer kunnen verhinderen. De draadloze wifi-netwerken, waarop ook externen aan de slag kunnen, zijn gescheiden van het bedrijfsnetwerk. Het SSC voert uitwijktesten uit, zodat getest wordt dat de gemeentelijke dienstverlening bij een calamiteit bij een andere gemeente opgepakt kan worden. In principe kan de dienstverlening aan de balie in een halve dag elders opgepakt worden en binnen een week zijn alle processen elders operationeel. Gemeenten zelf zijn verantwoordelijk voor de backup van hun eigen systemen. Een enkele respondent geeft aan dat daarop bij de procedure nog verbeteringen aangebracht kunnen worden.

Er is bij het SSC noch bij de gemeenten een Computer Emergency Response Team (CERT) aangetroffen. Dat is een team, samengesteld uit IT-professionals aangevuld met onder andere management en communicatie, dat snel en multidisciplinair kan reageren op grote incidenten en crises. Wel is er bij het SSC een rampendraaiboek met instructies hoe te handelen bij een crisis, dat jaarlijks wordt geüpdatet en in de TPM wordt meegenomen.

Het SSC is bezig met uitrollen van nieuw wachtwoordbeleid en een 2-staps verificatie (ook bekend als 2-factor authentication, 2FA). Dat is nu al wel voor thuis- en op afstand werken (plaatsonafhankelijk werken of telewerken) geïmplementeerd, maar nog niet standaard voor de aanwezige desktops. Plaatsonafhankelijk werken kan alleen door in te loggen in een Citrix-omgeving, hiervoor moet je gemachtigd zijn door het SSC, aangevraagd door de privacy-officer of één van de afdelingshoofden.

Raadsleden hebben ook toegang tot vertrouwelijke informatie. Die krijgen ze via RaadDigitaal, of wordt ter inzage gelegd. Binnenkort gaan de raden van alle Kempengemeenten over naar iBabs. De devices (tablets e.d.) voor raadsleden worden decentraal aangeschaft en men beschikt over een eigen device. Om aan de gemeentelijke informatie te komen zijn de devices beveiligd met een 2-staps verificatie.

4.4 Is het mogelijk om oneigenlijk toegang te krijgen tot (bijzondere) persoonsgegevens en andere gevoelige informatie die de gemeenten in beheer hebben? Zo ja, wat zijn de mogelijke consequenties?

Bij de beveiliging van informatie spelen de technische organisatie van de systemen en gedragsaspecten van medewerkers de hoofdrol. Het SSC laat jaarlijks pen-testen door een extern bureau uitvoeren, het ene jaar op de technische beveiliging van de systemen, het andere jaar op awareness bij de medewerkers. Op basis daarvan worden verbeterplannen opgesteld en uitgevoerd.

De rekenkamercommissie heeft in de periode augustus-september 2018 door CybersecurIT pen-testen laten uitvoeren bij de gemeenten Eersel, Oirschot en Reusel-De Mierden. Doel is om de algehele gesteldheid van de gemeenten op het gebied van digitale veiligheid te testen, met een nadruk op de bescherming van persoonsgegevens en ongeautoriseerde toegang tot de systemen. De gemeentesecretarissen en de manager van het SSC zijn in juni 2018 daarvan op de hoogte gesteld. Alle vijf gemeenten die op automatisering samenwerken

in Kempenverband, en het SSC, hebben een vrijwaringsverklaring voor computer- en huisvredebreuk getekend om de pen-testen te kunnen laten uitvoeren.

Deze pen-testen bestonden uit:

- Technische test op de (sub)domeinen en daarbij horende e-mailadressen van de gemeenten Eersel, Oirschot en Reusel-De Mierden
- Inlooptesten op de locaties van de gemeenten Eersel, Oirschot en Reusel-De Mierden
- Versturen van een zogenoemde 'phishing e-mail' naar medewerkers van de drie gemeenten

Onderzoek is gedaan naar de mogelijkheid schade aan te richten of binnen te dringen bij het IT-netwerk en de fysieke locatie van de gemeenten. Daarbij is de nodige zorgvuldigheid in acht genomen om geen schade of ongewenste uitval te veroorzaken. Gedurende de testen kon bij ontdekking van de bezigheden van de hackers geëscaleerd worden tot de gemeentesecretaris. Deze was op de hoogte en kon dan ingrijpen. Dat is gebeurd, na afloop van de inlooptest in Reusel-de Mierden en Oirschot. Daardoor kon melding bij politie vanwege huisvredebreuk achterwege blijven.

Bevinding uit de technische test is dat de IT-infrastructuur, het geheel van hardware, software en applicaties van de gemeenten er 'stevig' bij staat en slechts in beperkte mate potentiële risico's kent. Alleen een kwaadwillende met veel inzet van tijd en middelen zou daarop een digitale inbraak kunnen bewerkstelligen. Wel zijn wachtwoorden aangetroffen van een aantal e-mailadressen in gebruik bij de gemeenten die door hacks van onder andere sociale media op straat zijn terecht gekomen. Als het wachtwoordenbeleid wordt nageleefd en deze regulier worden vernieuwd, vormt dat in de basis geen probleem. Verder is er op een systeemonderdeel verouderde software aangetroffen.

De inlooptesten op de locaties van de gemeenten bestonden uit observatie, binnendringen onder valse voorwendselen en binnendringen om technische activiteiten uit te voeren. De testen tonen aan dat het voor een buitenstaander mogelijk is om met enige moeite fysiek toegang te krijgen tot computers en werkplekken van medewerkers. Bij de ene gemeente iets makkelijker dan bij de andere, maar het lukte bij alle drie de gemeenten om onder valse voorwendselen ongeautoriseerd (vertrouwelijke) informatie te verzamelen. Bij de derde inlooptest, om technische activiteiten uit te voeren, is getracht om van buitenaf, met een laptop en antennes, een alternatief wifi-netwerk op te zetten en het interne wifi-netwerk 'af te luisteren'. Dat lukte bij twee van de drie gemeenten, namelijk Oirschot en Reusel-De Mierden. Daarmee konden accountgegevens (gebruikersnaam en gecodeerd wachtwoord) van medewerkers getraceerd worden. Gecodeerde wachtwoorden van een aantal werknemers konden achterhaald worden omdat het zwakke wachtwoorden betroffen. Daarmee konden de 'ethische hackers' zich toegang verschaffen tot informatie.

De derde test betrof het versturen van een fraudulente e-mail ('phishing mail'), met als doel vergaren van persoonsgegevens en daarmee oneigenlijke toegang verkrijgen. Bij Eersel en Oirschot kon via 'spoofing' een mail vanuit een e-mailadres van de gemeente verstuurd worden. Daarmee wint een phishing mail valselijk aan betrouwbaarheid en zijn ontvangers genegen deze te vertrouwen en mogelijk op een verdachte link te klikken. Bij de drie gemeenten is een kleine groep medewerkers aangeschreven. In Eersel en Oirschot, waar een 'gespoofde' e-mail is verstuurd, is door in totaal 3 medewerkers op de link geklikt en zijn

gebruikernamen en wachtwoorden bemachtigd. In Reusel-de Mierden is geen van de medewerkers ingegaan op de phishing-mail.

Meteen na de inlooptesten zijn medewerkers van Eersel alsnog alert geworden en hebben zij het incident gemeld. Daarop is actie ondernomen, waaronder het eerder vermelde contact met de rekenkamercommissie. De FG is geraadpleegd en adviseerde de indringer als een mogelijk datalek te melden bij de AP, en ervan te leren. Een enkele medewerker die op de phishing e-mail is ingegaan heeft het incident achteraf gemeld bij het SSC. Daarop zijn de wachtwoorden gewijzigd. De gemeentesecretarissen zijn door de rekenkamercommissie direct na de pen-testen op de hoogte gesteld van de risico's op informatiebeveiliging waar meteen actie op ondernomen moest en kon worden. Op basis van een volledig technisch rapport van de pen-testen heeft de rekenkamercommissie een gesprek gehad met de verantwoordelijken bij de gemeenten en SSC. Met de technische rapporten kunnen zij verder actie ondernemen om procedures aan te scherpen en de veiligheid van de digitale infrastructuur te verbeteren.

Gebouwbeveiliging is daarbij een punt van aandacht, dat ook al hiervoor is benoemd. Na de inlooptest hebben de gemeenten de procedures gecheckt, de toegangen gecontroleerd op verbeterpunten. Ook hebben alle drie de gemeenten het incident met de indringer gebruikt om informatiebeveiliging opnieuw onder de aandacht van medewerkers te brengen. Respondenten geven aan dat daardoor de awareness verder is verhoogd.

4.5 In welke mate is de raad in de gelegenheid zijn kaderstellende en controlerende rol waar te maken?

De raden zijn in principe in staat om de kaderstellende en controlerende rol op informatiebeveiliging en privacy waar te maken, conform de geldende regelgeving. Tot nu toe wordt informatiebeveiliging vooral opgevat als een onderwerp onder bedrijfsvoering, iets waar met name de colleges en ambtenaren intern mee aan de slag moeten. De raden kennen in het kader van de bedrijfsvoering op informatiebeveiliging en privacy, budgetten toe. Bij uitbreiding van taken, zoals de implementatie van de AVG, wordt de raad gevraagd om akkoord te geven op de uitbreiding van onder andere de formatie binnen de eigen gemeente of voor het SSC.

Door de respondenten wordt ervaren dat informatiebeveiliging politiek geen 'hot issue' is. Vanuit de raden komen weinig vragen, op een enkele keer na als er zich elders een incident hierop heeft voorgedaan dat de pers heeft gehaald. Een tijd geleden heeft een raadslid uit één van de Kempengemeenten die niet in dit rekenkameronderzoek is betrokken, een geslaagde poging gedaan om het onderwerp via een hack op de agenda te zetten,. Recent is in één van de raden gevraagd of de gemeente klaar was voor de AVG. Verder blijft het volgens de respondenten relatief stil. Over het algemeen interpreteren zij de afwezigheid van vragen, ad hoc of naar aanleiding van aangereikte (jaar)verslagen, als een teken van vertrouwen in de uitvoering door college en management op deze terreinen.

Dat kan natuurlijk te maken hebben met wijze waarop de raad geïnformeerd wordt over onderwerpen als informatiebeveiliging en privacy. In principe voldoen de colleges aan de rapportageplicht zoals afgesproken in de BIG (zie volgende §5.6). Wat zoveel betekent dat de raad summier op informatiebeveiliging wordt geïnformeerd. De mate waarin de raad zijn kaderstellende en controlerende rol kan waarmaken kan het best beantwoord worden in de context van de volgende onderzoeksvraag.

4.6 Hoe is de informatievoorziening aan de raad?

De colleges voldoen met betrekking tot de informatievoorziening aan de vereisten uit de BIG, namelijk eens per jaar in de P&C-cyclus de raad informeren over informatiebeveiliging in het kader van de rapportage over de bedrijfsvoering. In de jaarverslagen van de gemeenten wordt summier aandacht besteed aan informatiebeveiliging, en dan met name op procesindicatoren. Het SSC rapporteert in de jaarverslagen al iets dieper over informatiebeveiliging. Bij grote incidenten, die zich nog weinig hebben voorgedaan, worden de raden geïnformeerd. Een informatieavond "Wat willen jullie weten?" over informatiebeveiliging en privacy, voor de gemeenteraad van Reusel-De Mierden heeft volgens een aantal geïnterviewden weinig respons en aandacht opgeleverd.

De BIG-richtlijnen zijn in VNG-verband afgesproken, ook de beperkte richtlijn over rapportage aan de raad. We zien evenwel bij de VNG de mening beginnen post te vatten dat de raad meer meegenomen moet worden op onderwerpen als informatiebeveiliging en privacy. Met de VNG constateert de rekenkamercommissie dat deze onderwerpen kritieke succesfactoren in de dienstverlening van gemeenten zijn, en dat gemeenten hierop grote bestuurlijke, financiële en maatschappelijke risico's lopen. En daarmee de aandacht van de gemeenteraden verdienen. Mede daarom wordt ENSIA geïmplementeerd, om de verticale verantwoording richting landelijke toezichthouders en de horizontale verantwoording richting gemeenteraad vorm te geven. De gemeenten zijn druk bezig ENSIA verder te implementeren. De gemeenten zijn niet door de eerste audit op ENSIA gekomen en daarover is aan de raden gerapporteerd. Daarover is in de raden geen vraag gesteld en respondenten geven aan een actievere opstelling van de raden te missen.

Figuur 2. ENSIA-model, oplevering 2019.

HORIZONTAAL		VERTICAAL		OPLEVERING
RAPPORTAGE	ONDERWERPEN	Stelsel	Vorm	Voor datum
	Beleid, doelstellingen & ambities	SUWI	Collegeverklaring + assurancerapport	1-5 ENSIA
	Samenvatting beeld & resultaten 2018	DigiD	Collegeverklaring + assurancerapport	1-5 ENSIA
	Belangrijkste beheersmaatregelen	BAG	Vaststelling rapportage + agendering	1-5 ENSIA
	Meerjarenperspectief	BGT	Vaststelling rapportage + agendering	1-5 ENSIA
		BRO	Vaststelling rapportage + agendering	1-5 ENSIA
		BRP/PUN	Ondertekening uittreksel door college	14-2 RvIG & AP
JAARVERSLAG GEMEENTE				15 -7 BZK

Naar aanleiding van de niet behaalde eerste audit op ENSIA zijn verbeterplannen opgesteld en is de tweede audit wel gehaald. De bijna 80 vragen in ENSIA worden in Kempenverband ingevuld, behalve waar het lokale zaken betreft. Die vullen de gemeenten zelf in. Gemeenten zijn zelf verantwoordelijk voor de ENSIA-rapportage aan de raden. Over de invulling van de horizontale rapportage aan de raad, wat vormvrij is, is nog niet nagedacht.

5 Conclusies en aanbevelingen

5.1 Conclusies

De Kempengemeenten Eersel, Oirschot en Reusel-De Mierden, ondersteund door het SSC waarin zij o.a. op ICT samenwerken, hebben informatiebeveiligingsbeleid vastgesteld op basis van de Baseline Informatiebeveiliging Gemeenten (BIG). De gemeenten waren er relatief vroeg bij met de vaststelling van het beleid in 2014. Daarna lijkt een tijd de urgentie te ontbreken bij de gemeenten om beleid en plannen periodiek conform de BIG te vernieuwen. Daardoor lijkt een gestructureerde aanpak op informatiebeveiliging een afwezig te zijn geweest. Gemeenten hebben, naar aanleiding van audits en assessments, op onderdelen verbeter- en actieplannen opgesteld. Het SSC laat uitwijktesten en pen-testen uitvoeren en stelt op basis van die resultaten verbeteracties op. Op onderdelen vinden verbeteracties plaats, maar een integrale aanpak ontbreekt.

Eind 2018 is nieuw informatiebeveiligingsbeleid geformuleerd, mede doordat de introductie van de AVG en ENSIA het op de agenda hebben gezet. Het nieuwe beleid is op basis van de BIG geschoeid, met een vooruitkijkende blik naar de Baseline Informatiebeveiliging Overheid (BIO) die vanaf 2020 gaat gelden. Begin 2019 moet het beleid handen en voeten krijgen met een jaarplan met activiteiten, op basis van een GAP- en risicoanalyse. Daarmee krijgen de gemeenten de risico's op informatiebeveiliging en gegevensbescherming in beeld en kunnen zij de activiteiten prioriteren.

De gemeenten voldoen aan de wettelijke vereisten op de periodieke assessments en (zelf)evaluaties op de applicaties die bij de gemeenten draaien. Hooguit moeten marginale verbeteracties ondernomen worden om alsnog te voldoen aan de gestelde eisen.

Gemeenten voldeden op 25 mei 2018 aan de minimumeisen van de AVG. Daarna moest en moet nog het nodige uitgevoerd worden om volledig aan de AVG te gaan voldoen, zoals afronding van de verwerkingsregisters, bepalen waarop privacy impact assessment (pia's) uitgevoerd moeten worden en waar nodig AVG-proof-verwerkersovereenkomsten sluiten. Gemeenten zijn daarmee druk aan de slag en zij stellen daar een activiteitenplan voor op.

Het SSC biedt op ICT schaalvoordelen, qua infrastructuur en gespecialiseerde kennis. Uit de pen-testen die het SSC zelf uitvoert en die door de rekenkamercommissie zijn uitgevoerd, blijkt dat de technische infrastructuur er 'stevig' bij staat. 80% van de infrastructuur op ICT is hetzelfde voor de vijf gemeenten. Op veel onderdelen wordt gebruik gemaakt van de aanwezige kennis, zoals met het invullen van vragen in het kader van ENSIA. Opvallend is dat de CISO-functie ontbrak bij de gemeenten en SSC/GRSK. Met het nieuwe beleid is besloten de CISO-functie op gemeenteniveau in te vullen. De FG, met een vergelijkbare controlerende en adviserende rol als de CISO, is wel bij de GRSK gepositioneerd. De IBD heeft in het dreigingsbeeld op informatiebeveiliging voor 2019 gemeenten geadviseerd de CISO-functie fors te versterken. Menskracht en kennis op deze cruciale functie gaan verdeeld worden over verschillende gemeenten. Dat levert voordelen met betrekking tot lokale kennis, maar kan ook kwetsbaar zijn.

Het SSC mist op een aantal onderdelen van het informatie(beveiligings)beleid doorzettings- en slagkracht. Er is een aantal schijven waarover de besluitvorming loopt, waardoor de gemeenten risico lopen op ineffectiviteit en inefficiëntie. Dat wordt gevoeld door de uitvoerders op de werkvloer, die roeien moeten met de aangereikte riemen. Zo kan met een

strikter gezamenlijk beleid op bijvoorbeeld 'choose your own device (CYOD) efficiënter en effectiever gehandeld worden. Op andere terreinen wordt wel het nodige gerealiseerd door het SSC in samenspraak met de gemeenten, of gaat alsnog binnenkort gerealiseerd worden, zoals een ISMS dat met de PDCA-cyclus is gekoppeld.

Uit de bevindingen blijkt dat er een risico bestaat op inefficiëntie en onrechtmatigheid door een beperkte logging (registratie van activiteiten op data) en de wijze waarop autorisaties van medewerkers en externen zijn ingeregeld. Het risico bestaat dat accounts na een functiewisseling of uitdiensttreding nog geruime tijd doorlopen. Ook op fysieke beveiliging is een risico te constateren, namelijk dat toegangsbadges nog in handen kunnen zijn van mensen die niet meer in dienst zijn van de gemeente. Gemeenten geven aan hiervan op de hoogte te zijn en van zins te zijn daar verbeteracties op uit te voeren, onder andere door autorisaties aan functies toe te kennen in plaats van personen.

De rekenkamercommissie constateert dat er geen Computer Emergency Response Team (CERT) aanwezig is bij de gemeenten of SSC. Dat is een multidisciplinair samengesteld team dat bij grote incidenten en crises kan optreden. Er is wel een jaarlijks geüpdatet draaiboek voor acties als zich calamiteiten voordoen. Het gemis van een multidisciplinair CERT kan een risico op ineffectiviteit betekenen bij een crisissituatie.

Gemeenten ondernemen de nodige activiteiten om het bewustzijn van de risico's op informatiebeveiliging en privacy te verhogen. Uit de pen-testen die de rekenkamercommissie heeft laten uitvoeren blijkt dat er op de awareness bij medewerkers nog winst te behalen valt. Het lijkt erop dat de 'awareness' toeneemt, maar het vergt een constante inspanning medewerkers alert te houden. Zeker daar de bedreigingen turbulent wijzigen en toenemen. De inlooptesten laten zien dat de gebouwbeveiliging en de wijze waarop medewerkers toegang verlenen verbetering behoeven. Dat zou met nieuwe testen bij de gemeenten periodiek getest en onder de aandacht gebracht kunnen worden. Uit de pen-testen volgde in ieder geval dat het wachtwoordenbeleid geüpdatet moet worden. De secretarissen zijn daarvan in een vroeg stadium van dit onderzoek op de hoogte gebracht.

Gemeenteraden stellen zich nog niet heel actief op informatiebeveiliging en privacy op, terwijl het kritische succesfactoren zijn in de dienstverlening en zich in het aandachtsveld van de raad zouden moeten bevinden. De raad beschikt zelf ook over vertrouwelijke informatie en over 'devices' waarop vertrouwelijke informatie van de gemeenten aanwezig kan zijn. Overigens zijn deze met een 2-factor verificatie redelijk goed beveiligd. Een handleiding of gedragscode over hoe om te gaan met vertrouwelijke informatie of informatiebeveiliging in het algemeen voor raadsleden is niet aangetroffen.

De raad voert slechts marginaal zijn kaderstellende en controlerende rol uit en lijkt daar ook niet toe te worden uitgenodigd of gefaciliteerd. Informatiebeveiliging is geen politiek 'hot issue', niet 'sexy' en wordt door menigeen als taai ervaren. Met de AVG is de aandacht voor gegevensbescherming en informatiebeveiliging toegenomen. Het is de uitdaging aan college, raad en ambtenaren om het bestuurlijke gesprek over deze onderwerpen op een goede en toegankelijke wijze te voeren. ENSIA biedt daarvoor een gelegenheid bij uitstek. Naast een verplicht deel met collegeverklaring en assurancerapport op de applicaties, met name voor de verticale verantwoording, is er een vormvrij deel voor de horizontale verantwoording richting raad.

5.2 Suggesties en aanbevelingen

De rekenkamercommissie doet naar aanleiding van bovenstaande conclusies de volgende aansporingen en aanbevelingen. De gemeenten zijn bezig met nieuw beleid en daar passen suggesties om met een aantal activiteiten en aanpakken door te gaan beter bij dan aanbevelingen. De aanbevelingen aan colleges en raden hebben op basis van de bevindingen en conclusies een urgenter karakter.

De rekenkamercommissie doet de gemeenten de suggestie om verder te gaan

- met het actualiseren van beleid op informatiebeveiliging, risicoanalyses uit te voeren en operationele handvatten op informatiebeveiliging en gegevensbescherming op te stellen
- met de uitbreiding van een automatische logging voor monitorings- en handhavingsdoeleinden
- met uitvoering van periodieke pen-testen op de technische aspecten en de gedragsaspecten van informatiebeveiliging
- met inzetten op cultuur dat medewerkers elkaar aanspreken op gedrag
- met het implementeren van het toekennen van autorisaties op functie
- met de implementatie van de maatregelen in het kader van de AVG, de BIG en vanaf 2019 de BIO

De rekenkamercommissie beveelt de colleges aan

- Een Informatiemanagementsysteem (ISMS) te implementeren op informatie-beveiliging en gegevensbescherming en deze te koppelen aan PDCA-cyclus
- De fysieke toegang van de gebouwen te checken op risico's en indien nodig maatregelen daarop te nemen
- Technische maatregelen door SSC te laten nemen zo dat 'spoofing' (e-mails versturen vanaf een vervalst e-mail adres) wordt voorkomen
- In samenspraak met het SSC het wachtwoordenbeleid aan te scherpen
- Naast pen-testen op technisch en awareness vlak periodiek inlooptesten bij de gemeenten te laten uitvoeren
- Het beleid op het verlenen en intrekken van autorisaties te herijken met een regelmatiger check op autorisaties bij functiewisseling en vertrek van (externe) medewerkers
- De CISO-functie ten behoeve van alle Kempengemeenten te positioneren bij GRSK
- Een Computer Emergency Response Team (CERT) op te zetten

De rekenkamercommissie beveelt de raden aan

- Kaders te stellen op het gebied van informatiebeveiliging en gegevensbescherming en zich actief te laten informeren over de voortgang van maatregelen hierop
- Verzoek het college een gedragscode voor de raad op te stellen hoe om te gaan met informatie op gegevensdragers en 'devices' (apparaten zoals tablets en smartphones)
- Met de colleges in gesprek te gaan om het vormvrije deel van ENSIA vorm te geven
- De colleges te verzoeken de voortgang op de aansporingen en op de aanbevelingen bij de eerstvolgende rapportage in het kader van ENSIA, medio 2019, aan de raad te rapporteren.

6 Bestuurlijke reacties

gemeente Eersel
Kempisch wonen in een wereldregio

Aan de Rekenkamercommissie
Kempengemeenten
T.a.v. mevrouw M. Boer
p/a Postbus 12
5520 AA EERSEL

Uw brief van
Uw kenmerk

Telefoonnummer 0497-531300
Bijlage(n)

Eersel, d.d. 13 mei 2019
Ons kenmerk 19.07061

Onderwerp Bestuurlijke reactie onderzoeksrapport 'Informatiebeveiliging en privacy'

Geachte mevrouw Boer,

Op 8 april jl. hebben wij via de mail het onderzoeksrapport 'Informatiebeveiliging en privacy, gemeenten Eersel, Oirschot en Reusel-de Mierden' (hierna te noemen het 'rapport') van u ontvangen met het verzoek om hier voor 20 mei 2019 een bestuurlijke reactie op te geven.

In onze vergadering van 7 mei jl. hebben wij de inhoud van het rapport besproken en onderstaande bestuurlijke reactie geformuleerd:

Algemeen:
Op de eerste plaats willen wij uw initiatief om onderzoek te doen naar informatiebeveiliging en privacy positief benadrukken. Wij onderschrijven uw mening dat informatiebeveiliging en privacy belangrijke thema's zijn voor de gemeente. Een onderzoek naar de stand van zaken betreffende de bestaande kaders en richtlijnen, naast genomen BIG-conforme maatregelen biedt handvatten om de bestaande invulling te evalueren en door te ontwikkelen.

Opmerkingen over het rapport:
Het rapport is zeer algemeen van aard, daar de bevindingen in het rapport zowel van toepassing zijn op de gemeente Eersel als de gemeente Oirschot en de gemeente Reusel-de Mierden. Informatiebeveiliging is in grote mate een organisatorische aangelegenheid, waardoor verschillen in de manier waarop de informatiebeveiliging geregeld is, onvermijdelijk zijn. De algemene beschrijving maakt het moeilijk te duiden welke constateringen op de gemeente Eersel betrekking hebben. Gerichte verbeteracties op basis van benoemde actiepunten zijn daarom moeilijk over te nemen.

Aanbevelingen
De suggestie om verder te gaan met reeds opgepakte activiteiten in navolging van het nieuwe beleid nemen wij aan ter kennisname met de intentie om beschreven activiteiten actief voort te zetten.
Een aantal van de door u genoemde aanbevelingen is zinvol en zal door ons worden overgenomen. Bij enkele aanbevelingen plaatsen wij een aanvullende opmerking, daar wij de aanbeveling niet of niet in volledigheid overnemen:

Een aantal van de door u benoemde maatregelen worden bij de gemeente Eersel reeds opgepakt, zoals het uitvoeren van checks op toegekende autorisaties bij zowel interne als externe medewerkers. Uw aanbeveling om dit te doen nemen wij daarom mee als aandachtspunt om hier een extra controle op te laten plaatsvinden.

Ook de aanbeveling om een CERT (Computer Emergency Response Team) op te zetten nemen wij ter kennisgeving over. Een CERT team bestaat reeds, als onderdeel van het gemeentelijke rampen- en calamiteitenbeleid.

De rol van CISO is in de organisatie technisch al ingevuld, waarbij tevens aandacht is geweest voor het beleggen van taken volgens het vier ogen principe. Het kwetsbaarheidsrisico wordt daarmee verkleind. Uw aanbeveling om de CISO officieel te benoemen, gezien het belang van een duidelijk aanspreekpunt voor informatiebeveiliging zowel binnen als buiten de organisatie, hebben wij overgenomen. Wij zijn echter van mening dat de CISO niet gepositioneerd dient te worden binnen de GRSK maar binnen de gemeente zelf. Als functionaris belast met het waarborgen van de informatiebeveiliging van de organisatie, waarbij niet alleen het coördineren van de werkzaamheden betreffende het informatiebeveiligingsbeleid en daaruit vloeiende maatregelen van belang is, maar des te meer het stimuleren van het beveiligingsbewustzijn en het adviseren over goede informatiebeveiliging in de organisatie, is toegankelijkheid van de CISO van groot belang. Positionering van de CISO binnen de gemeentelijke organisatie zorgt daarnaast niet alleen voor betere toegankelijkheid, maar bevordert ook de signaalfunctie van de CISO en de daaruit voortvloeiende advies- of zelfs escalatierol bij beveiligingsincidenten. De CISO is daarom intern benoemd.

Het overnemen van de aanbeveling om de gemeenteraad over de bevindingen en verbeterpunten uit dit rapport te informeren in de eerstvolgende ENSIA rapportage is niet mogelijk. Het verantwoordingstraject eindigt op 30 april. De ENSIA rapportage is daarom reeds aan de gemeenteraad verstrekt. De bevindingen uit dit rapport en gemaakte voortgang betreffende de verbeterpunten zullen daarom apart aan de raad worden verstrekt.

Wij hopen u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,

burgemeester en wethouders van Eersel

de heer ing. H.M.L. Offermans
Secretaris

de heer J.A.M. Vos
Waarnemend burgemeester

19.U001769

Gemeente Oirschot

Postbus 11
5688 ZG Oirschot

Bezoekadres
Deken Frankenstraat 5
5688 AK Oirschot

T (0499) 58 33 33
E info@oirschot.nl
I www.oirschot.nl

facebook.com/oirschot
twitter@gem_oirschot
Whatsapp 06 - 23 20 98 13

IBAN nr. NL90BNGH0285076108
BTW-nr. NL0011.22.224.B03
KvK nr. 17285344

Rekenkamercommissie Kempengemeenten
Postbus 12
5520 AA Eersel

Ons kenmerk	: HCLA01 / 19.U001769
Uw kenmerk/brief	:
Bijlagen	:
Onderwerp	: Bestuurlijke reactie Onderzoeksrapport Informatiebeveiliging en privacy
Contactpersoon	: Hans Claassen
Datum	: 4 juni 2019

Geachte heer Groen,

Op 8 april 2019 ontvingen wij het Onderzoeksrapport Informatiebeveiliging en privacy gemeenten Eersel, Oirschot en Reusel-de Mierden. U verzocht ons om een bestuurlijke reactie voorafgaand aan definitieve verzending van het rapport. Deze reactie treft u onderstaand aan.

Met belangstelling hebben wij kennis genomen van het onderzoeksrapport. Informatiebeveiliging krijgt in toenemende mate landelijke belangstelling. Niet in het laatst omdat in toenemende mate vertrouwelijke persoonsgegevens op straat komen te liggen terwijl dit niet de bedoeling is. U heeft in uw rapport dan ook de vraag beantwoord: Zijn (bijzondere) persoonsgegevens en andere bijzondere gevoelige informatie in veilige handen bij de gemeenten Eersel, Oirschot en Reusel-de Mierden?

De conclusies in uw rapport onderschrijven wij:

- De gemeenten hebben een actueel informatiebeveiligingsbeleid dat op basis van een risico-analyse in 2019 wordt vertaal in een informatiebeveiligingsplan met activiteiten op risicovolle onderwerpen.
- Gemeenten voldoen aan de minimale vereisten van de Algemene Verordening Gegevensbescherming
- Het SSC biedt op ICT schaalvoordelen, qua infrastructuur en gespecialiseerde kennis. Zij mist slagkracht om onderdelen van het beveiligingsbeleid door te zetten met name als gevolg van de procedures bij de besluitvorming.

- Risico's bestaan op inefficiency en onrechtmatigheden door beperkte logging van activiteiten en het beheer van autorisaties en accountants van medewerkers en externen.
- Het ontbreekt aan een Computer Emergency Respons Team om in crisissituaties snel te kunnen handelen.
- Gemeente ondernemen activiteiten om het bewustzijn van risico's op informatiebeveiliging en privacy te verhogen maar dat mag nog meer zijn.
- De gemeeenteraden stellen nog niet heel actief op informatiebeveiliging en privacy op maar worden daartoe ook niet toe uitgenodigd of gefaciliteerd.

Onderstaand de suggesties en aanbevelingen met daarbij onze reactie van hoe wij met de suggesties en aanbevelingen omgaan:

Algemeen:

Verder gaan met:

1. Actualiseren van het informatiebeveiligingsbeleid en op basis van risico-analyses operationaliseren van dit beleid. **Reactie:** bij de CISO bekend en een informatiebeveiligingsplan komt in het derde kwartaal gereed.
2. Uitbreiding van logging faciliteiten: **Reactie**: via de informatiebeheer beleggen bij het SSC, inclusief de monitoring.
3. Uitvoering van pentesten op de technische aspecten en de gedragsaspecten van informatiebeveiliging: **Reactie**: Dit onderwerp moet onderdeel worden van de normen die leiden tot een Third Party mededeling van het SSC aan de gemeenten rondom de beveiliging van de automatiseringsomgeving.
4. Inzetten op cultuur dat medewerkers elkaar aanspreken op gedrag. **Reactie**: is een onderwerp van de bijeenkomst met de medewerkers op 22 juni in het kader van informatiebeveiliging en privacy.
5. Het implementeren van het toekennen van autorisatie op functies. **Reactie**: monitoren dat een onderdeel is van het informatiebeveiligingsplan van het SSC voor wat betreft het gemeentebrede deel.
6. Implementatie van de maatregelen in het kader van de AVG. **Reactie**: onderdeel hiervan is de bijeenkomst met de medewerkers op 22 juni.

Aanbeveling voor de colleges:

1. Implementatie van een nformatiemanagementsysteem op informatiebeveiliging en gegevensbescherming en deze koppelen aan de PDCA-cyclus. **Reactie:** informatiebeveiliging is een specifiek onderwerp in de paragraaf bedrijfsvoering van de begroting, bestuursrapportages en jaarrekening en daarmee onderdeel van de PDCA-

cyclus. Wij zorgen voor een meer prominente aandacht ook om de raad in de gelegenheid te stellen haar kaderstellende en controlerende rol in te vullen.

2. Checken van de risico's bij de fysieke toegang tot het gebouw en treffen van maatregelen. **Reactie**: is een onderwerp van het op te stellen informatiebeveiligingsplan (derde kwartaal 2019).
3. Technische maatregelen laten nemen door het SSC om het versturen van emails van een vervalst email-adres te voorkomen. **Reactie**: monitoren dat een onderdeel is van het informatiebeveiligingsplan van het SSC voor wat betreft het gemeentebrede deel.
4. In samenspraak met het SSC het wachtwoordbeleid aanscherpen: **Reactie**: monitoren dat een onderdeel is van het informatiebeveiligingsplan van het SSC voor wat betreft het gemeentebrede deel.
5. Naast pen-testen op technisch en awareness vlak periodiek inlooptesten bij de gemeenten laten uitvoeren. **Reactie:** monitoren dat een onderdeel is van het informatiebeveiligingsplan van het SSC voor wat betreft het gemeentebrede deel.
6. Het beleid op het verlenen en intrekken van autorisatie te herijken met een regelmatiger check op autorisatie bij functiewisseling en vertrek van (externe) medewerkers. **Reactie:** monitoren dat een onderdeel is van het informatiebeveiligingsplan van het SSC voor wat betreft het gemeentebrede deel.
7. De CISO-functie ten behoeve van alle Kempengemeente te positioneren bij de GRSK. **Reactie**: wij willen hiervoor wel het gesprek aangaan maar willen de aandacht voor informatiebeveiliging en privacy gewaarborgd zien voor Oirschot, mede omdat ook geconstateerd is dat de awareness op dit onderwerp verbeterd kan worden.
8. Een Computer Emergency Response Team op te zetten. **Reactie:** dit vinden wij belangrijk en moet een onderdeel zijn van het informatiebeveiligingsplan van het SSC voor wat betreft het gemeentebrede deel.

<u>Aanbeveling voor de raad</u>:

1. Kaders te stellen op het gebied van informatiebeveiliging en gegevensbescherming en zich actief te laten informeren over de voortgang van maatregelen hierop. **Reactie**: Rekening houdend met de komst van het In Control Statement met ingang van 2021 zullen wij in de paragraaf Bedrijfsvoering van de begroting het informatiebeveiligingsbeleid vertalen in kaders voor die de raad. Kaders die wij als college uitwerken in activiteiten waarmee het college aangeeft op het gebied van informatiebeveiliging en privacy in control te zijn.
2. Een gedragscode voor de raad op te stellen hoe om te gaan met informatie op gegevensdragers en devices (zoals tablets en smartphones). **Reactie**: wordt op dit moment al opgepakt in het kader van het project mobiele telefonie. Dit zou dan verbreed moeten worden naar een code voor de raad. Wij vinden dat ook dit onderwerp behoort tot het informatiebeveiligingsplan dat in het najaar wordt gepresenteerd.

3. Het vormgeven van het vormvrije deel van ENSIA. **Reactie:** dat nemen wij mee bij de uitwerking van de eerste aanbeveling voor de raad.
4. De colleges te verzoeken de voortgang op de aansporingen en de aanbevelingen bij de eerstvolgende rapportage in het kader van ENSIA, medio 2019, aan de raad te rapporteren. **Reactie:** wij nemen dit mee in de eerstvolgende bestuursrapportage de raad in oktober 2019

Tot zover onze bestuurlijke reactie. Graag zien wij de definitieve onderzoeksrapportage tegemoet.

Vragen

Als u nog vragen heeft dan kunt u contact met Hans Claassen. Hij is bereikbaar via telefoonnummer (0499) 58 33 33.

Met vriendelijke groet,
burgemeester en wethouders,

Ad de Jong
secretaris

Judith Keijzers-Verschelling
burgemeester

Rekenkamercommissie Kempengemeenten
Postbus 12
5520 AA EERSEL

Onderwerp : Bestuurlijke reactie rekenkameronderzoek Informatiebeveiliging en Privacy
Uw kenmerk :
Ons kenmerk : 19.07039

Reusel, 20 mei 2019

Geachte Mevrouw Boer,

Op 8 april 2019 ontvingen wij van u het onderzoeksrapport 'Informatiebeveiliging en privacy, gemeenten Eersel, Oirschot en Reusel-de Mierden'. Wij hebben kennis genomen van de feitelijkheden, conclusies en aanbevelingen die hierin zijn weergegeven. U heeft ons verzocht om eventuele opmerkingen in een bestuurlijke reactie terug te sturen. Middels deze brief sturen wij u onze reactie op het rapport toe.

Hoewel wij het eens zijn met veel van de door u gestelde conclusies en we de meeste aanbevelingen zullen overnemen, kunnen wij ons niet vinden in alle bevindingen en aanbevelingen zoals deze door u gesteld zijn. Hieronder hebben we een aantal punten uiteengezet.

Bevindingen
In het hoofdstuk '5. Bevindingen' beschrijft u de stand van zaken bij de gemeenten zoals deze was ten tijde van de interviews. Inmiddels zijn we een aantal maanden verder en geeft deze beschrijving geen actueel beeld meer van de huidige situatie, aangezien wij met veel van de aanbevelingen al aan de slag zijn (geweest). Deze aanbevelingen zullen wij, met de huidige situatie in ons achterhoofd, dus van u overnemen.

In het onderzoeksrapport heeft u de centrale onderzoeksvraag opgesplitst in drie thema's; Beleid en kaderstelling, Uitvoering en Bestuurlijk proces. De suggesties en aanbevelingen die u heeft opgenomen in 'Hoofdstuk 6. Conclusies en Aanbevelingen' zijn echter voornamelijk gericht op de uitvoering van informatiebeveiliging. Onze opmerkingen gaan dan ook met name over de aanbevelingen ten aanzien van de maatregelen die in uw rapportage onder het thema Uitvoering vallen.

Monitoring en logging
Als suggestie geeft u aan dat wij onze automatische logging voor monitorings- en handhavingsdoeleinden moeten uitbreiden. Hoewel het uiteraard goed is achteraf te kunnen inzien wie wat in welke applicatie gedaan heeft, is het niet zonder meer toegestaan om een logging van een applicatie te gebruiken voor handhavingsdoeleinden. Alleen indien er voldoende aanwijzingen van misbruik zijn, mag een logging gebruikt worden om onrechtmatig gebruik of fraude te onderzoeken. Monitoring of logging is voor veel applicaties dus handig, maar zorgt niet per definitie voor betere handhavingsmogelijkheden. Daarnaast zorgt een logging ook niet dat het risico op inefficiëntie en onrechtmatigheid bij het toewijzen van autorisaties aan medewerkers vermindert, zoals u in het

rapport stelt. Hiervoor zijn maatregelen aan de voorkant nodig, zoals een beter proces voor het aanmelden van een nieuwe medewerker.

CISO-functie
U geeft verder onder andere als aanbeveling om 'De CISO-functie ten behoeve van alle Kempengemeenten te positioneren bij de GRSK'. Wij zijn het niet eens met deze aanbeveling. De omschrijving die wordt gegeven aan een CISO is: "De CISO is dé spin in het web als het gaat om de beveiliging van informatie binnen de gemeente. Hij is verantwoordelijk voor het implementeren van, en toezicht houden op het informatiebeveiligingsbeleid binnen de gemeente. De CISO heeft een centrale rol in het beheren van alle processen die daarmee te maken hebben en moet daarbij voldoen aan de BIG." Ons inziens is dit een rol die binnen de gemeente uitgevoerd moet worden, zodat de CISO kan zien wat er speelt in de gemeente en daar direct op in kan spelen. Dit is anders dan de rol van een Functionaris Gegevensbescherming (FG), die meer een ondersteunende en toezichthoudende rol heeft. Tot slot zorgt het positioneren van de CISO-functie binnen de GRSK niet voor het vergroten van de menskracht en kennis die gemeenten in huis hebben op het gebied van informatieveiligheid, maar mogelijk zelfs voor minder menskracht en kennis in de gemeente zelf.

Uitvoering onderzoek
Tot slot hebben wij nog een opmerking ten aanzien van het onderzoeksproces. Hoewel de gemeentesecretarissen van te voren op de hoogte zijn gebracht van de aanstaande pen-testen, zijn zij niet geïnformeerd wanneer deze precies zouden plaatsvinden. Hierdoor zijn verschillende collega's lang bezig geweest met het achterhalen van de indringer en is zelfs bijna aangifte gedaan bij de politie.
In het vervolg zouden wij willen verzoeken de gemeentesecretarissen meer informatie te geven zodat eventuele aangiftes of andere maatregelen voorkomen kunnen worden.

Vragen?
Heeft u nog vragen? Dan kunt u contact met me opnemen. U bereikt me op maandag t/m vrijdag via telefoonnummer 0497 - 650 022 of via e-mail t.stoppelenburg@reuseldemierden.nl.

Met vriendelijke groet,
namens het college van burgemeester en wethouders,

Tessel Stoppelenburg
informatiemanager / beleidsmedewerker Interne Dienstverlening
team Interne Dienstverlening

7 Nawoord

Wij danken de colleges voor hun reacties en zijn verheugd te constateren dat informatiebeveiliging en privacy hoog op de bestuurlijke agenda staan.

Uit de reacties maken wij op dat alle drie de colleges het grootste deel van onze aanbevelingen opvolgt.

Op een aantal onderdelen van de reacties gaan wij graag nog kort in:

Eersel

Burgemeester en wethouders van Eersel stellen dat het onderzoeksrapport algemeen van aard is. Dat herkennen wij. Wij hebben de informatie inderdaad geclusterd op een aggregatieniveau dat wij voor de raad interessant achten. Meer gedetailleerde en gemeente-specifieke informatie hebben wij -uit het oogpunt van privacy en risicobeheersing- weergegeven in een zogenaamd penetratietest-rapport. Dit rapport hebben wij als vertrouwelijk/geheim aangemerkt, overhandigd aan de gemeentesecretaris en in een persoonlijk gesprek toegelicht. Op basis van bevindingen uit laatstgenoemd rapport zijn organisatorische en bedrijfsvoeringsmaatregelen in de gemeente doorgevoerd. Wij achten het niet in het belang van de gemeente als dit rapport openbaar wordt.

Reusel-De Mierden

Het college van Reusel-De Mierden geeft aan niet geïnformeerd te zijn over het precieze tijdstip van uitvoering van de penetratietesten en dat, als gevolg daarvan, diverse collega's lang bezig zijn geweest met het achterhalen van de indringer. Dit vinden wij spijtig. Echter, in een gesprek met de gemeentesecretarissen hebben wij vooraf de procedure van de penetratietesten toegelicht en aangegeven in welke week deze plaats zouden vinden. Dit is een gebruikelijke methode. Desondanks is het spijtig dat de test tot onnodige commotie heeft geleid.

Verder gaat het college in op de logging activiteiten van gebruikers. Het is niet onze bedoeling geweest om logging neer te zetten als enige middel om onrechtmatig gebruik of fraude te voorkomen. In de betreffende passage van ons rapport waarnaar het college verwijst staat daarom ook "de wijze waarop autorisaties van medewerkers en externen zijn ingeregeld" genoemd als maatregel aan de voorkant om inefficiëntie en onrechtmatigheid te voorkomen.

Tenslotte geeft het college aan dat logging van een applicatie niet zonder meer is toegestaan voor handhavingsdoeleinden. Met deze visie zijn wij het niet eens. Logging is een technische en organisatorische maatregel die vereist is in de BIG en de BIO, en ook in de AVG. Om incidenten te monitoren en bijvoorbeeld te controleren of medewerkers geen toegang tot teveel gegevens hebben. Daarmee kan een antwoord gegeven worden op de 5 W-vragen:

- Wat gebeurde er?
- Wanneer gebeurde het?
- Waar gebeurde het?
- Wie was betrokken?
- Waar komt het vandaan?

Zie hiervoor ook de in maart 2019 geüpdatete versie van de handreiking Aanwijzing Logging van de IBD.

Oirschot

Het college van Oirschot geeft aan dat, rekening houdend met de komst van het In Control Statement met ingang van 2021, het informatieveiligheidsbeleid in de paragraaf Bedrijfsvoering van de begroting zal worden vertaald in kaders voor die de raad.

CISO

Alle drie de colleges onderschrijven de belangrijke rol die voor de CISO is weggelegd. Wij adviseren deze functionaris te positioneren in de GRSK. Deze aanbeveling wordt door de colleges van Eersel en Reusel-De Mierden niet overgenomen. Het college van Oirschot wil daarover wel het gesprek wel aangaan, maar willen eveneens de aandacht voor informatieveiligheid en privacy gewaarborgd zien voor Oirschot. De drie colleges geven alle duidelijke argumenten voor hun keuze, die wij respecteren.

Bijlage 1. Verklarende woordenlijst en afkortingen

2FA	Twee factor authenticatie, zo wordt op 2 verschillende manieren gecheckt of degene die inlogt degene is die hij/zij aangeeft te zijn (zie 2-stapsverificatie)
2-staps-verificatie	zie 2FA
ACIB	Algemeen Contactpersoon Informatiebeveiliging, ontvangt berichten van algemene aard van de Informatiebeveiligingsdienst voor gemeenten (IBD)
AP	Autoriteit Persoonsgegevens
Applicatie	Softwareprogramma, zoals de BAG, BRP, SUWInet enz.
AVG (GDPR)	Algemene Verordening Gegevensbescherming, Europese regelgeving die de privacyregels in de Europese lidstaten harmoniseert (GDPR = General Data Protection Regulation)
BAG	Basisregistratie Adressen en Gebouwen, applicatie met onder andere gegevens over adressen en gebouwen in de gemeente
BIG	Baseline Informatiebeveiliging Gemeenten, maatregelen voor de informatiebeveiliging bij gemeenten, in 2013 als standaard afgesproken in VNG-verband
BIO	Baseline Informatiebeveiliging Overheid, verwachting is dat hier de BIR en BIG in zullen opgaan vanaf 2020
BIR	Baseline Informatiebeveiliging Rijksdienst, geldt als basis voor de BIG
BIV	Beschikbaarheid – Integriteit – Vertrouwelijkheid. Termen waarop de beveiligings-risico's van de informatie/applicaties zijn geënt
BRP	Basisregistratie Personen, applicatie met persoonsgegevens van de inwoners
BYOD	Bring your own device, betekent dat medewerkers en externen hun eigen apparaten (laptops, smartphones, usb-sticks enz.) meenemen en inloggen in het gemeentelijk systeem
CERT	Computer Emergency Response Team, multidisciplinair samengesteld team dat kan acteren op incidenten en crises
CIO	Chief Information Officer
CISO	Chief Information Security Officer
Cloud	De cloud staat voor een netwerk van computers die een soort 'wolk van computers' vormt, waarbij de eindgebruiker niet weet op hoeveel of welke computer(s) de software draait of waar die computers precies staan
CYOD	Choose your own device, beleid dat inhoudt dat medewerkers en eventueel externen apparaten (laptops, smartphones, usb-sticks enz.) kunnen kiezen uit een beperkt assortiment, waarop de veiligheidsmaatregelen reeds zijn aangebracht
DPIA (ook PIA)	Data protection impact assessment, analyse op risico's in verband met privacy en gegevensbescherming bij verwerkingsprocessen. Onder de AVG verplicht bij gegevensverwerking met waarschijnlijk een hoog privacyrisico.
ENSIA	Eenduidige Normatiek Single Information Audit, eenmalige informatieverstrekking en eenmalige IT-audit voor de horizontale (richting gemeenteraad als toezichthouder) en verticale verantwoording (richting landelijke toezichthouders)
FG	Functionaris gegevensbescherming, verplicht voor overheden.
GAP	Is de Engelse term voor ‘kloof’. Dat betekent hier het verschil tussen de bestaande situatie en de gewenste situatie

GAP-analyse	Controle of en in welke mate de maatregelen uit de BIG geïmplementeerd zijn
GDPR	General Data Protection Regulation (zie AVG)
GBA	Gemeentelijke Basisadministratie
GR	Gemeenschappelijke regeling
IBD	Informatiebeveiligingsdienst voor gemeenten
ICT	Informatie- en communicatietechnologie
IP-adres	Internetprotocol adres, bestaande uit (momenteel) 4 setjes van drie cijfers. Met behulp van deze set cijfers is elke computer en apparaat dat op internet is aangesloten te traceren
IPv6	Is de opvolger van het traditionele IP-adres. De oude IP-adressen, eigenlijk IPv4, raakten op. Onder andere vanwege de groei van het aantal apparaten dat op internet aangesloten wordt
ISMS	Information security management system
KING	Kwaliteitsinstituut Nederlandse Gemeenten, heet tegenwoordig VNG Realisatie
OWASP	Open Web Application Security Project
P&C-cyclus	Planning & Control cyclus
PDCA	Plan-Do-Check-Act beleidscyclus
Phishing mail	Vorm van internet oplichting en fraude, door middle van een vals e-mail bericht 'hengelen' naar inlog- of andere persoonsgegevens
PIA (ook DPIA)	Privacy impact assessment, analyse op risico's in verband met privacy en gegevensbescherming bij verwerkingsprocessen. Onder de AVG verplicht bij gegevensverwerking met waarschijnlijk een hoog privacy risico.
PKI-certificaat	Public Key Infrastructure. Een PKI(overheid)-certificaat is een internationale standaard voor de digitale ondertekening bij het versturen van gegevens en berichten.
Privacy by default	Onderdeel van privacy by design, waarbij de standaardinstellingen zo privacy-vriendelijk mogelijk zijn ingesteld
Privacy by design	Betekent dat bij het ontwerp van producten en diensten nagedacht wordt over privacy
RIVG	Rijksdienst voor Identiteitsgegevens
SSO	Single Sign On, op 1 werkplek via 1 aanmelding toegang krijgen tot alle applicaties waar de gebruiker recht op heeft
Spoofing	Het verzenden van e-mails waarbij het e-mail adres van de afzender vervalst is
TPM	Third Party Memorandum. Verklaring dat de derde partij, die de gegevens voor de gemeente bewerkt voldoet aan de geldende richtlijnen inzake informatiebeveiliging
Url	Uniform Resource Locator. Verwijst naar een unieke adres waarmee de locatie van een webpagina op internet wordt aangegeven of een e-mailadres
VCIB	Vertrouwd Contactpersoon Informatiebeveiliging, ontvangt berichten van vertrouwelijke aard van de Informatiebeveiligingsdienst voor gemeenten (IBD)
Verwerkingsregister	Register waarin de gemeente bijhoudt welke persoonsgegevens de gemeente en de verwerkers die deze inschakelt verwerkt
VNG Realisatie	Kwaliteitsinstituut van de VNG (voorheen KING)
VPN	Virtueel privé netwerk (versleutelde beveiligde verbinding)

Bijlage 2. Lijst geraadpleegde stukken en lijst respondenten

De geraadpleegde stukken en de geïnterviewde personen zijn hieronder weergegeven, per onderdeel/gemeente.

SSC

- Rapportage Third Party Mededeling ICT-beheersprocessen SSC de Kempen 2018, 6-8-2016 + oplegnotitie
- Penetratie Test, december 2017-januari 2018
- SSC de Kempen, continuïteitsplan, 2-1-2018
- Handboek Operations SSC, Beheerprocesbeschrijvingen en bijbehorende werkinstrukties, 15-2-2018, dynamisch document
- InformatiebeveiligingsMaatregelen planning SSC/GRSK 2018, zd
- Rapportage interne beveiligingsaudit, Inzis BV, 12-3-2018

Eersel

- 10 gouden regels informatiebeveiliging-privacy
- 201806 ENSIA Activiteitenplanning – Concept
- 201806 ENSIA Plan van aanpak – DEF
- Aanmelding ACIB bij IBD
- Aansluitformulier VCIB bij IBD
- Bevindingen nulmeting Informatieveiligheid & Privacy
- Blog intranet gemeente Eersel - Afsluiten verwerkersovereenkomst
- Blog intranet gemeente Eersel - vanaf nu geldt de AVG
- Blog Intranet gemeente Eersel - wat is een datalek en hoe te handelen
- Checklist 'verwerkersovereenkomsten' en model verwerkersovereenkomst
- Collegeverkkaring ENSIA, 24-4-2018
- Eersel_Verbeterplan SuWinet-aansluiting 2017
- Eersel_Verbeterplan_DigiD_Aansluitingen 2017
- Handboek Operations SSC, 4-2-2018 (zie SSC)
- Incidentenregister datalekken 2018
- Informatiebeveiligingsbeleid v12 def 2014
- Informatiebeveiligingsplan definitief 2014, 3-3-2015
- Informatieveiligheidbeleid Kempen 2018 – concept
- Notitie PO instrumenten voor mobiel werken_ versie 3
- Privacybeleid gemeente Eersel 2018
- Procedure meldplicht datalekken Eersel
- Rapportage Zelfevaluatie Informatieveiligheid Eersel
- TPM Iburgerzaken Eersel 2017
- TPM SIM Eersel 2017
- Vaststelling privacybeleid gemeente Eersel Gemeenteblad 24-05-2018
- Vaststelling privacybeleid sociaal domein kempengemeenten 24-05-2018
- Verwerkingsregister gemeente Eersel dynamisch
- Verwerkingsregister GRSK

- Wachtwoordenpolicy

Reusel-De Mierden

- 201806 ENSIA Activiteitenplanning
- 201806 ENSIA Plan van aanpak – DEF
- Aanstellen VCIB
- Bevindingen gap analyse BING v3 def 2014
- Bezoekers in het gemeentehuis
- Cleandeskbeleid, 17-8-2018
- Collegeverklaring ENSIA 2017
- Enquête informatiebeveiliging definitief
- Informatiebeveiligingsbeleid SSC De Kempen v12 def, 4-12-2014
- Informatiebeveiligingsplan Kempen 2015
- Informatieveiligheidbeleid Kempen concept 2018, 9 oktober 2018
- Intranet document AVG
- Kennissessie Persoonlijk contact met inwoners, powerpoint
- Kennissessie Rechten van betrokkenen, powerpoint
- Kennissessie Verwerkersovereenkomst, powerpoint
- Lijst van respondenten
- Medewerkersbijeenkomst 13-09-2018, powerpoint
- Model Verwerkersovereenkomst, 2-11-2018
- Notitie PO instrumenten voor mobiel werken_ versie 3
- Poster vakantie informatieveiligheid2
- Presentatie informatiebeveiliging en privacy voor college
- Privacybeleid Gemeente Reusel - de Mierden
- Privacybeleid GRSK en Kempengemeenten
- Privacybeleid Sociaal Domein Kempengemeenten, maart 2018
- Procedure Meldplicht datalekken
- Procedure Rechten van Betrokkenen
- Procedure Verwerkersovereenkomst
- Rollen en namen (op informatiebeveiliging en privacy)
- TPM-verklaring iBurgerzaken herG55LKW DigiD 1819 TPM - Gemeente Reusel-De Mierden
- TPM-verklaring SIM 2017, 29-11-2017
- Verbeterplan DigiD aansluitingen
- Verbeterplan SuWinet-aansluiting

Oirschot

- B&W Algemene Verordening Gegevensbescherming, 22-5-2018
- Benoeming FG, 26-4-2018
- Mandaatregister aanvulling AVG gemeente Oirschot
- Privacybeleid Oirschot, 22-5-2018
- Privacybeleid sociaal domein Kempengemeenten 2018, maart 2018
- Privacyreglement Oirschot, 22-5-2018
- Privacystatement Oirschot, zonder datum
- Verwerkingsregister gemeente Oirschot--VNG--versie 1.0
- Verwerkingsregister GRSK 1.3

- AQR9LV PRLG DigiD beveiligingsassessment TPM - Gemeente Oirschot, 27-9-2018
- Collegeverklaring ondertekend zonder bijlagen, 24-4-2018
- Flyer AVG
- Informatiebeveiligingsbeleid SSC De Kempen v11, 28-10-2014
- Informatiebeveiligingsplan SSC De Kempen definitief, 3-3-2015
- Informatieveiligheidbeleid Kempen, 9-10-2018
- Presentatie_IB_Bewustwording1
- TPM SSC 2018, 8-6-2018
- U-WA.05 20171129 TPM Oirschot, 29-11-2017
- Verbeterplan DigiD aansluitingen-Oirschot

Functies van geïnterviewde respondenten

- Informatiemanager en beoogd chief information security officer (CISO), Reusel-De Mierden
- Burgemeester, Reusel-De Mierden
- Plaatsvervangend secretaris, Reusel-De Mierden
- Gemeentesecretaris, Eersel
- Gegevensbeheerder en functionaris informatiebeveiliging, Eersel
- Burgemeester, Eersel
- Privacyfunctionaris, Eersel
- Afdelingshoofd Dienstverlening, Eersel
- Gemeentesecretaris, Oirschot
- Concerncontroller (tevens CISO), Oirschot
- Informatiemanager, Oirschot
- Wethouder, Oirschot
- Manager SSC De Kempen
- Team coördinator H.A.S., SSC De Kempen
- Securitybeheer, SSC De Kempen
- Functionaris gegevensbescherming (FG), GRSK

Bijlage 3. Onderzoeksvragen en normen

Hieronder gaan we nader in op de onderzoeksvragen en de normen die de basis vormen voor de beoordeling door de rekenkamercommissie. In de tweede kolom zijn de normen weergegeven op basis waarvan de rekenkamercommissie beoordeelt of de uitvoering van het informatiebeveiligingsbeleid in de drie Kempengemeenten voldoet aan de geldende regels.

A. Beleid en kaderstelling	Normen
1. Welke kaders en richtlijnen hebben raad en college met elkaar afgesproken ten aanzien van informatiebeveiliging? Hoe is de kwaliteit van deze kaders en richtlijnen?	In de BIG is afgesproken, dat het integrale beleid op het terrein van informatiebeveiliging door de colleges van B&W moet worden vastgesteld en gepubliceerd voor werknemers en relevante externe partijen. Het college draagt het beleid actief uit.[2] De rol van de Chief Information Security Officer (CISO) is beschreven en ingevuld conform de richtlijnen in de BIG.[3]
2. Hebben de gemeenten een goed beeld van de belangrijkste risico's op het gebied van informatiebeveiliging en in het bijzonder de bescherming van (bijzondere) persoonsgegevens en andere gevoelige informatie?	Het beleid is risico gebaseerd en een verantwoordelijkheid van het lijnmanagement. Het management stelt naar aanleiding van een GAP-analyse het informatiebeveiligingsbeleid op. In de risicoanalyse geeft het management aan of risico's beheerst dan wel geaccepteerd worden, inclusief de bijbehorende maatregelen uit de BIG. Jaarlijks wordt op basis van deze risicoanalyse het informatiebeveiligingsplan ingevuld. [4] In de BIG hebben gemeenten afgesproken dat risico's op informatieveiligheid die betrekking hebben op externe partijen, die bijvoorbeeld persoonsgegevens verwerken, expliciet worden meegenomen. Daarover moet jaarlijks worden gerapporteerd. Het aspect informatiebeveiliging moet behandeld worden in overeenkomsten met derde partijen.[5] Ook de AVG stelt eisen aan de overeenkomst tussen verwerkingsverantwoordelijke, in dit geval de gemeente, en de verwerker. Bijvoorbeeld met betrekking tot het toepassen van passende technische en organisatorische maatregelen, opdat de verwerking aan de vereisten van de AVG voldoet en de bescherming van de rechten van de betrokkene is gewaarborgd.[6]
B. Uitvoering	
3. Hebben de gemeenten adequate maatregelen genomen om de (bijzondere) persoonsgegevens en andere gevoelige informatie die zij in beheer hebben te beschermen tegen de belangrijkste veiligheidsrisico's? Bij deze vraag worden zowel processen, organisatie, afspraken als houding & gedrag bedoeld.	Het totaal aan maatregelen geeft voldoende waarborgen voor een goede bescherming van de (bijzondere) persoonsgegevens en andere gevoelige informatie die de gemeenten in beheer hebben. Ten aanzien van de beoordeling van het beveiligingsbeleid is in de BIG geregeld dat er periodieke beveiligingsaudits worden uitgevoerd. Over het functioneren van informatiebeveiliging wordt volgens de P&C-cyclus gerapporteerd aan het lijnmanagement.[7]

2 Zie Tactische BIG, items 5 en 6, resp. Informatiebeveiligingsbeleid en Interne organisatie.
3 Zie Tactische BIG, item 6.1.2, Coördineren van de beveiliging.
4 Zie Tactische BIG, items 5 en 6, resp. Informatiebeveiligingsbeleid en Interne organisatie.
5 Zie Tactische BIG, item 6.2, Externe Partijen.
6 Zie AVG, artikel 28.
7 Zie Tactische BIG, item 6.1.8, Beoordeling van informatiebeveiligingsbeleid; 15.2, Naleving van beveiligingsbeleid en –normen en technische naleving.

	In de BIG is opgenomen dat er een procedure wordt vastgesteld voor de wijze waarop informatie-beveiligingsgebeurtenissen en zwakke plekken in de beveiliging worden beheerd en gerapporteerd. Ook geeft de BIG aan dat er geleerd moet worden van de incidenten.[8] In de BIG is afgesproken dat op basis van een risicobeoordeling een continuïteitsplan met betrekking tot informatiebeveiliging wordt opgesteld. Daarmee worden essentiële procedures voor continuïteit geïdentificeerd, zoals het veilig stellen, herstel en reconstructie van informatie enz.[9] In de BIG is afgesproken om (integraal) te leren van beveiligingsmeldingen met als doel beheersmaatregelen te verbeteren.[10] Als randvoorwaarde is in de BIG onder andere geformuleerd dat informatieveiligheid een verantwoordelijkheid is van het lijnmanagement en dat kennis en expertise essentieel zijn.[11] Vanaf 1-1-2016 moeten in het kader van de Meldplicht ernstige datalekken direct gemeld worden bij de Autoriteit Persoonsgegevens en soms aan de betrokkenen. Dat is nu geregeld in de AVG.[12]
4. Is het mogelijk om oneigenlijk toegang te krijgen tot (bijzondere) persoonsgegevens en andere gevoelige informatie die de gemeenten in beheer hebben? Zo ja, wat zijn de mogelijke consequenties?	Het totaal aan maatregelen geeft voldoende waarborgen voor een goede bescherming van de (bijzondere) persoonsgegevens en andere gevoelige informatie die de gemeenten in beheer hebben. De getroffen maatregelen ter beveiliging van de (bijzondere) persoonsgegevens en andere gevoelige informatie vloeien logisch voort uit de risicoanalyses en zijn overeenkomstig de huidige stand van de techniek.[13]
C. Bestuurlijk proces	
5. In welke mate is de raad in de gelegenheid zijn kaderstellende en controlerende rol waar te maken?	De raden zijn gepositioneerd om de kaderstellende en controlerende rol die zij hebben met betrekking tot het gemeentelijk beleid op informatiebeveiliging en privacy, adequaat op te pakken. Daartoe dienen zij tijdig en volledig geïnformeerd te worden in het kader van de P&C-cyclus (zie ook ENSIA hierna).[14]
6. Hoe is de informatievoorziening aan de raad?	In de BIG hebben gemeenten afgesproken dat over het functioneren van de informatiebeveiliging aan het management en bestuur wordt gerapporteerd, in het kader van de P&C-cyclus. De raden moeten minimaal eens per jaar geïnformeerd worden. De Eenduidige Normatiek Single Information Audit (ENSIA) verbindt vanaf 2017 de verschillende verantwoordingsprocedures met de P&C-cyclus.[15]

8 Zie Tactische BIG, item 13, Beheer van informatiebeveiligingsincidenten.
9 Zie Tactische BIG, item 14, Bedrijfscontinuïteitsbeheer.
10 Zie Tactische BIG, item 13.2.2, Leren van informatiebeveiligingsincidenten.
11 Zie Tactische BIG, 1.3, Randvoorwaarden.
12 Zie AVG, artikelen 32 en 33.
13 Zie § 1.4 Normenkaders en aansluitvoorwaarden, Tactische BIG, p. 3. De verschillende normen op dit vlak, als minimumvereisten beschreven, zijn opgenomen in de hoofdstukken 6,7,9,10,11 en 12 van de BIG, zie Tactische BIG, p. IX.
14 Zie Tactische BIG, item 6.1.8, Beoordeling van het informatiebeveiligingsbeleid. Voor de rapportage over informatiebeveiliging in het kader van de P&C-cyclus wordt meestal een Information Security Management System (ISMS) opgesteld.
15 De verschillende verantwoordingsprocedures betreffen de applicaties: Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT) en de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet). Deze worden in ENSIA gekoppeld aan de P&C-cyclus.