Quick Scan Informatiebeveiligingsbeleid Neder-Betuwe

29-3-2017, Neder-Betuwe

Inhoud

Conclusies, aansporingen en aanbevelingen

De gemeente heeft reeds in 2013-2015 stappen gezet om informatiebeveiliging conform de maatregelen uit de BIG te implementeren. Er is een GAP-analyse gemaakt, het informatiebeveiligingsbeleid is vastgesteld en er is een handboek informatiebeveiligingsbeleid vastgesteld. Het beeld is dat de gemeente goed op weg is gegaan, maar dat in 2016 enige vertraging in de implementatie is opgetreden. De gemeente heeft in de loop van 2016 de draad weer opgepakt met de verdere en integrale implementatie van de BIG. De risicoanalyse wordt bijgewerkt en een gestructureerde P&C-cyclus door middel van een ISMS wordt opgezet. De bedoeling is dat deze in het eerste kwartaal van 2017 gereed komt.

De aansturing is aan de top van de organisatie goed belegd. De burgemeester is portefeuillehouder en is zeer betrokken op informatieveiligheid, samen met de gemeentesecretaris. Alle respondenten geven aan dat de rol van de burgemeester cruciaal is voor het draagvlak binnen de organisatie. Het is afwachten hoe de portefeuilleverdeling en betrokkenheid binnen het college op dit onderwerp na het vertrek van de burgemeester zal zijn. Door toenemende digitalisering en kwetsbaarheid van systemen is het noodzakelijk dat de betrokkenheid op informatiebeveiliging ook in de toekomst minstens even groot zal zijn als nu het geval is.

De gemeente Neder-Betuwe heeft een groot deel van het gegevensbeheer geoutsourcet. Dat is een te verdedigen keuze, mede gelet op hetgeen van een kleine gemeentelijke organisatie geëist mag worden met betrekking tot aanwezige kennis, expertise en voorzieningen op ICT-gebied. Meer gemeenten volgen die lijn, ook grotere, zoals recent de gemeente Groningen.[1] Daardoor is slechts een basis aan operationele kennis nodig binnen de organisatie. Het is wel gewenst dat bij het lijnmanagement strategische kennis aanwezig is op de risico's op het informatiebeveiliging, zodat de organisatie hierop 'in control' is. Desondanks blijft het risico van personeelswisselingen en verlies van kennis onvermijdelijk bij een kleine organisatie als de gemeente Neder-Betuwe. Mogelijk zijn hierover afspraken met naburige gemeenten te maken om lacunes tijdelijk op te vangen.

In het beleid is de rol van informatiebeveiligingscoördinator per afdeling beschreven, maar deze mist in de uitvoering. De taken van deze coördinator op informatiebeveiliging zijn niet expliciet in een functie of rol belegd. Impliciet zijn de taken wel belegd, en de applicatiebeheerders voeren deze taken in de praktijk uit. Van een andere rol, de algemeen contactpersoon informatiebeveiliging (ACIB), bleek bij de betreffende medewerker niet bekend te zijn dat hij deze vervulde. Niet alle functies en taken zijn expliciet conform het vastgestelde informatiebeveiligingsbeleid bij de betreffende

[1] Binnenlands Bestuur, 5-2-2017.

medewerkers belegd of bekend. De rekenkamercommissie constateert dat daardoor een risico op ondoeltreffendheid in de uitvoering van het informatiebeveiligingsbeleid aanwezig is.

De gemeente is zich ervan bewust dat een van de grootste risico's onachtzaamheid bij medewerkers is, of het niet voldoende onderkennen van de risico's. De incidenten die zich in 2016 voordeden zijn daaraan te wijten. De gemeente acteert daarop en is bezig met bewustwordingscampagnes. Helaas zullen dit soort incidenten nooit helemaal vermeden kunnen worden. Kwaad-willenden gaan steeds geavanceerder te werk gaan en de technische beveiliging loopt daarop per definitie achter. Voor zover de rekenkamercommissie heeft kunnen constateren lijkt er bij de medewerkers sprake van een open meldcultuur te zijn. Dat is noodzakelijk om de dreiging van software van kwaadwillenden snel te achterhalen en schade zoveel mogelijk te beperken.

De gemeenteraad is nauwelijks aangesloten op de uitvoering van het informatiebeveiligingsbeleid. Terwijl raadsleden zich in het algemeen afvragen hoe het ervoor staat met de uitvoering ervan. En niet ten onrechte, want informatiebeveiliging en de borging van de privacy, van bij de gemeente in beheer ondergebrachte gegevens, zijn kritieke prestatie-indicatoren voor de dienstverlening van de gemeente. Raadsleden vertrouwen erop dat de uitvoering goed gaat en dat zij tijdig op de hoogte worden gebracht als er iets mis gaat. De raad was echter maar van één van de twee incident op de hoogte gebracht. De rekenkamercommissie constateert dat de raad zijn controlerende en kaderstellende rol op bedrijfsvoering, niet optimaal kan vervullen door de te geringe informatievoorziening in de P&C-cyclus en het ontbreken van heldere afspraken op tussentijds informeren.

Dit onderzoek van de rekenkamercommissie is een quick scan, op basis van deskresearch en interviews. Om de uitvoering meer diepgaand te testen is een ander onderzoek vereist. De gemeente heeft al eens een mystery guest ingehuurd om op de afdelingen rond te lopen en de uitvoering van het informatiebeveiligingsbeleid op een aantal aspecten te toetsen. De gemeente is van plan dit vaker te doen. Uit onderzoek, onder andere door rekenkamers, blijkt dat de inhuur van een 'ethisch' hacker andere kwetsbaarheden van de informatiebeveiliging kan blootleggen. De rekenkamercommissie geeft het college in overweging het systeem aan een dergelijke test bloot te stellen.

Resumerend

Resumerend constateert de rekenkamercommissie op basis van deze quick scan dat de gemeente aan een groot deel van de normen op informatiebeveiligingsbeleid voldoet. De bestuurlijke aansturing van informatiebeveiligingsbeleid is goed belegd in de organisatie. De meeste richtlijnen en uitgangspunten op informatiebeveiliging zijn op basis van een risicoanalyse beschreven, en de meeste functies, zoals de CISO, zijn belegd. Op terrein van de ICT is veel uitbesteed. De systemen en de checks daarop zijn, voor zover op basis van deze quick scan is te constateren, dusdanig ingericht dat de continuïteit van de dienstverlening is geborgd. Dat geldt ook voor de veilige

opslag en verwerking van informatie, ook bij derden. Er wordt voldoende aandacht besteed aan de bewustwording van het personeel op de risico's van informatieveiligheid.

Op dit moment functioneert managementbeheerssysteem op informatiebeveiliging nog niet. Het (ISMS) is in het tweede kwart van 2017 gereed. Zorgpunten zijn het expliciet beleggen van de in het beleid geformuleerde functies en borging van de benodigde kennis op informatiebeveiliging bij het lijnmanagement. De gemeenteraad is nog niet volledig aangesloten op het informatiebeveiligingsbeleid.

Bovenstaande leidt tot de volgende aansporingen voor het college en een aanbeveling voor de raad.

Aansporingen

Aansporingen voor het college

- Ga verder met de voorgenomen implementatie van de maatregelen uit de BIG, de risicoanalyse, het ontwikkelen van het ISMS en de update van het Handboek Informatiebeveiligings-beleid.
- Definieer in het Handboek welke operationele en strategische kennis en expertise op ICT bij het lijnmanagement aanwezig moet zijn.
- Beleg de rollen, taken en functies die in het Handboek staan beschreven expliciet bij medewerkers in de uitvoering.
- Blijf inzetten op bewustwording en het gedrag van medewerkers op informatiebeveiliging.

Aanbeveling

Aanbeveling voor de raad

- Informatiebeveiliging is een kritieke prestatie-indicator voor de dienstverlening van de gemeente aan burgers en instellingen/bedrijven. Maak met het college afspraken over hoe en wanneer u geïnformeerd wil worden op het aspect informatiebeveiliging in het kader van de bedrijfsvoering.

Toelichting: De praktijk hierop bij andere gemeenten is divers. Te denken valt aan (half)-jaarlijkse rapportage van een aantal kritieke prestatie-indicatoren, zoals de prioriteiten in het jaarlijks te updaten handboek, aanwezigheid van 'in control' statements van het lijnmanagement indien deze worden afgegeven, het percentage deelname medewerkers aan bewustwordingssessies, aantal incidenten en eventueel beheersmaatregelen, enz. Over incidenten met een hoge bestuurlijke, financiële of maatschappelijke impact heeft de raad aangegeven direct en volledig geïnformeerd te willen worden.

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. Berichten in media over ontoereikende beveiliging van sites en datalekken door onzorgvuldige acties van ambtenaren en leveranciers doen het vertrouwen van de burger niet bepaald goed. 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 de burgers aantasten.

De burger mag erop vertrouwen dat de overheid informatieveiligheid serieus neemt en alles wat technisch mogelijk is doet om kwaadwillenden buiten de digitale poort te houden en tracht menselijke fouten te voorkomen. In 2013 hebben de burgemeesters in VNG-verband afgesproken zich te houden aan een aantal richtlijnen, verzameld in de Baseline Informatieveiligheid Gemeenten, (BIG). Regelgeving is strikter geworden en sinds januari 2016 is het verplicht datalekken bij de Autoriteit Persoonsgegevens te melden.

Redenen voor de rekenkamercommissie Neder-Betuwe om een quick scan uit te voeren naar het informatieveiligheidsbeleid van de gemeente. Etienne Lemmens van Prae Advies en Onderzoek heeft het veldwerk voor dit onderzoek uitgevoerd.

Leeswijzer

Voor de inleiding worden de conclusies, aansporingen en aanbevelingen gepresenteerd. Hieronder gaan we in hoofdstuk 2 in op het doel van het onderzoek, de onderzoeksvragen en de normen. In hoofdstuk 3 beschrijven we kort de onderzoeksaanpak. In hoofdstuk 4 worden per onderzoeksvraag de bevindingen gepresenteerd. Daar wordt aangegeven in welke mate de bevindingen voldoen aan de norm.

2 Doel, onderzoeksvragen en normen

Het doel van deze quick scan is om inzicht te geven in de huidige staat van beveiliging van informatie bij de gemeente Neder-Betuwe, het vergroten van de bewustwording van het belang en de kennis van informatiebeveiliging bij raad, college van B&W en organisatie en het formuleren van concrete verbeteracties.

De centrale vraag is: Heeft de gemeente Neder-Betuwe de informatieveiligheid voldoende georganiseerd en geborgd?

Deze vraagstelling is nader uitgewerkt in een aantal deelvragen. In de onderstaande tabel zijn deze onderzoeksvragen opgenomen. In de tweede kolom zijn de aan die deelvraag gerelateerde normen opgenomen. De normen zijn grotendeels afkomstig uit de Baseline Informatieveiligheid Gemeenten (BIG) en de Wet Bescherming Persoonsgegevens (Wbp).

Tabel 1. Onderzoeksvragen en normen

Onderzoeksvragen	Normen
1. Hoe heeft het college van B&W de punten van de Resolutie opgepakt? Geldt de BIG als norm voor het basis beveiligingsniveau van de gemeente?	• Het college van B&W heeft integraal beleid op informatiebeveiliging, gebaseerd op de BIG, vastgesteld en gepubliceerd. • Het integrale beleid op informatieveiligheid is gebaseerd op een systematische analyse en assessment van de risico's.
2. Hoe is het informatiebeveiligingsbeleid vormgegeven in de gemeente? Wie zijn er als verantwoordelijken aangesteld en is er aandacht voor bewustwording?	• De gemeente heeft uitgangspunten voor beheer, gebruik en uitwisseling van (persoons)gegevens beschreven en vastgesteld. • De gemeente heeft een Chief Information Security Officer (CISO) benoemd. • Informatieveiligheid is een verantwoordelijkheid van het lijnmanagement. Kennis en expertise moeten op dat niveau aanwezig zijn. • De gemeente schenkt aandacht aan bewustwording bij medewerkers en heeft de organisatie ingericht op constant leren en verbeteren.
3. Welke risico's accepteert het college van B&W voor de gemeente en welke niet? Welke politiek-bestuurlijke en maatschappelijke gevolgen kan dit hebben in geval van een incident? Is de privacy van de burgers gegarandeerd?	• De gemeente heeft de risico's op informatieveiligheid vastgesteld en geanalyseerd. • In het Informatiebeveiligingsplan is beschreven welke risico's beheerst of geaccepteerd worden, inclusief de bijbehorende maatregelen uit de BIG. Tevens is gemeld op welk niveau het plan is vastgesteld. • De richtlijnen en beleidsregels voldoen aan de belangrijkste bepalingen uit de Wet bescherming persoonsgegevens.[2]
4. Functioneert de Planning & Control (P&C)cyclus van informatieveiligheid binnen de gemeente? Vindt er een	• Over het functioneren van de informatiebeveiliging wordt aan management en bestuur gerapporteerd in het kader

[2] De belangrijkste richtlijnen uit de Wbp zijn: Persoonsgegevens mogen alleen in overeenstemming met de wet en op een behoorlijke en zorgvuldige manier worden verwerkt; Persoonsgegevens mogen alleen voor welbepaalde, vooraf uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld. En alleen verder worden verwerkt voor daarmee verenigbare doeleinden; Degene van wie persoonsgegevens worden verwerkt, moet op de hoogte zijn van de identiteit van de organisatie of persoon die de persoonsgegevens verwerkt en van het doel van de gegevensverwerking; De gegevensverwerking moeten op een passende manier worden beveiligd. Voor bijzondere gegevens, zoals over ras, gezondheid en geloofsovertuiging, gelden extra strenge regels.

jaarlijkse toetsing plaats, om na te gaan of de gemeente 'in control' is op het gebied van informatie-veiligheid via peer reviews, audits of self-assessments? Wat zijn de resultaten van deze toetsing? Wordt de cyclus jaarlijks bijgesteld op basis van lessons learned?	van de P&C-cyclus.[3] • In de P&C-cyclus wordt gerapporteerd over de periodieke beveiligingsaudits, zoals de zelfevaluaties op de Basisregistratie Personen (BRP) en Paspoorten en Nederlandse Identiteitskaarten (PNIK), audits op de Basisregistratie Adressen en Gebouwen (BAG) en SUWINET. • De gemeente rapporteert de jaarlijkse assessments van de DIGID-loketten aan Logius. • Ten behoeve van de accountantscontrole wordt jaarlijks een ICT-survey gehouden. • Over het thema digitale veiligheid wordt gerapporteerd aan 'waarstaatjegemeente.nl'.[4] • De gemeente heeft een procedure vastgesteld voor de wijze waarop informatiebeveiligingsgebeurtenissen en zwakke plekken worden beheerd en gerapporteerd. • De gemeente leert van de incidenten en heeft de organisatie ingericht op constant leren en verbeteren.
5. Zijn binnen de gemeente procedures opgesteld voor incidenten? Welke risico's loopt de gemeente in geval van verstoring of cyberaanval, ook wanneer deze verstoring elders in de keten plaatsvindt? Hoeveel incidenten zijn er in de afgelopen periode (maand/half jaar) geweest? Worden die incidenten bij de Informatiebeveiligingsdienst voor gemeenten (IBD)() en indien nodig bij de Autoriteit Persoonsgegevens gemeld?	• Op basis van een risicobeoordeling is een continuïteitsplan met betrekking tot informatiebeveiliging opgesteld. Met daarin de essentiële procedures voor continuïteit, zoals veilig stellen, herstel en reconstructie van informatie. • Risico's op informatieveiligheid die betrekking hebben op externe partijen zijn expliciet meegenomen in de integrale risicoanalyse. • De gemeente is aangesloten bij de IBD[5]. De gemeente meldt incidenten op informatieveiligheid aan de IBD, en krijgt meldingen terug. • Datalekken worden aan de Autoriteit Persoonsgegevens gemeld.
6. Is er per domein zicht op het netwerk van landelijke en regionale partners waarin de gemeente opereert? Is er zicht op de informatiehuishouding en de informatie-uitwisseling in dit netwerk van actoren? Is er zicht op de borging van informatie-veiligheid in de praktijk bij deze actoren? Worden er (contractuele) afspraken over informatieveiligheid gemaakt bij het opzetten van (regionale) samenwerkings-verbanden en bij de inkoop van diensten?	• Risico's op informatieveiligheid die betrekking hebben op externe partijen zijn expliciet meegenomen in de integrale risicoanalyse, en daar wordt jaarlijks over gerapporteerd in de P&C-cyclus. • Het aspect informatiebeveiliging wordt behandeld in overeenkomsten met derde partijen.
7. Op welke wijze is de gemeenteraad betrokken bij het informatieveiligheids-	• De gemeenteraad is gepositioneerd om zijn kaderstellende en controlerende taak met betrekking tot

[3] In de P&C-cyclus wordt gerapporteerd aan het lijnmanagement. Voor rapportage aan de gemeenteraad in het kader van de P&C-cyclus geeft de BIG geen richtlijnen. Vanwege het bestuurlijke, financiële en publieke belang van informatieveiligheid, en het belang dat raadsleden vaak hechten aan het onderwerp, stellen wij voor reguliere rapportage aan de raad mee te nemen als norm. Zie daarvoor §4.7 en de norm.

[4] Dit is geen eis binnen de strategische of tactische BIG, maar in de Resolutie van de VNG staat dat degenen die de resolutie aannemen ermee instemmen dat: "Gemeenten de lokale invulling rondom het thema van informatieveiligheid transparant maken voor burgers, bedrijven en (keten)partners. Deze transparantie wordt onder meer behaald door gebruik te maken van waarstaatjegemeente.nl. Deze openbare informatie vormt de basis voor jaarlijkse collegiale beoordeling (peer reviews)."

[5] Aansluiting bij de IBD is geen eis in de BIG. Voor aansluiting moeten 4 stappen gerealiseerd zijn: benoeming van twee functionarissen Algemene Contactpersoon Informatiebeveiliging (ACIB) en Vertrouwde Contactpersoon Informatiebeveiliging (VCIB); doorgeven van IP-adressen en URL's en doorgeven van de in gebruik zijnde hard- en software (de zogenoemde ICT-foto) aan de IBD.

beleid?	informatieveiligheid adequaat te kunnen vervullen.

3 Aanpak

Om de onderzoeksvragen te beantwoorden is gekozen voor een aanpak die de volgende elementen bevat:

- Deskresearch
- Interviews en groepsgesprekken
- Raadsverkenning

De documenten die door de onderzoeker zijn geraadpleegd zijn terug te vinden in bijlage 1.

Deskresearch en interviews

Op basis van de deskresearch zijn itemlijsten opgesteld die input vormden voor gesprekken met de diverse bestuurders en functionarissen op informatieveiligheid en ICT. De lijst met respondenten is opgenomen in bijlage 2. Met de applicatie-beheerders zijn 2 groepsgesprekken gehouden. Bij het gesprek met burgemeester Veerhoek waren de adjunct manager bedrijfsvoering en de ICT-coördinator aanwezig. Deze laatste was ook aanwezig bij het gesprek met gemeentesecretaris Nijhuis-Quanjel.

De deskresearch en de interviews hebben geleid tot de bevindingen zoals deze in hoofdstuk 4 worden weergegeven.

Raadsverkenning

Op 7 februari is een raadsverkenning gehouden waarin een aantal bevindingen op hoofdlijnen zijn gepresenteerd. Voornaamste doel van de raadsverkenning was om het reeds bestaande draagvlak bij de raad voor het onderwerp en het onderzoek te vergroten, en input voor de nota van bevindingen te genereren. Dat laatste met name met betrekking tot de laatste onderzoeksvraag, hoe de gemeenteraad betrokken wenst te worden op het onderwerp informatieveiligheid. Op de raadsverkenning van dinsdag 7 februari waren zeven raadsleden aanwezig.

4 Bevindingen

In dit hoofdstuk worden de onderzoeksvragen per paragraaf beantwoord. Aan het eind van elke paragraaf wordt aangegeven of de gemeente al dan niet (deels) voldoet aan de norm. De daarvoor gebruikte kleuren zijn: groen = de gemeente voldoet aan de norm, oranje = de gemeente voldoet deels aan de norm, rood = de gemeente voldoet niet aan de norm.

4.1 Onderzoeksvraag 1

Hoe heeft het college van B&W de punten van de Resolutie opgepakt? Geldt de BIG als norm voor het basis beveiligingsniveau van de gemeente?

Informatiebeveiligingsbeleid

Het college van B&W heeft het *Informatiebeveiligingsbeleid 2015-2017* op 19 januari 2016 vastgesteld. Dit document bevat het integrale beleid op basis van een risicoanalyse, de zogenoemde GAP-analyse.[6] De toenmalige informatiemanager heeft de GAP-analyse in 2014 in samenwerking met het externe bedrijf SecWatch opgesteld. De daaraan ten grondslag liggende risicoanalyse is in samenwerking met het lijnmanagement opgesteld.

Het college van B&W heeft op 19 januari 2016, bij de vaststelling van het informatiebeveiligingsbeleid, ook besloten het handboek informatiebeveiliging jaarlijks te actualiseren, conform de afspraken in de BIG. De laatste versie dateert van juli 2015. Het handboek is in 2016 niet geactualiseerd. Bij de actualisering van het informatiebeveiligingsbeleid komen we daar op terug (zie §4.2).

Bij de start van de implementatie van de BIG in 2015 is als risico gesignaleerd *"onvoldoende resources, onvoldoende borging door huidige reactieve manier van werken (beperkte mate van vastlegging en procesmatig werken), wegvallen commitment en verantwoordelijkheden door veranderende organisatiestructuur en personeelswisselingen, vertraging door andere prioriteiten."* Een deel daarvan, zoals veranderende organisatiestructuur en personeelswisselingen, heeft waarschijnlijk vertragend effect gehad op de implementatie van de BIG. De huidige CISO is pas sinds eind 2016 aan de slag met de inrichting van het informatiebeveiligingsbeleid en de opzet van de Plan-Do-Check-Act-(PDCA-)cyclus en het Information Security Management System (ISMS). In het kader van deze quick scan hebben we niet kunnen constateren dat een reactieve manier van werken (beperkte mate van vastlegging en procesmatig werken) effect heeft gehad op de implementatie, hoogstens een vertragend effect. De organisatie is momenteel bezig de processen en procedures in het ISMS vast te leggen. Uit de interviews komt het beeld naar voren dat er geen

[6] GAP-analyse laat het verschil ('gap' = Engels voor kloof)) tussen de bestaande situatie en de gewenste situatie.

sprake is van wegvallen van commitment aan de top van de ambtelijke organisatie en bestuur. Er is een budget op de post 'Informatie en Automatisering' in de begroting en er bestaat geen angst voor onvoldoende resources, of:

> *"Er is een budget en wat we merken is, als het om zaken gaat die nodig zijn voor veiligheid, er geen "Nee" volgt. Dan wordt gekeken hoe het vraagstuk zo snel mogelijk is op te lossen."*

• Het college van B&W heeft integraal beleid op informatiebeveiliging, gebaseerd op de BIG, vastgesteld en gepubliceerd.	Voldoet aan de norm
• Het integrale beleid op informatieveiligheid is gebaseerd op een systematische analyse en assessment van de risico's.	Voldoet aan de norm

4.2 Onderzoeksvraag 2

Hoe is het informatiebeveiligingsbeleid vormgegeven in de gemeente? Wie zijn er als verantwoordelijken aangesteld en is er aandacht voor bewustwording?

Informatiebeveiligingsbeleid

De uitgangspunten voor gegevensbeheer staan in het *Informatie-beveiligingsbeleid 2015-2017* aangegeven en het *Informatie-beveiligingshandboek*. Het handboek is niet in 2016 geüpdatet en er is geen integraal privacyprotocol met specifieke richtlijnen van de Wet bescherming persoonsgegevens aangetroffen (zie ook §4.3). Vandaar dat de gemeente nog niet volledig voldoet aan de gestelde norm. De concrete toepassing van de uitgangspunten in een beheers-systeem volgt met de opzet van het ISMS. Dat gebeurt in samenwerking met het externe bedrijf Complions.

De CISO moet, in overleg met lijnmanagement, op basis van een risicoanalyse jaarlijks vaststellen welke risico's er zijn en welke prioriteiten gesteld worden. In het ISMS kunnen taken en planning worden ingebracht en verantwoordelijken worden aangewezen. Met dit traject is de CISO bezig en het is de verwachting dat het ISMS in het tweede kwartaal van 2017 gereed is. Volgens de CISO wordt deze volledig gebaseerd op de BIG en op de GAP- of risicoanalyse.

Verantwoordelijkheden

Het college van B&W is integraal verantwoordelijk voor het Informatiebeveiligingsbeleid. De burgemeester is de portefeuille-houder Informatiebeveiligingsbeleid. De directie stelt jaarlijks het beleid op en het college van B&W toetst het beleid jaarlijks.

In het informatiebeveiligingsbeleid zijn de algemene uitgangspunten voor beheer, gebruik en uitwisseling van (persoons)gegevens beschreven en vastgesteld. Gegevens zijn geclassificeerd op basis van beschikbaarheid (wanneer en hoeveel), integriteit (juistheid, volledigheid en tijdigheid) en vertrouwelijkheid (bevoegdheden en mogelijkheden). De afdelingen zijn verantwoordelijk voor het bewustzijn op beveiliging, bedrijfscontinuïteit en de naleving van de regels en richtlijnen.[7]

[7] Informatiebeveiligingsbeleid 2015-2017, p. 7.

Functies en rollen

In de gemeente is een Chief Information Security Officer (CISO) benoemd. Deze is sinds medio 2016 in dienst en heeft recent het benodigde certificaat behaald. Daarmee voldoet de gemeente Neder-Betuwe aan de norm. De CISO is de ICT-coördinator. Verder zijn er bij ICT de volgende functies ondergebracht, een systeembeheerder en een helpdeskmedewerker.

Tevens zijn er applicatiebeheerders in de verschillende afdelingen, met taken op informatiebeveiliging. Zij zijn onder andere verantwoordelijk voor gebruik, beheer en zelfevaluaties van de applicaties, zoals de Basisadministratie Adressen en Gebouwen (BAG). Zij regelen de toegang tot de gegevens in de applicaties, meldingen van incidenten en de (zelf)evaluaties.

Coördinatoren

Daarnaast vervullen medewerkers rollen op het terrein van de informatiebeveiliging. In het Informatiebeveiligingshandboek zijn functies van informatiebeveiligingscoördinatoren beschreven die binnen afdelingen en processen tactische/operationele taken gedelegeerd krijgen. De onderzoeker heeft gevraagd om deze medewerkers te interviewen, maar deze bleken er niet te zijn. In plaats daarvan zijn applicatiebeheerders gevraagd deel te nemen aan de groepsgesprekken. Zij zijn gevraagd of zij zich herkennen in de rol van informatiebeveiligingscoördinator. Zij gaven aan weinig van doen te hebben met informatieveiligheid. Bij doorvragen bleek dat ze een aantal taken vervullen die in het Informatiebeveiligingshandboek zijn toegeschreven aan de informatiebeveiligingscoördinatoren.[8] De applicatiehouders geven aan onder andere verantwoordelijk te zijn voor de interne assessments en de implementatie van de maatregelen die daar uit voort vloeien. De rollen van de informatie-beveiligingscoördinatoren per afdeling zijn niet expliciet toegewezen, en zullen ook niet worden toegewezen volgens het management en de CISO. De taken zijn impliciet toebedeeld aan de applicatie-beheerders.

Mei 2018

De regels op gegevensbeveiliging worden Europees gelijkgeschakeld. Overheden en bedrijven hebben tot 25 mei 2018 de tijd om richtlijnen aan te passen en functionarissen aan te stellen of rollen toe te wijzen. Momenteel is de gemeente Neder-Betuwe bezig te bezien hoe de functie/rol van Functionaris gegevensbeveiliging, die vanaf mei 2018 verplicht is, in te vullen. De IBD gaat voorzetten doen hoe daarmee om te gaan.

Kennis

Er is volgens de respondenten voldoende kennis in huis om informatiebeveiliging goed te implementeren. De systeembeheerder en de CISO hebben de technische kennis. De top van het management heeft de benodigde kennis. De CISO en de adjunct manager bedrijfsvoering zijn de vertrouwde contactpersonen informatiebeveiliging (VCIB, zie §4.5) en volgen regelmatig de bijeenkomsten van de IBD.

---

[8] Die taken zijn o.a. het coördineren van implementatie van het beleid, ondersteunen van interne en externe assessments en bewaking en onderhoud van geïmplementeerde maatregelen. Zie: Informatiebeveiligingshandboek, vs 2015, p. 22.

De CISO en het lijnmanagement zijn betrokken bij de inventarisatie van de risico's en worden betrokken bij de melding van incidenten. De applicatiebeheerders overzien hun deel van de systemen en zijn verantwoordelijk voor meldingen, de zelfevaluaties en de verbeteracties daarop.

Kennis en expertise

Volgens de BIG is informatieveiligheid een verantwoordelijkheid van het lijnmanagement en de kennis en expertise moeten op dat niveau aanwezig zijn. De gemeente heeft evenwel de keuze gemaakt een deel van hetgeen op ICT benodigd is te 'outsourcen' en een deel zelf in huis te hebben. Volgens de burgemeester is ICT geen kerntaak van de overheid, en bijgevolg hoeft de gemeente niet alle kennis daarop in huis te hebben. Zo huisvest ('host') bijvoorbeeld Pink alle applicaties in de Cloud. Er is volgens de burgemeester alleen basisinfrastructuur in huis nodig, de rest wordt ingekocht. Het lijnmanagement wordt door de CISO betrokken bij de risicoanalyse en het opzetten van het ISMS. Het lijnmanagement zou dan de basiskennis in huis moeten hebben om de risico's op informatie-beveiliging te kunnen inschatten en prioriteiten te stellen. We hebben in het kader van deze quick scan niet onderzocht of dat basisniveau aan kennis en expertise bij het lijnmanagement daadwerkelijk aanwezig is. De basiskennis is, zoals in de ambtelijke reactie is gesteld, aanwezig bij ICT en deze kunnen het lijnmanagement meenemen. Daarmee voldoet de gemeente niet geheel aan de letter en de geest van de BIG, die informatieveiligheid primair een verantwoordelijkheid laat zijn van het lijnmanagement.

Bewustwordingscampagnes

Informatiebeveiliging betreft niet alleen aandacht voor technische maatregelen. Vaak wordt gezegd dat het grootste risico op de stoel voor het computerscherm zit. Volgens de respondenten is er voldoende aandacht voor bewustwording van de risico's op informatiebeveiliging bij de medewerkers. ICT heeft op intranet eigen pagina's, daar worden informatiebeveiligingsbeleid en -handboek, protocollen en meldingen over ontwikkelingen en bedreigingen op ICT voor de medewerkers gepubliceerd.

In 2015 heeft Swinth IvO-Partners bewustwordingsbijeenkomsten voor medewerkers van de gemeente gehouden. Mede naar aanleiding van twee incidenten in 2016 (zie §4.5), is begin 2017 een bewustwordingscampagne gehouden.[9] In april staat in het kader van de bewustwording een serious game van Recourse op de rol. Gemeentesecretaris, CISO, communicatie en een deel van het lijnmanagement gaat in een spelsetting een crisis op informatie-beveiliging simuleren.

De respondenten hebben de indruk dat medewerkers de richtlijnen op informatieveiligheid naleven. Of alle medewerkers de richtlijnen daadwerkelijk naleven is in het kader van deze quick scan niet onderzocht. Hierna volgen staan de bevindingen op naleving door een 'mystery guest'.

[9] Volgens één van de respondenten zou ook de raad daarbij betrokken worden, maar dat is vooralsnog niet het geval.

Afgesproken is dat, medewerkers die met persoonsgegevens in de cloud[10] werken, de computer en het scherm in ieder geval altijd afgesloten moet worden als men deze niet gebruikt. Daarnaast heeft systeembeheer centraal een aantal zaken van te voren ingeregeld op de computers. Zo wordt het systeem na 15 minuten in slaapmodus gezet, en moeten medewerkers opnieuw met een wachtwoord inloggen. Ook is ingesteld dat de wachtwoorden elke anderhalve maand gewijzigd moeten worden. Dat zijn richtlijnen die gebruikelijke zijn en door de IBD aangeraden worden.

Mystery guest

Er is eind 2015 een mystery guest ingehuurd die op afdelingen rondliep en onder andere keek of er onbeheerd privacygevoelige gegevens lagen op bureaus of bij printers. Deze mystery guest heeft één medewerker kunnen vinden die van het bureau wegliep en het computerscherm met gegevens 'open' liet staan. In de interviews wordt aangegeven dat de meeste medewerkers elkaar er op aanspreken. Er wordt bij vermeld dat men er niet constant mee bezig is, maar als men het ziet, wordt zo nodig wordt de collega herinnerd aan de afspraak computers en schermen niet onbeheerd 'open' te laten staan.[11]

• De gemeente heeft uitgangspunten voor beheer, gebruik en uitwisseling van (persoons)gegevens beschreven en vastgesteld.	Voldoet deels aan de norm
• De gemeente heeft een Chief Information Security Officer (CISO) benoemd.	Voldoet aan de norm
• Informatieveiligheid is een verantwoordelijkheid van het lijnmanagement. Kennis en expertise moeten op dat niveau aanwezig zijn.	Voldoet deels aan de norm
• De gemeente schenkt aandacht aan bewustwording bij medewerkers en heeft de organisatie ingericht op constant leren en verbeteren.	Voldoet aan de norm

4.3 Onderzoeksvraag 3

Welke risico's accepteert het college van B&W voor de gemeente en welke niet? Welke politiek-bestuurlijke en maatschappelijke gevolgen kan dit hebben in geval van een incident? Is de privacy van de burgers gegarandeerd?

Risico-inventarisatie

De risico's op informatieveiligheid zijn in 2014 geïnventariseerd en beoordeeld op kwetsbaarheid en dreiging van een incident. Dat is gebeurd op basis van de BIG-richtlijnen en in overleg met de top van het lijnmanagement, ondersteund door het externe bedrijf Complions. Aan de hand daarvan zijn prioriteiten vastgesteld en opgepakt. Deze zijn vastgelegd in het *Informatiebeveiligingsbeleid 2015-2017*.

In het *Plan van Aanpak BIG Gemeente Neder-Betuwe*, begin 2015 opgesteld door Complions naar aanleiding van de risicoanalyse, is aangegeven dat de meeste richtlijnen van de BIG verplicht zijn. Als

[10] In de cloud wordt door Pink Roccade de zogenoemde Makelaar gehost, waar de gemeente veel van de kwetsbare (persoons)gegevens heeft ondergebracht. Medewerkers en externe partijen kunnen, mits geautoriseerd, toegang tot deze gegevens krijgen.

[11] In één van de interviews werd gewag gemaakt van inhuur van een zogenoemde ethisch hacker. Dat hebben we niet kunnen verifiëren in de stukken of in andere interviews.

prioriteit wordt aangehouden om in de eerste fase met ICT processen als leermoment te beginnen, en daarna de primaire processen in het Sociale Domein. Het argument daarvoor is het feit dat hierin met veel privacy gevoelige informatie wordt gewerkt. Deze prioriteitsstelling is met het oog op de bestuurlijke en maatschappelijke gevolgen van mogelijke incidenten genomen.

Informatiebeveiligingshandboek

Volgens het *Informatiebeveiligingsbeleid 2015*-2017 is het de bedoeling dat de risico's jaarlijks worden geïnventariseerd en prioriteiten worden vastgesteld. Deze zouden in het informatie-beveiligingshandboek moeten worden opgenomen. De laatste versie van het handboek is van juli 2015. In 2016 is geen nieuwe versie van het handboek verschenen. Vandaar dat de gemeente op dit punt deels aan de norm voldoet. In de interviews wordt aangegeven dat de CISO momenteel bezig is het Information Security Management Systeem (ISMS), op basis van de Plan-Do-Check-Act-cyclus (PDCA-cyclus) te updaten. Dat proces wordt volgens de CISO in het tweede kwartaal van 2017 afgerond. Doel is deze te koppelen aan de P&C-cyclus, door afdelingen reguliere en periodieke voortgangs-rapportages te laten afleggen.

Richtlijnen privacy

Er worden op verschillende beleidsterreinen privacygevoelige persoons- en andere gegevens bewaard en bewerkt door en/of namens de gemeente. Algemene richtlijnen zijn in het Informatiebeveiligingsbeleid en het handboek vastgelegd. En er staat een algemene verwijzing naar de richtlijnen van de Wet bescherming persoonsgegevens op de website van de gemeente. Specifieke richtlijnen van de Wet bescherming persoonsgegevens zijn niet vastgelegd in één integraal privacyprotocol. Afspraken met derden hoe om te gaan met bewerking en bescherming van persoons-gegevens en hoe te handelen bij datalekken worden in bewerkings-overeenkomsten vastgelegd (zie ook de norm in §4.6).

Voor zover we in het kader van deze Quick scan hebben kunnen constateren voldoet beheer, bewerking van persoonsgegevens door en namens de gemeente Neder Betuwe aan de belangrijkste bepalingen uit de Wet Bescherming persoonsgegevens.

• De gemeente heeft de risico's op informatieveiligheid vastgesteld en geanalyseerd.	Voldoet aan de norm
• In het Informatiebeveiligingsplan is beschreven welke risico's beheerst of geaccepteerd worden, inclusief de bijbehorende maatregelen uit de BIG. Tevens is gemeld op welk niveau het plan is vastgesteld.	Voldoet aan de norm
• De richtlijnen en beleidsregels voldoen aan de belangrijkste bepalingen uit de Wet bescherming persoonsgegevens.[12]	Voldoet aan de norm

[12] De belangrijkste richtlijnen uit de Wbp zijn: Persoonsgegevens mogen alleen in overeenstemming met de wet en op een behoorlijke en zorgvuldige manier worden verwerkt; Persoonsgegevens mogen alleen voor welbepaalde, vooraf uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld. En alleen verder worden verwerkt voor daarmee verenigbare doeleinden; Degene van wie persoonsgegevens worden verwerkt, moet op de hoogte zijn van de identiteit van de organisatie of persoon die de persoonsgegevens verwerkt en van het doel van de gegevensverwerking; De gegevensverwerking moeten op een passende manier worden beveiligd. Voor bijzondere gegevens, zoals over ras, gezondheid en geloofsovertuiging, gelden extra strenge regels.

4.4 Onderzoeksvraag 4

Functioneert de P&C-cyclus van informatieveiligheid binnen de gemeente? Vindt er een jaarlijkse toetsing plaats, om na te gaan of de gemeente 'in control' is op het gebied van informatie-veiligheid via peer reviews, audits of self-assessments? Wat zijn de resultaten van deze toetsing? Wordt de cyclus jaarlijks bijgesteld op basis van lessons learned?

P&C-cyclus

In het *Informatiebeveiligingsbeleid 2015-2017* staat dat de afdelingen verantwoordelijk zijn voor het bewustzijn op beveiliging, bedrijfs-continuïteit en de naleving van de regels en richtlijnen op informatie-beveiliging.[13] Onder andere daarover moet in de P&C-cyclus de managementrapportages aan directie en college van B&W worden gerapporteerd. Aan management en college van B&W wordt onder andere gerapporteerd over de uitslagen op de periodieke zelf-assessments en de externe audits. En er wordt gerapporteerd over de opvolging van de maatregelen naar aanleiding van de assessments en audits. Er is nog geen gestructureerd systeem waarop de informatiecyclus geborgd is. Het ISMS wordt daartoe ontwikkeld (zie § 4.1 en 4.2).

Externe audits

Jaarlijks dienen zelfevaluaties en externe audits uitgevoerd te worden op de applicaties waarmee de gemeente (persoons)gegevens bewerkt en/of laat bewerken. Hieronder geven we aan welke dat zijn geweest in 2016.

Bij applicaties waarmee via DigID met de overheid wordt gecom-municeerd, zoals iBurgerzaken, dient jaarlijks een audit te worden uitgevoerd. De resultaten daarvan moeten aan Logius worden aangereikt. Het is voor het eerst dat de gemeente met iBurgerzaken werkt en de DigID-controle moest laten uitvoeren. Dat is uitgevoerd door Duijnborgh Audit. De andere DigID-audit voor de gemeente Neder-Betuwe worden is door Pink Roccade uitgevoerd.[14] De gemeente krijgt de rapportages van de DigID-audits en controleert zo of de audits zijn gehouden en hoe gescoord wordt. Verder heeft de gemeente er weinig bemoeienis mee. Op de onderzochte criteria is geconstateerd dat de gemeente voldoet.

Over de applicatie SUWInet moet gerapporteerd worden aan het Ministerie van Sociale Zaken en Werkgelegenheid. Voor de Sociale Dienst en het gebruik van SUWInet werkt de gemeente Neder-Betuwe samen met de gemeente Buren. Deze gemeente faciliteert de audit van SUWInet. Het Ministerie toetst en rapporteert via Buren aan Neder-Betuwe. Uit de rapportage blijkt dat de applicatie voldoet aan de gestelde normen.

---

[13] Informatiebeveiligingsbeleid 2015-2017, p. 7.

[14] De audits op Burgerzaken zijn in 2016 uitgevoerd door Pink Roccade en Duijnborgh Audit.

De applicatie voor paspoorten wordt door een door de Rijksoverheid geaccrediteerde auditor gecontroleerd. De CISO geeft aan dat de gemeente daar geen bemoeienis mee heeft.

Zelfevaluaties

De gemeente voert zelfevaluaties uit op de applicaties die te maken hebben met de Basisadministratie Adressen en Gebouwen (BAG), Basisregistratie Personen (BRP) en Reisdocumenten. De zelf-evaluaties worden gedaan op basis van landelijk vastgestelde vragenlijsten. De resultaten worden naar de betreffende rijksdienst opgestuurd.

Naar aanleiding van de resultaten op de vragenlijsten, stellen de applicatiebeheerders indien nodig een actieplan op. Dat wordt besproken in het MT. Daar wordt gemonitord of de acties daadwerkelijk worden ingezet en of het probleem wordt opgelost. Als voorbeeld wordt genoemd de signalering dat met een badge van een medewerker, die al uit dienst was, geprobeerd werd om toegang te krijgen tot de ruimte waar de reisdocumenten worden bewaard. De procedure bij uitdiensttreding werd nagetrokken en het bleek dat deze adequaat werd toegepast maar dat de tenaamstelling van de badge nog niet was gewist. Dit werd alsnog gedaan.

Alle verplichte audits en zelfevaluaties zijn in 2016 uitgevoerd en uit de vragenlijsten blijkt dat de scores voldoende, of voldoende hoog zijn. Op een enkel punt wordt niet maximaal gescoord, maar is de score alsnog voldoende. De CISO geeft aan dat de burgemeester de lat hoog legt en minimaal een 95%-score eist.

IT-audit accountant

De accountant voert jaarlijks bij de interimcontrole in het najaar de IT-audit uit. In de Managementletter waren naar aanleiding hiervan 2 opmerkingen opgenomen over de autorisatie en het wachtwoordenbeleid. Dit beleid voldeed niet aan de richtlijnen van het informatiebeleidsplan en zou te gemakkelijk kunnen leiden tot een hack.

Op het wachtwoordbeleid is meteen actie ondernomen. Over de autorisatie is overleg tussen ICT en de afdeling P&O hoe dit goed te regelen. Daarover zal worden gerapporteerd in de jaarrekening van 2016.

Privacy

Het team control geeft aan een zelfscan te willen uitvoeren op de privacy van gegevens. Dat is naar aanleiding van het bericht in de media dat het slecht gesteld was met de privacy van gegevens bij 40 gemeenten. Minister Plasterk van BZK is daarvoor ter verantwoor-ding geroepen. Dat is de aanleiding van privacy een punt te maken en aandacht te geven.

Incidenten

Hier gaan we in op de procedures rond incidenten op informatie-veiligheid, bij vraag 5 (§4.5) wordt ingegaan op de incidenten. De procedure om incidenten en lekken te melden is beschreven in het *Informatiebeveiligingshandboek*.

"Medewerkers moeten incidenten en afwijkingen melden aan coördinatoren, servicedesk, ACIB of lijnmanagement." [15]

Aan deze procedure wordt in de bewustwordingssessies met medewerkers aandacht besteed. Zie voor het niet aanwezig zijn van informatiebeveiligingscoördinatoren de bevindingen in §4.2.

Via de helpdesk komen meldingen binnen over vraagstukken op het gebied van ICT en informatieveiligheid, van 'niet kunnen inloggen' tot en met 'het programma werkt niet'. De meldingen worden geïndexeerd en doorgezet naar de systeembeheerder. Als een melding meerdere keren voorkomt, dan wordt er een 'problem' geregistreerd. Blijkbaar volstaat een standaardoplossing dan niet meer. Getracht wordt het binnenshuis op te lossen, en desnoods wordt met de leverancier contact opgenomen.

Leercyclus

Er wordt tot nu toe zoveel mogelijk gedaan ad hoc te leren van de ervaringen, incidenten en 'lessons learned'. Via de intranetsite worden deze wel gedeeld. Echter, de opzet van een gestructureerde PDCA-cyclus is volgens planning pas in het tweede kwartaal 2017 gereed.

Rapportage aan 'waarstaatjegemeente.nl'

De gemeente rapporteert niet aan de KING over gemeentelijke indicatoren die gepubliceerd worden op 'waarstaatjegemeente.nl'. Dat geldt dus ook niet voor informatie op het gemeentelijke informatiebeveiligingsbeleid. Het is overigens geen noodzaak in het kader van de BIG. Wel is door de VNG en KING bij de resolutie ten behoeve van het aannemen van de BIG, gesteld dat het wenselijk zou zijn als gemeenten op die site ook over informatiebeveiligingsbeleid zouden rapporteren. Om burgers, en externe partijen te informeren over het gemeentelijk beleid op informatieveiligheid. Uit de ambtelijke reactie blijkt dat de gemeente van plan is vanaf 2017 aan 'waarstaatjegemeente.nl' te gaan rapporteren.

• Over het functioneren van de informatiebeveiliging wordt aan management en bestuur gerapporteerd in het kader van de P&C-cyclus.[16]	Voldoet deels aan de norm
• In de P&C-cyclus wordt gerapporteerd over de periodieke beveiligingsaudits, zoals de zelfevaluaties op de Basisregistratie Personen (BRP) en Reisdocumenten voor IdentiteitsGegevens (RIVG), audits op de Basisregistratie Adressen en Gebouwen (BAG) en SUWINET.	Voldoet aan de norm
• De gemeente rapporteert de jaarlijkse assessments van de DigID-loketten aan Logius.	Voldoet aan de norm
• Ten behoeve van de accountantscontrole wordt jaarlijks een ICT-survey gehouden.	Voldoet aan de norm
• Over het thema digitale veiligheid wordt gerapporteerd aan 'waarstaatjegemeente.nl'.[17]	Voldoet niet aan de norm [18]

[15] Informatiebeveiligingshandboek, juli 2015, p. 24.

[16] In de P&C-cyclus wordt gerapporteerd aan het lijnmanagement. Voor rapportage aan de gemeenteraad in het kader van de P&C-cyclus geeft de BIG geen richtlijnen. Vanwege het bestuurlijke, financiële en publieke belang van informatieveiligheid, en het belang dat raadsleden vaak hechten aan het onderwerp, stellen wij voor reguliere rapportage aan de raad mee te nemen als norm. Zie daarvoor §4.7 en de norm.

• De gemeente heeft een procedure vastgesteld voor de wijze waarop informatiebeveiligingsgebeurtenissen en zwakke plekken worden beheerd en gerapporteerd.	Voldoet aan de norm
• De gemeente leert van de incidenten en heeft de organisatie ingericht op constant leren en verbeteren.	Voldoet aan de norm

4.5 Onderzoeksvraag 5

Zijn binnen de gemeente procedures opgesteld voor incidenten? Welke risico's loopt de gemeente in geval van verstoring of cyberaanval, ook wanneer deze verstoring elders in de keten plaatsvindt? Hoeveel incidenten zijn er in de afgelopen periode (maand/half jaar) geweest? Worden die incidenten bij de IBD (Informatiebeveiligingsdienst) en indien nodig bij de Autoriteit Persoonsgegevens gemeld?

Procedure melding afwijkingen en incidenten

Er is een procedure opgesteld over hoe medewerkers moeten omgaan met afwijkingen en incidenten met betrekking tot het informatiebeveiligingsbeleid. Medewerkers dienen deze volgens het informatiebeveiligingshandboek te melden bij het lijnmanagement, of, zoals het *Informatiebeveiligingsbeleid 2015-2017* aanvult, bij de medewerker informatiebeveiliging. In de praktijk de systeembeheerder, helpdeskmedewerker, de CISO, de adjunct-manager bedrijfsvoering en de gemeentesecretaris, die dit altijd meldt aan de burgemeester.. Als de CISO afwezig is komen de meldingen terecht bij de adjunct bedrijfsvoering. Uiteindelijk krijgt de gemeentesecretaris en de burgemeester de meldingen gerapporteerd.

Deze afspraak tot melding maakt integraal deel uit van de standaardformulering bij de aanstelling van ambtenaren (integriteitsverklaring). De gemeentesecretaris wijst de medewerkers bij de aanstelling op hun verantwoordelijkheid met betrekking tot informatiebeveiliging. Bij externen wordt dat in de overeenkomst van opdracht geregeld. Uit de ambtelijke reactie blijkt dat externen ook een integriteitsverklaring bij de gemeentesecretaris afleggen. Daarin worden ze gewezen op hun verantwoordelijkheid met betrekking tot informatiebeveiliging.

Incidenten, kwetsbaarheden, klachten of afwijkingen worden geregistreerd. De CISO beoordeelt de meldingen en onderneemt indien nodig actie. Als er sprake is van een vermoeden tot een lek met persoonsgegevens moet dat gemeld worden aan de Autoriteit Persoonsgegevens. Voorts wordt aangeraden ook de IBD van incidenten en kwetsbaarheden op de hoogte te stellen. Dat is geen verplichting, maar wordt gewenst om aangesloten gemeenten en andere overheden te waarschuwen voor een mogelijke dreiging.

---

[17] Dit is geen eis binnen de strategische of tactische BIG, maar in de Resolutie van de VNG staat dat gestreefd wordt naar transparantie voor ketenpartners en dat deze onder meer bereikt wordt door gebruik te maken van waarstaatjegemeente.nl.

[18] Omdat dit geen harde norm is, maar als een streven door de VNG is verwerkt in de resolutie waarmee de BIG is aangenomen, is het niet voldoen aan deze norm met een oranje kleur aangegeven in plaats van een rode.

Twee incidenten in 2016

Er zijn 2 incidenten geweest in 2016 waarbij sprake was van een aanval op de informatiebeveiliging van de gemeente. Dat gebeurde beide keren door het openen en aanklikken van een link in een email met 'ransomsoftware' door een medewerker. Ransomsoftware is een kwaadaardig programma dat delen van de informatie in het geïnfecteerde systeem versleuteld en in 'gijzeling' neemt. De gebruiker kan niet meer bij de gegevens, en krijgt na betaling van een vaak forse losgeldsom de sleutelcode om weer bij de informatie te komen.

Bij de eerste aanval duurde het lang voordat het incident gemeld werd, en was ondertussen een deel van de administratie en de uitwisselingsschijf met Pink Roccade geïnfecteerd. De gebruiker die de ransomsoftware activeerde had in eerste instantie niet door dat iets ernstigs gebeurd was. De tweede keer werd het incident sneller gemeld en kon de schade beperkt worden. Met behulp van de Pink Roccade en de eigen inspanningen van systeembeheer heeft de gemeente de schade kunnen indammen. De informatie is met behulp van backups weer hersteld. En er zijn soft- en hardware maatregelen genomen om deze incidenten in de toekomst te voorkomen.[19]

De incidenten zijn niet bij de Autoriteit Persoonsgegevens en niet bij de IBD gemeld.Melding bij de Autoriteit Persoonsgegevens is verplicht bij alleen al een vermoeden tot een datalek. Bij de controle en na overleg bleek geen informatie naar buiten te zijn gegaan. In dat geval is er sprake van een beveiligingslek, en geen datalek, zodat er geen melding bij de Autoriteit Persoonsgegevens noodzakelijk is.

Meldcultuur

De leidinggevenden en bestuurders geven aan dat de aanval met ransomsoftware een menselijke fout was. En dat kan iedereen overkomen. Ze geven aan dat het zaak is ervan te leren. Daarmee lijkt een open meldcultuur nagestreefd te worden. Als deze er niet is, bestaat het risico dat kwaadaardige software langer dan nodig onder de radar blijft en grotere schade aan systeem en opgeslagen gevoelige informatie toebrengt. Bovendien kunnen de boetes die de Autoriteit Persoonsgegevens oplegt pittig zijn als meldingen niet tijdig gedaan worden. Daarvoor wordt naar een open meldcultuur gestreefd, niet om te straffen maar om te leren.

Procedures bij incidenten

De gemeente Neder-Betuwe is aangesloten bij de IBD. Dat is geen eis in de BIG, maar wordt over het algemeen wel aangeraden, onder andere door de VNG. Als de gemeente aangesloten is, levert IBD dienstverlening en krijgen gemeenten bijvoorbeeld meldingen over kwetsbaarheden die elders worden geconstateerd. Voor de aansluiting zijn vier stappen nodig:

- benoeming van twee functionarissen Algemene Contactpersoon Informatiebeveiliging (ACIB)
- benoeming van Vertrouwde Contactpersoon Informatiebeveiliging (VCIB)
- doorgeven van IP-adressen en URL's (webadressen)

[19] Om eventuele kwaadwillenden niet wijzer te maken, gaan we hier niet verder op in.

- doorgeven van de in gebruik zijnde hard- en software

Deze stappen zijn doorlopen en de aansluiting op de IBD is gerealiseerd. De gemeente krijgt incidentmeldingen van de IBD en kan gebruik maken van de dienstverlening van de IBD.

Rollen

Er zijn 2 VCIB-rollen belegd, bij de CISO en de adjunct manager bedrijfsvoering. Tijdens het interview bleek dat een van de algemene contactpersonen (ACIB) niet wist dat hij die rol had. Daarmee is die rol niet als zodanig expliciet belegd. Naar de IBD toe is de rol overigens wel belegd en zijn de ACIB's als zodanig aangemeld. Zij krijgen de informatie en acteren daar ook op.

Bij de risicoanalyse in 2014 is gekeken naar de identificatie van risico's op informatiebeveiliging bij derden die persoonsgegevens van burgers van de gemeente bewerken. Toen werd deels aan de norm op informatieveiligheid voldaan. Momenteel worden in bewerkings-overeenkomsten met derden afspraken over informatieveiligheid gemaakt. De gemeente vraagt Third Party Memoranda (TPM) op om zeker ervan te zijn te dat de externe partij aan de geldende regels en richtlijnen voldoet. Op deze wijze wordt voldaan aan de controle of externe partijen de informatiebeveiliging op orde hebben en zich houden aan de afspraken.

De afspraken zijn nog niet met alle partijen geheel sluitend, zoals de afspraken over datalekken en de financiële risico's daarop. De Autoriteit Persoonsgegevens kan forse boetes opleggen en de gemeente is aansprakelijk bij een datalek van gegevens die namens de gemeente worden beheerd en/of verwerkt. Eventuele boetes zijn niet altijd op de externe partij te verhalen. Met name bij (bijna) monopolisten, zoals Centric en Pink Roccade, is het lastig de risico's in de contracten te adresseren.

De gemeente is niet altijd in staat om contracten en overeenkomsten met derden geheel zelfstandig af te sluiten, zoals bij bovenlokale samenwerkingsverbanden. De last van de controle op een adequate beveiliging van de gegevens ligt daar en de gemeente krijgt daarover gerapporteerd.

Backups en uitwijk

Voor de borging van de continuïteit van de gemeentelijke dienst-verlening zijn een paar zaken van belang. Hoe vaak en hoe lang is het systeem 'down'? En hoe snel kan, in geval van een calamiteit, de gemeentelijke dienstverlening weer hervat worden? De downtime van het gemeentelijk systeem wordt continu gemonitord door Pink Roccade, en deze voldoet aan de normen. Ook de uitwijktest wordt uitgevoerd door Pink Roccade. Daarbij wordt gekeken hoe de procedure verloopt om bij een ernstige verstoring de dienstverlening op te starten, eventueel elders. De uitwijktest in 2016 voldeed aan de gestelde normen.

Overige informatiebeveiligings-aspecten

Losse papieren bij de printers vormen een zeker risico met betrekking tot de informatiebeveiliging. In de interviews is aangegeven dat prints alleen opgehaald kunnen worden bij de printer met behulp van de persoonlijke 'druppel'. Als men met de druppel bij de printer

inlogt en de printopdracht geeft, dan wordt de printopdracht van de server gehaald en naar de betreffende printer gestuurd en afgedrukt. Over het algemeen neemt men dan de prints wel mee.

De website van de gemeente is sinds midden januari 2017 volledig beveiligd. De site was al beveiligd voor het internetverkeer via de beveiligde verbinding 'https://'. Tot medio januari kon de site via een onbeveiligde http://-adressering benaderd worden, maar dat kan niet meer. Het e-mailverkeer is beveiligd. Beide claims, beveiligde internetsite en beveiligd emailverkeer zijn via internet.nl gecheckt en bevestigd.[20]

BYOD

Alle apparaten waarmee medewerkers en externen in het gemeentelijk systeem inloggen worden gecheckt op virussen en 'malware'. De medewerkers kunnen daarna direct in het systeem werken en hebben rechtstreeks toegang tot de benodigde gegevens. De gegevens kunnen gedownload worden, op kantoor van de gemeente en thuis. Voor externen die toegang willen hebben tot gegevens, wordt een zogenoemde virtuele omgeving gecreëerd waarin ze met de benodigde gegevens kunnen werken. De informatie blijft bij de gemeente en kan niet ontvreemd worden.

Raadsinformatiesysteem

Het raadsinformatiesysteem, het cloudgebaseerde Notubizz, is afgeschermd van de rest van de systemen binnen de gemeente. De griffie bereidt de vergaderstukken voor de gemeenteraad voor en laadt deze in Notubizz in, waardoor deze voor de raadsleden toegankelijk zijn. Vanwege die scheiding kunnen geen lekken plaatsvinden tussen het gemeentelijk gegevenssysteem en het raadsinformatiesysteem.

• Op basis van een risicobeoordeling is een continuïteitsplan met betrekking tot informatiebeveiliging opgesteld. Met daarin de essentiële procedures voor continuïteit, zoals veilig stellen, herstel en reconstructie van informatie.	Voldoet aan de norm
• Risico's op informatieveiligheid die betrekking hebben op externe partijen zijn expliciet meegenomen in de integrale risicoanalyse.	Voldoet aan de norm
• De gemeente is aangesloten bij de IBD. De gemeente meldt incidenten op informatieveiligheid aan de IBD, en krijgt meldingen terug.	Voldoet deels aan de norm
• Datalekken worden aan de Autoriteit Persoonsgegevens gemeld.	Voldoet aan de norm

4.6 Onderzoeksvraag 6

Is er per domein zicht op het netwerk van landelijke en regionale partners waarin de gemeente opereert? Is er zicht op de informatiehuishouding en de informatie-uitwisseling in dit netwerk van actoren? Is er zicht op de borging van informatieveiligheid in de praktijk bij deze actoren? Worden er (contractuele) afspraken over

[20] Iedereen kan op www.internet.nl checken of de website van een domeinnaam beveiligd is tegen omleiding naar een vals IP-adres met behulp van DNSSEC-beveiliging. Tevens kan iedereen checken of de website beveiligd is via een TLS-verbinding.
Daar kan ook de check uitgevoerd worden op beveiliging van een e-mail adres via DNSSEC, DKIM, DPF, DMARC en TLS.

informatieveiligheid gemaakt bij het opzetten van (regionale) samenwerkingsverbanden en bij de inkoop van diensten?

In het *Informatiebeveiligingshandboek* versie 2015 is een overzicht opgenomen van interactie inzake informatiedeling met derden. Er is op de verschillende domeinen, en de verschillende applicaties binnen die domeinen, zicht op de partners (landelijk en regionaal) waar de gemeente gegevens mee uitwisselt. Voor elke bewerker van informatie worden bewerkingsovereenkomst gesloten, zo blijkt uit de interviews.

Makelaar

Veel van de gemeentelijke gegevens worden gekoppeld via de zogenoemde GegevensMakelaar. Dat is een cloudgebaseerde applicatie van Pink Roccade waar de gemeente op aangesloten is. Het aantal medewerkers van de gemeente dat toegang heeft tot de Makelaar is beperkt. Andere partijen waar de gemeente de informatie mee deelt, moeten daar ook op aangesloten worden. Externe partijen moeten daarvoor een zogenoemd Public Key Infrastructure-certificaat (PKI-certificaat) aanvragen. Daarmee wordt verzenden en ontvangen van gegevens digitaal ondertekend en beveiligd. Zij krijgen rechten toegewezen voor toegang tot specifieke set van gegevens, en er wordt bijgehouden wie welke informatie opvraagt.

Van de partijen, waarmee de gemeente samenwerkt en informatie deelt, wordt een TPM gevraagd om aan te tonen dat de externe partij voldoet aan de richtlijnen op het gebied van informatieveiligheid. Zie ook de bevindingen in §4.5.

Sociaal domein

Voor de Sociale Dienst werkt de gemeente Neder-Betuwe samen met de gemeente Buren. Daarover zijn al opmerkingen gemaakt bij de bevindingen in §4.4.

De informatiestroom en -beveiliging met betrekking tot Wmo en Jeugdzorg wordt voor 10 gemeenten gezamenlijk geregeld in de Regio Rivierenland. De medewerkers op het sociaal domein zitten in de overleggen van deze Gemeenschappelijke regeling (GR). Het regionale inkoopbureau is nauw betrokken bij de contractvorming en heeft volgens de gemeentesecretaris vol aandacht voor de het aspect informatiebeveiliging.

In regionaal verband wordt het verantwoordings- en controleproces met betrekking tot de zorgverlening vanaf 2016 gecoördineerd. Er worden accountantsverklaringen en prestatieoverzichten uitgewisseld, en uiteraard ook cliëntgegevens. Elke gemeente krijgt alleen de rekeningen en gegevens van de eigen cliënten. Dat verkeer verloopt sinds kort via een beveiligde verbinding, via de server van Rivierenland. Aangekondigd wordt dat de gegevens er zijn en dan zijn ze slechts beperkte tijd te downloaden.

Uit een van de interviews blijkt dat niet alle zorgaanbieders even alert en veilig met de informatie via de mail omgaan. Het berichtenverkeer van de regio naar de gemeente verloopt in ieder geval via een beveiligde verbinding.

Risicoanalyse en P&C-cyclus

In de risicoanalyse van 2014 is aandacht geschonken aan de risico's op informatiebeveiliging met betrekking tot derde partijen. En dat zal meegenomen worden in de huidige risicoanalyse. De P&C-cyclus, op basis van het ISMS is nog niet op orde (zie ook §4.1 en §4.2). Op de norm van het aspect informatiebeveiliging in overeenkomsten met derde partijen voldoet de gemeente Neder-Betuwe, zie ook §4.3.

• Risico's op informatieveiligheid die betrekking hebben op externe partijen zijn expliciet meegenomen in de integrale risicoanalyse, en daar wordt jaarlijks over gerapporteerd in de P&C-cyclus.	Voldoet deels aan de norm
• Het aspect informatiebeveiliging wordt behandeld in overeenkomsten met derde partijen.	Voldoet aan de norm

4.7 Onderzoeksvraag 7

Op welke wijze is de gemeenteraad betrokken bij het informatieveiligheidsbeleid?

Bedrijfsvoering

De raad heeft uiteraard het budgetrecht op het gemeentelijk beleid vanwege de kaderstellende rol. De burgemeester is van mening dat informatiebeveiliging bedrijfsvoering is en de verantwoordelijkheid daarvoor ligt niet bij de gemeenteraad. Hij is er beducht voor dat de raad teveel wordt meegezogen in de bedrijfsvoering. De raad mag ervan uitgaan dat het goed gaat en krijgt gerapporteerd als dat niet het geval zou zijn. College van B&W en gemeentesecretaris informeren de raad elk jaar over bedrijfsvoering in de het jaarverslag en elk half jaar in de bestuursrapportages (berap). Tevens geeft de burgemeester aan dat informatieveiligheid vooral met mensen, gedrag en cultuur te maken heeft. Daarop moet volgens de burgemeester de gemeente blijven investeren. En hij geeft aan dat het lastig is op dat mens- en cultuuraspect de raad te informeren.

Het klopt dat de raad over bedrijfsvoering wordt gerapporteerd in de jaarstukken. In de jaarrekening, de versie voor de raad, wordt in de paragraaf bedrijfsvoering niet ingegaan op informatieveiligheid. Noch in de andere paragrafen gerelateerd aan de term 'veiligheid'. In de jaarrekening wordt veiligheid vooral geassocieerd met fysieke veiligheid. De bestuursrapportages hebben we niet ingezien, maar te veronderstellen is dat de aard van de rapportage op bedrijfsvoering en in het bijzonder informatiebeveiliging niet zal afwijken van de jaarrapportage. Wel krijgt de raad de opmerkingen van de accountant in de managementletter over ICT, en de activiteiten die naar aanleiding daarvan zijn genomen.

Raadsverkenning

Het beeld dat de raad nauwelijks is aangesloten op het onderwerp informatiebeveiliging wordt bevestigd in de raadsverkenning die op 7 februari is gehouden.

Drie van de zeven aanwezige raadsleden geven aan zich in het algemeen zorgen te maken over informatiebeveiliging. Zij gaven aan via het budgetrecht betrokken te zijn op het onderwerp en alleen op incidenten geïnformeerd te zijn geworden. Daarbij werd opgemerkt

dat zij van slechts één van de twee incidenten op de hoogte zijn gebracht.

Gevraagd naar hoe en wanneer zij geïnformeerd willen worden, geven de aanwezige raadsleden aan dat zij in de P&C-cyclus over informatiebeveiliging alleen jaarlijks op hoofdlijnen of prioriteiten geïnformeerd wensen te worden. Informatiebeveiliging valt onder bedrijfsvoering en zij hebben er vertrouwen in dat de uitvoering van informatiebeveiliging in de ambtelijke organisatie en bestuur voldoende aandacht krijgt en op orde is.

De raadsleden geven ook aan op incidenten snel geïnformeerd te willen worden. Raadsleden huiveren bij het idee dat een voorval, op de beveiliging van gegevens die de gemeente beheert of namens de gemeente worden beheerd, in de pers of op sociale media wordt uitgemeten terwijl zij niet op de hoogte zijn gebracht. Dat moet in hun ogen stante pede gebeuren. Naast het beperken van het incident, wil de raad zo snel mogelijk geïnformeerd worden over aard en omvang van hetgeen is voorgevallen en de maatregelen die genomen worden om verdere schade te voorkomen.

• De gemeenteraad is gepositioneerd om zijn kaderstellende en controlerende taak met betrekking tot informatieveiligheid adequaat te kunnen vervullen.	Voldoet deels aan de norm

5 Reactie van College van B&W

gemeente
Neder-Betuwe

Bezoekadres:
Burgemeester Lodderstraat 20, Opheusden
Postadres:
Postbus 20, 4043 ZG Opheusden

Telefoon: 14 0488
Telefax: (0488) 44 99 99

E-mail: info@nederbetuwe.nl
Website: www.nederbetuwe.nl
BNG IBAN:
NL83 BNGH 0285094955
KvK: 30276311
BTW: NL810162593B01

Aan de rekenkamercommissie

uw brief van: 8 maart 2017
uw kenmerk:
ons kenmerk: Z/17/046773/UIT/17/74518
behandeld door: de heer Waterman
bijlage(n):

Onderwerp: Zienswijze rekenkameronderzoek Quick Scan Informatiebeveiligingsbeleid

Opheusden, 28 maart 2017

Geachte commissie,

U hebt ons in de gelegenheid gesteld om onze zienswijze te geven over het concept-rapport Quick Scan Informatiebeveiligingsbeleid. Graag maken wij van deze gelegenheid gebruik.

Allereerst merken wij op dat wij met u het grote belang onderkennen van bewustwording en kennis van informatiebeveiliging. Het gebruik van digitale informatie met persoonlijke en gevoelige data neemt toe maar daarmee ook de kwetsbaarheid. Het verrichtte onderzoek is dan ook actueel en geeft ons handvatten om verder op de ingeslagen weg voort te gaan naar verbetering van de veiligheid en vergroting van de bewustwording bij alle betrokkenen.

Wij kunnen ons in grote lijnen vinden in dit rapport. Het geeft naar onze mening een goed beeld van waar we op dit moment staan en waar op onderdelen intensivering van de aanpak nodig is. Wij vinden, zoals ook in het rapport is verwoord, dat het bij dit thema vooral gaat om een bedrijfsvoeringaangelegenheid. Echter met een zodanig karakter dat inbreuk op de beveiliging grote gevolgen kan hebben voor de privacy van burgers en onze dienstverlening en daarom politiek en bestuurlijk relevant.

Met betrekking tot de uitkomst van het onderzoek merken wij op dat bij sommige onderdelen uw oordeel is dat wij gedeeltelijk aan de gestelde norm voldoen. Wij hechten er aan hierbij aan te geven dat het daarbij gaat om normen die door u zijn gesteld, aanvullend op de normen van de BIG (Baseline Informatiebeveiliging Gemeenten).
We doelen daarbij specifiek op:
Tabel pag. 14: Het vastleggen van uitgangspunten voor beheer, gebruik en uitwisseling van (persoons)gegevens; Deze informatie zullen wij actualiseren;
Tabel pag. 18: Rapportage via de P&C cyclus aan de raad: De BIG geeft hiervoor geen richtlijnen. Wij zullen na afstemming met de raad rapporteren via de P&C cyclus;
Tabel pag. 18: De rapportage aan 'waarstaatjegemeente.nl' Dit is geen eis van de BIG maar een aanbeveling van de VNG die wij overigens gaan opvolgen;

Tabel pag. 22: De aansluiting van de gemeente bij de IBD (Informatiebeveiligingsdienst gemeenten); Dit is geen eis in de BIG maar een keuze die wij zelf hebben gemaakt. Het nog niet melden van incidenten aan de IBD dat daaruit voortvloeit, zal in voorkomende gevallen plaatsvinden.
De hoofdlijn is dat wij wel voldoen aan de normen van de BIG.

Wij beperking onze reactie verder tot de genoemde aansporingen voor het college en aanbevelingen aan de gemeenteraad.

Aansporingen voor het college
Wij kunnen hier kort over zijn. Wij geven hieraan gevolg. Een deel van de maatregelen waren al in uitvoering, de andere genoemde punten zoals het definiëren van kennis en expertise in het handboek en het expliciet beleggen van rollen, taken en functies nemen wij over. Een maatregel om te voldoen aan de nieuwe regels op het gebied van gegevensbeveiliging voor mei 2018 is de aanstelling van een functionaris gegevensbescherming. Wij zullen daarbij ook nagaan of samenwerking met een of meer buurgemeenten mogelijk is.

Aanbevelingen voor de raad
Graag willen wij met de raad afstemmen over de wijze waarop wij in de informatiebehoefte op passende wijze kunnen voorzien.
Wellicht dat over het hoe en wanneer bij de behandeling van dit rapport door de raad al opvattingen worden gedeeld. Wij zullen de raad in elk geval direct informeren over incidenten met een bestuurlijke, financiële of maatschappelijke impact. Bij de tweede bestuursrapportage zullen wij de raad informeren over de opvolging van de aangegeven verbeterpunten uit het rapport.

Tot slot.
We begonnen onze zienswijze met het aangeven van het grote belang van kennis en bewustwording van alle betrokkenen op het gebied van informatieveiligheid. Voortdurende waakzaamheid is daarbij geboden. Het door u uitgebrachte rapport, dat wij intern de nodige aandacht zullen geven, draagt daar zeker aan bij.

Met vriendelijke groet,

Burgemeester en wethouders van Neder-Betuwe,

de secretaris a.i., de burgemeester,

drs. M.G.J. Nijhuis-Quanjel ir. C.W. Veerhoek

6 Nawoord Rekenkamercommissie

De rekenkamercommissie kan in dit rapport met het nawoord zeer kort zijn. Wij zijn het college van burgemeester en wethouders zeer erkentelijk voor hun positieve reactie.

Een extra inspiratie om ons voor te bereiden op een volgend onderzoek en waarover wij nog voor het zomerreces met de gemeenteraad in overleg willen gaan.

De voorkeur van de rekenkamercommissie gaat uit naar het onderwerp `De drie transities`, waarbij het dan noodzakelijk is om samen met de raadsfracties een afbakening te bepalen en de te onderzoeken items helder voor ogen te krijgen.

Bijlage 1. Literatuurlijst

- Visio-Netwerk Tekening Neder-Betuwe 2013
- Applicatielanbdschap gemeente Neder-Betuwe
- Afdelingsplan bedrijfsvoering 2016
- Informatiebeveiligingsbeleid 2015-2017 gemeente Neder-Betuwe
- Informatiebeveiligingshandboek_Gemeente_NederBetuwe 1.0, juli 2015
- Bewustwording Neder-Betuwe 20150928 (presentatie door Swinth)
- Gouden Tips (behorend bij de Safe & Sound campagne van de IBD)
- Help, wat is er aan de hand? Bewustwording van de gevaren van het Internet. (presentatie Neder-Betuwe)
- Korte beschrijving en factsheet CIP Crisis game, 161121 (uitgevoerd door Recourse)
- Jaarstukken 2015, Gemeente Neder-Betuwe
- Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten, KING/VNG, juni 2016.
- GAP-analyse Gemeente Neder-Betuwe (uitgevoerd door SecWatch)
- Project initiation document Implementatie BIG (zonder datum)
- Plan van aanpak BIG. Gemeenten Neder-Betuwe 20150105 (opgesteld door CompLions, Deventer)
- Plan van aanpak Bijlage CompLions BIG Roadmap 2014
- Plan van aanpak Bijlage BIG_Norm verantwoordelijkheid matrix v1 0
- Applicatielijst 20161010
- Stand van zaken: controlepunten Accountant en AO, 20160531. (email)
- -Handreiking-CISO-functieprofiel-1.0.1, 20160803
- Bevestiging van uw registratie. Deelname Tichelaar aan Netwerkbijeenkomsten Functionaris Gegevensbescherming van VNG. 15 december zj.
- Functionaris gegevens bescherming (FG), 20161122
- Goedkeuring zelfevaluatie SUWINET Neder-Betuwe, 20151201
- Verbeterplan zelfevaluatie BRP en reisdocumenten 2015
- Vragenlijst BRP, 201611xx
- RapportageuitwijkenreconstructieNeder-Betuwe, 20160923
- Rapportage uitwijk en reconstructietest en draaiboek, 20160923
- Reconstructietes, 20160923. (printscreens)
- Uitwijktest, 20160923. (printscreens)
- Vragenlijst Reisdocumenten, november 16
- Vragenlijst_ZEPNIK_2016
- Rapport TPM 2016 DigiD PRLG inzake iBurgerzaken, 20161020
- DBA- GEM NEB DigiD iBurgerzaken LOGIUS, 20161026

Bijlage 2. Overzicht respondenten

Groepsgesprekken met applicatiebeheerders

- Annelies Peperkamp (Makelaar en civision waarderen)
- Arie van den Herik (civision middelen)
- Els Bulten (iBurgerzaken en DigID)
- Janine Bruijstens (Aeolus)
- Jannie van Blitterswijk (civision innen)
- Martijn de Vree (systeem- en netwerkbeheerder)
- Ria van Hattem (BAG)
- Roel Schroot (Decos)
- Ton Meijering (website)
- Yvonne van der Maeden (kadaster en BGT)

Gesprekken

- Mariet Nijhuis-Quanjel (gemeentesecretaris en hoofd P&O)
- Hans Smit (adjunct manager bedrijfsvoering)
- Gerrit Tichelaaar (CISO en ICT coördinator)
- Burgemeester C. Veerhoek (portefeuillehouder)
- Bert Waterman (concerncontroller)

Bijlage 3. Verklaring van gebruikte termen

ACIB	Algemeen Contactpersoon Informatiebeveiliging
BAG	Basisregistratie Adressen en Gebouwen
Berap	Bestuursrapportage, 2 x per jaar
BIG	Baseline Informatiebeveiliging Gemeenten
BRP	Basisregistratie Personen
BYOD	Bring your own device, betekent dat medewerkers en externen hun eigen apparaten (laptops, smartphons, usb-sticks enz.) meenemen en inloggen in het gemeentelijk systeem.
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.
GAP	Is de Engelse term voor ‘kloof’. Dat betekent hier het verschil tussen de bestaande situatie en de gewenste situatie.
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
P&C-cyclus	Planning & Control cyclus
PDCA	Plan-Do-Check-Act beleidscyclus
PKI-certificaat	Public Key Infrastructure. Een PKI(overheid)-certificaat is een internationale standaard voor de digitale ondertekening bij het versturen van gegevens en berichten.
RIVG	Rijksdienst voor Identiteitsgegevens
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