Quick Scan - Informatiebeveiliging gemeente Zoetermeer

In opdracht van de Rekenkamercommissie Zoetermeer

Utrecht, 03-12-2017

Drs. E.J.M. Lemmens, Prae Advies & Onderzoek

Inhoud

1 Samenvatting, conclusies en aanbevelingen

Met deze Quick Scan heeft de Rekenkamercommissie Zoetermeer een onderzoek uitgevoerd naar informatiebeveiliging. 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 rekenkamers. 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.

Achtergrond van het onderzoek

In 2013 hebben gemeenten zich verplicht te werken aan verbetering van de digitale veiligheid. Gemeenten hebben daarom de Baseline Informatiebeveiliging Gemeenten (hierna: BIG) opgesteld. Zij werden daarbij ondersteund door VNG en het Rijk. De BIG formuleert op strategisch en tactisch niveau eisen waaraan informatiebeveiliging bij gemeenten minimaal moet voldoen. De Rekenkamercommissie Zoetermeer heeft elf vragen over informatiebeveiliging geformuleerd. Deze vragen zijn onder andere gebaseerd op een vragenlijst van de rekenkamer van de gemeente Den Haag en de Taskforce Bestuur & Informatieveiligheid Dienstverlening (Taskforce BID) en gaan in op belangrijke aspecten van de BIG, zie hoofdstuk 3. Op die manier wil de rekenkamercommissie een beeld krijgen van de manier waarop het beleid rond informatieveiligheid op papier in de organisatie van de gemeente Zoetermeer is ingevoerd. De vragen gaan niet in op de operationele situatie van de ICT bij de gemeente Zoetermeer, maar op het tactische en strategische niveau van de BIG.

2 Inleiding

Informatieveiligheid is binnen gemeenten verscherpt op het netvlies gekomen na crises van enige jaren geleden. Zoals die in het nieuws kwamen bij DigiNotar en door Lektober.[1] Maar ook recenter het toenemend aantal meldingen van datalekken en virusaanvallen, zoals met ransomware 'Wannacry', in 2017. Deze hebben aangetoond dat onder andere gemeenten op digitaal gebied kwetsbaar zijn. Wat gebeurt er bijvoorbeeld als gevoelige informatie op straat komt te liggen? Of als de 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.

Op de Buitengewone Algemene Ledenvergadering van de VNG op 29 november 2013 hebben de aangesloten gemeenten in de Resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' besloten de Baseline Informatiebeveiliging Gemeenten (BIG) als basisnorm te nemen voor hun beleid op informatieveiligheid. Deze baseline is opgesteld door Rijk en gemeenten. Hierin zijn maatregelen opgenomen die gemeenten kunnen nemen om de veiligheid van de door de gemeente

[1] DigiNotar verzorgde elektronische handtekeningen en certificaten voor een groot deel van de overheid, zoals die van DigID. In juli 2011 ontdekte DigiNotar dat deze een maand eerder gehackt was en kwam daarmee pas eind augustus mee naar buiten. Uit onderzoek bleek dat DigiNotar fouten in de procedures en systemen had gemaakt. Dit leidde ertoe dat alle overheidscertificaten onveilig waren. In oktober 2011 bleek dat de websites van vijftig gemeenten en gemeentelijke diensten open stonden vanwege een verouderde Windows-versie. Daardoor konden kwaadwillenden informatie ophalen en bestanden aanpassen of wissen. Ook kon men door het lek DigID's misbruiken en namens een inwoner handelingen uitvoeren bij een van de vijftig 'lekke' gemeenten. Oktober 2011 werd daardoor Lektober genoemd.

beheerde informatie te verbeteren en te garanderen. Gemeenten hebben zich met deze resolutie een 'verplichte zelfregulering' opgelegd. Gemeenten zijn dus zelf aan zet.

De Rekenkamercommissie Zoetermeer heeft – gezien de risico's en het maatschappelijke en financiële belang van het onderwerp voor gemeenten – besloten informatieveiligheid in de gemeente Zoetermeer aan een onderzoek te onderwerpen. Met deze Quick Scan wil de rekenkamer-commissie inzicht geven in de stand van zaken rond de invoering van de BIG in de gemeente Zoetermeer. Het is een momentopname, omdat het beleidsterrein nog volop in ontwikkeling is. Prae Advies & onderzoek heeft het onderzoek voor de Rekenkamercommissie Zoetermeer uitgevoerd.

Leeswijzer

De aanpak voor deze Quick Scan schetsen we in hoofdstuk 3. In dat hoofdstuk zijn de elf onderzoeksvragen opgenomen. Deze vragen gaan in op de belangrijkste aspecten van gemeentelijk informatieveiligheidsbeleid. In hoofdstuk 4 worden de onderzoeksvragen beantwoord. De conclusies uit de bevindingen en de aanbevelingen naar aanleiding van de conclusies, ter verdere verbetering van het informatieveiligheidsbeleid in de gemeente Zoetermeer, zijn weergegeven in hoofdstuk 1 'Samenvatting, conclusies en aanbevelingen', aan dit hoofdstuk voorafgaand.

De voor dit onderzoek bestudeerde stukken en geïnterviewde personen zijn opgenomen in bijlage 1. Informatiebeveiliging is een terrein waarin veel afkortingen en (Engelse) termen worden gebruikt. Niet iedereen is daarin thuis, vandaar dat in bijlage 2 een verklarende woordenlijst en afkortingen is opgenomen.

3 Aanpak

De Rekenkamercommissie Zoetermeer heeft zich voor dit onderzoek deels gebaseerd op een notitie van de rekenkamer van de gemeente Den Haag en de Taskforce Bestuur & Informatieveiligheid Dienstverlening (Taskforce BID).[2] De vragen uit de notitie gaan in op de belangrijkste aspecten van de BIG. Deze vragen zijn aangevuld en aangepast aan de situatie van Zoetermeer.

Dit onderzoek is een Quick Scan en richt zich op de implementatie van de tactische en strategische maatregelen van de BIG. De vragen in deze Quick Scan gaan vooral in op de beleidsmatige aspecten van informatieveiligheid in de gemeente Zoetermeer. De vragen gaan niet in op de operationele aspecten van ICT. Operationele aspecten kunnen risico's op informatieveiligheid inhouden, maar deze vallen buiten de reikwijdte van deze Quick Scan.

Op 21 juli heeft mevr. S. Paulusma, de coördinator informatiebeveiliging [3], van de gemeente Zoetermeer ter informatie de startnotitie voor het onderzoek ontvangen. In de startnotitie zijn elf vragen opgenomen over informatieveiligheid en de uitvoering van de BIG-maatregelen.

De elf vragen zijn:

---

[2] Zie Notitie Opties rekenkameronderzoek Informatieveiligheid, rekenkamer Den Haag & Taskforce Bestuur & Informatieveiligheid Dienstverlening, 2014. (http://www.rekenkamerdenhaag.nl/rekenkamer/to/Workshop-digitale-veiligheid.htm)

[3] Doel van deze functie is het, op basis van de algemeen aanvaarde standaard BIG, zorgdragen voor een samenhangend pakket van maatregelen ter waarborging van de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie binnen een gemeente.

1. Stuurt de gemeente op de afspraken die benoemd zijn in de Resolutie ‘Informatieveiligheid, randvoorwaarde voor de professionele gemeente’ en in het bijzonder op de implementatie van de BIG en zo ja hoe?
2. Heeft de gemeente de risico’s op informatieveiligheidsvlak in een Informatiebeveiligingsplan benoemd, is helder in hoeverre risico’s beheerst dan wel geaccepteerd worden, inclusief de bijbehorende maatregelen uit de BIG, en op welk niveau is dit plan vastgesteld (ambtelijke organisatie, college, raad)?
3. Rapporteert en bespreekt de organisatie het functioneren van de cyclus van informatieveiligheid op management- en bestuursniveau (college en raad)? Is zij daarover transparant richting haar ketenpartners door via waarstaatjegemeente.nl te rapporteren over informatieveiligheid? Zijn er nog andere wijzen van rapporteren?
4. Is de continuïteit van de gemeentelijke dienstverlening gewaarborgd in geval van grootschalige uitval of verstoring van ICT en hoe is dat geregeld?
5. Kent de gemeente de leveranciers en partners waarmee ze samenwerkt en toetst zij die ook op informatieveiligheidsaspecten en zo ja hoe?
6. Is de gemeente ‘officieel’ aangesloten bij de Informatiebeveiligingsdienst voor gemeenten (IBD) en wat is de exacte status van deze aansluiting?
7. Weet de organisatie hoe te handelen bij een (ernstig) informatieveiligheidsincident en is er een incidentenmanagementproces ingevoerd? Hoe ziet dit eruit?
8. Wordt jaarlijks getoetst of de organisatie in control is op het gebied van informatieveiligheid via peer reviews, audits of zelfassessments? En wordt over het functioneren van de cyclus van informatieveiligheid gerapporteerd aan de raad?
9. Zijn de beleidsuitgangspunten nog valide of zijn er interne of externe ontwikkelingen die leiden tot heroverwegingen van de gemeentelijke risico-inschattingen? Indien dit laatste het geval is, wat zijn dan deze ontwikkelingen?
10. Is er een integrale aanpak voor organisatieleren op het gebied van informatieveiligheid? Hoe houdt de gemeente kennis vast en bouwt zij hierop door?
11. Hoe ver is de gemeente gevorderd met de voorbereidingen op implementatie van de Algemene verordening gegevensbescherming (AVG) van de EU?

De onderzoeker is gestart met deskresearch, bestudering van stukken over het informatie-beveiligingsbeleid van de gemeente. Welke stukken bestudeerd zijn, is in bijlage 1 weergegeven. De informatie hieruit vormde de input voor de interviews met wethouders en ambtenaren over de implementatie van de BIG. De respondenten die geïnterviewd zijn, zijn eveneens in bijlage 1 opgenomen.

4 Vraag en antwoord

Hieronder wordt in elf paragrafen ingegaan op de gestelde vragen en antwoorden. Waar nodig worden conclusies getrokken. Onder elke vraag is in cursieve letters de norm weergegeven, wat in de BIG op dat punt is afgesproken.

4.1 Stuurt de organisatie op de afspraken die benoemd zijn in de Resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' en in het bijzonder op de implementatie van de BIG en zo ja hoe?

Norm: 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 beleid is risico gebaseerd en een verantwoordelijkheid van het lijnmanagement. Deze stelt op basis van een analyse en assessments de risico's vast.[4]

Het integrale beleid is december 2014 door het college vastgesteld in het Informatiebeveiligings-beleid 2015-2017. Deze is gebaseerd op de maatregelen uit de BIG. Aan het beleid ligt de in 2014 door de gemeente zelf uitgevoerde GAP-analyse ten grondslag. Een Gap-analyse is een methode om een vergelijking tussen de bestaande en de gewenste situatie. Zo krijgt de organisatie inzicht in de te nemen maatregelen om de gewenste situatie te bereiken, namelijk voldoen aan de BIG-normen.

Op basis van het beleid is in 2015 en 2016 een informatiebeveiligingsplan door de directie vastgesteld. Eind 2016 is een nieuwe GAP-analyse uitgevoerd met behulp van een extern bureau, dat begin 2017 resulteerde in een vernieuwde risicoanalyse. Op basis daarvan is begin 2017 een memo vastgesteld met 6 prioriteiten voor 2017(zie ook §4.2.) De mening van de bij de GAP-analyse betrokken ambtenaren is dat de analyse van 2016 strenger is uitgevoerd en relevante informatie en beleidsinput heeft opgeleverd. Vooralsnog wordt geen nieuwe versie van het informatiebeveiligingsbeleid opgesteld dat gebaseerd is op de in 2016 opgestelde GAP-analyse (zie ook §4.9).

De gemeente Zoetermeer heeft als visie de komende jaren informatieveiligheid te verhogen en te professionaliseren. "Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van de gemeente en de basis voor het beschermen van rechten van burgers en bedrijven. Dat vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn" (in: Beleid werken met mobiele apparaten, 9-2-2017.)

Het huidige informatiebeveiligingsbeleid is risico-gebaseerd, met betrokkenheid vanuit directie en de afdeling I&A. Het middenmanagement is, volgens de meeste respondenten, slechts matig betrokken bij het vaststellen van de risico's op informatieveiligheid. Behalve bij de afdelingen met een hoog risicoprofiel op werken met privacygevoelige gegevens. Dat zijn met name de afdelingen Publieksplein en Werk, zorg en inkomen. Voor de overige afdelingen is dit nog een ontwikkelpunt.

De respondenten zijn van mening dat de governance goed geregeld is. In het verslag van de visitatie-commissie informatiebeveiliging van de VNG van maart 2017 is te lezen dat de commissie dezelfde

[4] Zie Tactische BIG, items 5 en 6, resp. Informatiebeveiligingsbeleid en Interne organisatie.

mening is toegedaan. Volgens de meeste respondenten kan het onderwerp informatiebeveiliging op groot draagvlak bij het college rekenen. Informatiebeveiliging is belegd bij wethouder Paalvast, die een affiniteit heeft met het onderwerp. Functioneel worden vraagstukken op dit terrein behandeld in de coördinatiegroep informatiebeveiliging. Daarin zijn de functionarissen op dit onderwerp vertegenwoordigd, met name uit de afdeling I&A. Afstemming met de andere beleidsterreinen vindt plaats in het Informatie Management Overleg (IMO). De linking pin tussen IMO en de directie is de directeur Bedrijfsvoering, die tegelijk ook de chief information security officer (CISO) is. Deels wordt de functie van CISO door de coördinator informatiebeveiliging ingevuld.

De vraag is of dit een adequate functieverdeling is. Van de ene kant is het gegeven dat de CISO-functie op directieniveau is belegd een signaal voor draagvlak voor het onderwerp informatie-beveiliging binnen de top van de organisatie. Van de andere kant heeft de CISO een van de lijn onafhankelijke taak met betrekking tot informatiebeveiliging. Beide functionarissen geven aan dat zij nooit problemen hebben ervaren en geven stellig aan dat zij geen problemen verwachten. Hier bestaat een risico op ineffectiviteit. Bij conflicterende belangen tussen de lijn en informatiebeveiliging is er een risico dat benodigde maatregelen om informatiebeveiliging te borgen niet, onvoldoende of te laat genomen worden.

Op beleidsterreinen, zoals privacy of zorg, werk en inkomen, kunnen gemakkelijk vraagstukken bovenkomen waarin informatieveiligheid een rol speelt. Mogelijke conflicten tussen beleidsterreinen worden in de bovengenoemde gremia, coördinatiegroep en IMO, besproken. Indien daar geen oplossing wordt gevonden, wordt geëscaleerd naar de betrokken wethouders en uiteindelijk het college. Volgens de wethouders liggen op dat vlak geen onduidelijkheden, daar de landelijke richtlijnen, zoals de BIG, worden gevolgd.

Het budget voor beleid op informatiebeveiliging is jaarlijks € 230.000. Volgens de betrokkenen ambtenaren is dat voldoende en krijgen ze geen 'nee' als antwoord op verzoek om noodzakelijke investeringen. De gemeenteraad is akkoord gegaan met de laatste aanvraag op informatie-beveiliging, na een enkele vraag over de duurzaamheid van de investering.

4.2 Heeft de gemeente de risico's op informatieveiligheidsvlak in een Informatiebeveiligingsplan benoemd, is helder in hoeverre risico's beheerst dan wel geaccepteerd worden, inclusief de bijbehorende maatregelen uit de BIG, en op welk niveau is dit plan vastgesteld (ambtelijke organisatie, college, raad)?

Norm: Zie voor wat in de BIG is afgesproken de norm in de vorige paragraaf, §4.1.

De GAP-analyse geeft weer in hoeverre de gemeente op streek is met de implementatie van maatregelen uit de BIG. Op basis van deze analyse maakt de gemeente een analyse van de risico's die de gemeente loopt. Gemeente Zoetermeer heeft de risico's op informatie en de applicaties die daarmee omgaan geïnventariseerd aan de hand van de zogenoemde BIV-criteria. Hiermee wordt getoetst in welke mate de informatie Beschikbaar is of moet zijn, de Integriteit en de Vertrouwelijkheid van de informatie. Voor de risicoanalyse van 2017 is ook imago meegewogen, dat wil zeggen in welke mate de gemeente politiek-bestuurlijk-maatschappelijke risico's loopt.

Daarmee heeft de gemeente de risico's op informatieveiligheid in beeld. Volgens het Informatiebeveiligingsbeleid 2015-2017 moet elk jaar een plan worden opgesteld met de prioriteiten

voor dat jaar. Voor 2017 is op basis van de risicoanalyse een lijst met zes prioriteiten opgesteld. Reden daarvoor is dat de risicoanalyse op basis van de GAP pas begin 2017 opgesteld is.

Informatiebeveiliging is een terrein dat turbulent in ontwikkeling is en zal blijven. Volgens de wethouder is 100% veiligheid op informatie niet te garanderen. Beveiligers en kwaadwillenden zijn in een race met elkaar verwikkeld, waardoor het nooit voor lange tijd te garanderen is dat een organisatie 'in control' is. Op de risico's die de gemeente redelijkerwijs kan kennen moet men voorbereid zijn, volgens de wethouder. Daartoe dienen de GAP- en risicoanalyse en de jaarplannen. ICT is volgens de respondenten technisch op orde. Belangrijk is de awareness onder de medewerkers, daar ligt volgens de wethouder en andere respondenten de grootste uitdaging (zie ook §4.10).

Op onderdelen wordt, naar aanleiding van de GAP-analyse of de risicoanalyse, beleid ontwikkeld. Als voorbeeld noemen we mobiele datadragers, zoals USB-sticks, en het plaats onafhankelijk werken (POW). De afdeling I&A heeft de poorten in hardware voor USB-sticks afgesloten. Gebruik van dit soort mobiele datadragers, en de mogelijke virussen en onbetrouwbare applicaties die daarop aanwezig kunnen zijn, brengt teveel risico's met zich mee. Men kan een aanvraag doen om alsnog met een USB-stick te kunnen werken. Dan gaat de coördinator informatiebeveiliging het gesprek aan waarbij getracht wordt begrip voor het beleid over te dragen en naar andere oplossingen te zoeken.

In principe is iedere medewerker geautoriseerd plaatsonafhankelijk te werken. Alleen een beperkte mag elders met privacygevoelige gegevens werken. Deze medewerkers kunnen in principe dezelfde systeem- en computeromgeving krijgen als op het werk. Echter is In sommige applicaties de printmogelijkheid uitgezet, zodat er extern geen hard copies van informatie op de laptop gemaakt kunnen worden. Er kan via 4G een beveiligde vpn-verbinding gemaakt worden. Echter, voor het thuis of elders werken met privacygevoelige informatie moet alsnog van tevoren specifieke afspraken met betrekking tot beveiliging worden gemaakt. De teammanager zou het gesprek met de medewerker daarover moeten kunnen aangaan. De coördinator informatiebeveiliging constateert dat de teammanagers daar nog niet de juiste handvatten voor hebben. Over het algemeen gaat de coördinator het gesprek aan.

4.3 Rapporteert en bespreekt de organisatie het functioneren van de cyclus van informatieveiligheid op management- en bestuursniveau (college en raad)? Is zij daarover transparant richting haar ketenpartners door via waarstaatjegemeente.nl te rapporteren over informatieveiligheid? Zijn er nog andere wijzen van rapporteren?

Norm: 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.[5] In de BIG zelf staat niets over rapporteren aan waarstaatjegemeente.nl over het thema informatieveiligheid. In de Resolutie van de VNG staat dat gestreefd wordt naar transparantie en dat deze onder meer bereikt wordt door gebruik te maken van waarstaatjegemeente.nl.

Uit de GAP-analyse van 2016 kwam naar voren dat er in de gemeente geen gestructureerd of geautomatiseerd managementrapportagesysteem op informatiebeveiliging aanwezig is. Op papier zijn er rapportageprotocollen, maar er is geen managementsysteem, zoals een Information Security Management System (ISMS). Dat is een geautomatiseerde tool waarmee rapportages met de spreekwoordelijke 'druk op de knop' gegenereerd kunnen worden en activiteiten in de leercyclus (PDCA-cyclus) gevolgd kunnen worden. Op basis van de risicoanalyse heeft het management voor andere prioriteiten gekozen dan de aanschaf of ontwikkeling van een ISMS in 2017. Door het ontbreken van een ISMS loopt de gemeente een risico op inefficiëntie. De rapportageprotocollen zijn volgens de CISO aanwezig, dus er is geen risico op ineffectiviteit. Maar het kost momenteel enige moeite om de rapportages in het kader van de P&C-cyclus te vullen. De gemeente is voornemens in 2018 een ISMS te implementeren.

Op dit vlak ligt een link met de in 2018 in te voeren Eenduidige Normatiek Single Information Audit (ENSIA). Hierin worden de aparte vragenlijsten of audits over verschillende applicaties gebundeld, onder andere vanwege de efficiëntie en vermindering van de verantwoordingslasten. Het zijn evaluaties die de gemeente zelf uitvoert, op basis van centraal opgestelde vragenlijsten over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigID), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWInet). Deze vragenlijsten worden vanaf 2018 samengevoegd in ENSIA, ten behoeve van de verticale verantwoording richting Rijk, en de horizontale verantwoording richting gemeenteraad. In het kader van ENSIA krijgt de raad vanaf 2018 gerapporteerd over de applicaties die in de gemeente draaien. In de stukken ter voorbereiding op de implementatie en uitvoering van ENSIA wordt de CISO voorgesteld als coördinator.

De gemeenteraad wordt via de paragraaf in de programmabegroting en de jaarrekening een keer per jaar geïnformeerd over informatiebeveiliging, samen met privacy. Over privacy krijgt de raad drie tot vier keer een memo. Er wordt geen tussentijdse informatie over incidentmeldingen naar de raad gezonden. De raad krijgt in het kader van de passieve informatieplicht wel vragen beantwoord over informatiebeveiliging. Er komen over dit onderwerp, volgens de respondenten, weinig vragen vanuit de raad. Wel als er in de media wordt gerapporteerd over incidenten zoals met de 'Wannacry'-ransomware of problemen rond SUWInet. De indruk bij de meeste respondenten is dat privacy als onderwerp bij raadsleden meer leeft dan informatiebeveiliging. In het informatiebeveiligingsbeleid is

[5] Zie Tactische BIG, item 6.1.8, Beoordeling van het informatiebeveiligingsbeleid.

college én gemeenteraad de bevoegdheid toegekend om een controle op de uitvoering uit te voeren. De raad heeft daar geen enkele keer gebruik van gemaakt. De wethouder is van mening dat informatiebeveiliging een zaak voor bedrijfsvoering is en dat de raad ervan mag uitgaan dat dit door het college en apparaat adequaat wordt uitgevoerd.

In de resolutie, aangenomen door de VNG, staat de aanbeveling aan gemeenten omwille van de transparantie over informatiebeveiliging te rapporteren op waarstaatjegemeente.nl. De gemeente Zoetermeer heeft dat twee jaar geleden reeds een keer gedaan. Het voornemen is om deze rapportages weer op te pakken. De coördinator informatiebeveiliging is contactpersoon daarvoor en gaat de mogelijkheden daartoe onderzoeken.

4.4 Is de continuïteit van de gemeentelijke dienstverlening gewaarborgd in geval van grootschalige uitval of verstoring van ICT en hoe is dat geregeld?

Norm: 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.[6]

De score op continuïteit in de GAP-analyse van 2016 is als mager aan te duiden. Naar aanleiding daarvan is continuïteit als een van de prioriteiten voor 2017 opgenomen. Voor de applicaties die geaudit worden is de continuïteit geborgd In 2016 en 2017 zijn diverse maatregelen genomen om de continuïteit te borgen, maar een ‘overall’ continuïteitsplan is niet opgesteld.

In 2016 is een nieuwe infrastructuur op ICT aanbesteed, met informatiebeveiliging als onderwerp. Daarbij is gekozen voor een verzwaring van de veiligheidseisen, onder andere door middel van het zogenoemde zero-trust concept. Voorheen vertrouwde een organisatie intern alles, en alles wat van buiten kwam moest worden gecheckt met scanners en firewalls. In het zero-trust-concept wordt ook het interne verkeer gecheckt. Daarvoor worden tussen applicaties en organisatieonderdelen firewalls opgezet. Zoetermeer is in 2016 begonnen met compartimenten inrichten rond vijf applicaties. Daar komen in 2017 meer compartimenten bij. Op die manier wordt voorkomen dat, wanneer een applicatie of mailverkeer binnen een afdeling besmet is met een virus, dit makkelijk kan overslaan naar een andere applicatie of afdeling.

Raadsleden hebben ook toegang tot gegevens op het gemeentelijk netwerk, zoals intranet en de applicaties waarvoor zij geautoriseerd zijn. Het mailverkeer voor raadsleden loopt via de eigen mailomgeving, via Xs4all. Daarnaast delen raadsleden vergaderstukken via Ibabs. In de planning is opgenomen dat in 2018 alle bestuurlijke stukken via Ibabs verspreid gaan worden.

De controle op de firewalls is grotendeels extern bij een gespecialiseerd bedrijf ondergebracht. Deze kan 24/7 monitoren en snel acteren op incidenten. Voor een gemeentelijke organisatie is dat lastiger te organiseren.

Met het oog op de continuïteit van de primaire processen zijn er twee interne datacenters ingericht, over twee gebouwen verdeeld. Deze worden direct met elkaar gesynchroniseerd. Als er een uitvalt kan relatief snel data van de ene naar de andere server worden overgezet. Tijdens de verhuizing is de

[6] Zie Tactische BIG, item 14, Bedrijfscontinuïteitsbeheer.

uitwijk een keer onvrijwillig getest, omdat de stroom uitviel. Verder is het systeem tijdens de verhuizing ook onder gecontroleerde omstandigheden stopgezet en opnieuw opgestart. Het systeem bleek snel weer 'up and running' te zijn zodat mensen meteen weer aan de slag konden. Back-ups worden dagelijks gemaakt en ondergebracht bij een externe partij.

4.5 Kent de gemeente de leveranciers en partners waarmee ze samenwerkt en toetst zij die ook op informatieveiligheidsaspecten en zo ja hoe?

Norm: 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.[7]

De gemeente verwerkt veel privacygevoelige gegevens van burgers, en vanwege de decentralisaties in het sociaal domein in toenemende mate van groepen kwetsbare burgers. Het is evident essentieel dat burgers en bedrijven/instellingen weten dat de gemeente prudent deze gegevens verwerkt of laat verwerken. In risicoanalyse en beleid is opgenomen dat de gemeente Zoetermeer niet het risico wil lopen op lekken door derden die voor de gemeente gegevens verwerken. Dat leidt tot meer veiligheidseisen aan leveranciers.

Informatieveiligheid wordt geadresseerd in een aparte paragraaf in contracten en verwerkers-overeenkomsten met derden. Volgens een van de respondenten is 'privacy' een onderdeel van de toolkit die medewerkers gebruiken bij aanbesteding en inkoop. De contracten zelf horen thuis bij de vakafdelingen en worden uiteindelijk steekproefsgewijs gecheckt door de accountant. De privacyfunctionaris kijkt aan de voorkant van het inkooptraject mee. De afdeling I&A kijkt ook mee voor het technische deel van de afspraken en het gebruik en ontwerp van de applicaties. De gemeente heeft volgens een van de respondenten in 2015 daar onderzoek naar gedaan en de raad in een memo over geïnformeerd.

Op het sociaal domein werkt de gemeente samen met veel éénpitters. Zij hebben niet altijd 'state of the art'-middelen om informatie te beveiligen. Dat maakt de adequate en veilige verwerking van de gegevens kwetsbaar. Maar ook bij een grote partij is dat niet vanzelfsprekend goed geregeld. Zo heeft de gemeente recent bij een gegevenskoppeling er een punt van gemaakt dat een applicatie van een gerenommeerde partij alle data onversleuteld over een onbeveiligde lijn zou versturen. Dat kan als je een stevige marktpartij bent, zoals de gemeente Zoetermeer. De marktpositie wordt uiteraard steviger als gemeenten samenwerken, zoals op inkoop van zorg in de regio Den Haag.

Respondenten signaleren dat leveranciers niet het risico van boetes van de Autoriteit Persoonsgegevens (AP) willen lopen. Boetes op datalekken door de AP uitgereikt kunnen tot een fors bedrag oplopen. Met name bij evident nalatig gedrag of niet adequaat reageren op een geconstateerd datalek. Derde partijen proberen eventuele boetes in het contract uit te sluiten of via een omweg alsnog te verhalen op de gemeente. Respondenten zien langzamerhand dat leveranciers via dialoog met opdrachtgevers naar oplossingen zoeken die door beide partijen wordt gedragen.

---

[7] Zie Tactische BIG, item 6.2, Externe Partijen.

Essentieel is dat het bewustzijn dat informatieveiligheid belangrijk is, aanwezig is bij de gemeentelijke afdeling die inhoudelijk over het domein gaat. Respondenten geven aan dat de monitoring op naleving van de contracten beter kan. Momenteel wordt vooral geacteerd op individuele meldingen van medewerkers. Het sociaal domein is een veld in ontwikkeling en niet alle aanbieders zijn aangesloten. Volgens een van de respondenten moet de gemeente zijn regierol hierin pakken en streven naar een gemeentebrede oplossing.

Specifiek wordt de informatiebeveiliging van data op bedrijfsvoering die extern wordt gehost wel getest. Dat zijn data van de afdelingen Belastingen en HRM. Deze systemen worden gecontroleerd en meegenomen in de penetratietesten (pentesten) die uitgevoerd worden. Bij HRM bleek in 2017 zich een incident te hebben voorgedaan en wellicht een lek, waarbij de afdeling HRM in eerste instantie dacht dat het mee zou vallen. Afdeling I&A stond erop dat het lek onderzocht zou worden, want het oordeel dat het meevalt kan slechts na onderzoek geconstateerd worden. Het bleek een beveiligingsincident te zijn, waarop geacteerd is, en vooralsnog geen datalek.

4.6 Is de gemeente 'officieel' aangesloten bij de Informatiebeveiligingsdienst voor gemeenten (IBD) en wat is de exacte status van deze aansluiting?

Norm: Aansluiting op de IBD is niet geregeld in de BIG zelf. De algemene en vertrouwde contactpersonen informatiebeveiliging (Algemene Contactpersoon Informatiebeveiliging [ACIB] en Vertrouwde Contactpersoon Informatiebeveiliging [VCIB]) van de gemeente kunnen aangesloten zijn bij de IBD. Dat is belangrijk, omdat de IBD meldingen van beveiligings-incidenten verzamelt en doorgeeft aan deze contactpersonen. En de IBD waarschuwt voor bedreigingen, zoals lekken in software.

De IBD krijgt meldingen van mogelijke dreigingen binnen, en zet deze door naar de gemeenten die aangesloten zijn. Indien nodig kunnen deze daarop actie ondernemen. Dat kunnen algemene meldingen zijn, zoals virusaanvallen, of meldingen van vertrouwelijke aard, zoals potentiële datalekken. Voor de aansluiting bij de IBD moeten vier stappen gerealiseerd zijn:

1-2. benoeming van twee functionarissen (ACIB en VCIB)
3. doorgeven van in gebruik zijnde IP-adressen[8] en URL's[9] aan IBD
4. doorgeven van bij de gemeente in gebruik zijnde hard- en software (de zogenoemde ICT-foto).

Aansluiting op de IBD is overigens geen maatregel in de BIG. Aansluiting is wel aangeraden in de resolutie die de gemeenten hebben aangenomen. Over het algemeen zijn de respondenten die met de IBD van doen hebben overtuigd van de zin van de meldingen van en ondersteuning door deze instantie.

De gemeente heeft twee algemene en twee vertrouwde contactpersonen voor de IBD benoemd. Het zijn dezelfde personen. Tevens is er en één algemene en één vertrouwde contactpersoon benoemd

[8] IP-adres (Internet Protocol): Elke computer die is aangesloten op het internet of een netwerk heeft een nummer (IP-adres) waarmee deze zichtbaar is voor alle andere computers op het internet. Men kan dit vergelijken met telefoonnummers.

[9] Url (Uniform Resource Locator): verwijst naar het unieke adres waarmee de locatie van een webpagina op internet wordt aangegeven of een e-mailadres.

als back-up. Vakanties worden onderling afgestemd, zodat steeds minimaal één van de contactpersonen aanwezig is en kan optreden. De meldingen van de IBD voor de contactpersonen komen bij de gemeente binnen. Als het een ernstige en voor de gemeente Zoetermeer risicovolle melding betreft, wordt de melding doorgeleid naar de CISO en de wethouder.

Stap 3 van de aansluiting, namelijk de bij de gemeente in gebruik zijnde IP-adressen en URL's doorgeven aan de IBD, is gezet. Stap 4 van de aansluiting, het aanleveren van de foto van de soft- en hardware, is nog niet gezet. Daarmee krijgt de gemeente geen kwetsbaarheidsmeldingen van de IBD die toegesneden is op de specifiek bij de gemeente in gebruik zijnde soft- en hardware. Gevraagd naar de reden waarom die stap niet is gezet, antwoorden respondenten dat zij schromen de blauwdruk van de gehele ICT-infrastructuur bij een externe partij neer te leggen. Volgens opgave van de IBD heeft, op moment van rapportage, 68% van de gemeenten alle 4 stappen van de aansluiting gezet. Uit de ambtelijke hoor en wederhoor blijkt dat de gemeente voornemens is deze stap ook te zetten.

4.7 Weet de organisatie hoe te handelen bij een (ernstig) informatieveiligheidsincident en is er een incidentenmanagementproces ingevoerd? Hoe ziet dit eruit?

Norm: In de BIG is opgenomen dat er een procedure wordt vastgesteld voor de wijze waarop informatiebeveiligingsgebeurtenissen en zwakke plekken in de beveiliging worden beheerd en gerapporteerd. Ook geeft de BIG aan dat er geleerd moet worden van de incidenten.[10]

De gemeente beschikt over een servicedesk/meldpunt bij de afdeling Facilitair waar meldingen van incidenten binnenkomen. Dat kan gaan over het opnieuw aanvragen van een wachtwoord tot de melding van een beveiligingsincident. De coördinator informatiebeveiliging heeft sinds kort twee keer per maand overleg, met de coördinator van de servicedesk en de security specialist van de afdeling I&A, om afspraken te maken welke meldingen geëscaleerd moeten worden en welke niet urgent zijn. Een geautomatiseerde incidententool om daar op te acteren is nog niet aanwezig. Dat kan een licht risico op ineffectiviteit inhouden.

Naar aanleiding van de evaluatie van incidenten in 2016 is beleid opgestart om tot een Computer Emergency Response Team (CERT) te komen. Deze is bedoeld voor incidenten en noodgevallen. Dit crisisbeheersingsbeleid is nog in ontwikkeling. de teammanager Automatisering, de securityspecialist van de afdeling I&A en de coördinator informatiebeveiliging in de rol van CISO maken deel uit van het CERT. In crisissituaties kunnen de betrokken ambtenaren snel met elkaar schakelen. Er is getest door een case voor te leggen en dan na te gaan hoe men moest reageren, zoals bijvoorbeeld bij een aanval met het 'Wannacry'-virus.

Op informatiegebied is In 2016 twee keer een aanval geweest met ransomware. Daar heeft de organisatie redelijk goed op kunnen reageren, met behulp van goede back-up voorzieningen kon de schade beperkt blijven. Dat is een reactieve respons en de snelheid van ingrijpen bepaalt de mate van verlies aan data/informatie. De afdeling I&A implementeert een applicatie die vooraf checkt of applicaties bekend en te vertrouwen zijn en die niet bekende applicaties direct blokkeert. De medewerkers van I&A vinden dit in combinatie met andere maatregelen een goede proactieve oplossing.

[10] Zie Tactische BIG, item 13, Beheer van informatiebeveiligingsincidenten.

Op privacy zijn in 2017 16 incidenten geweest, waarvan de helft is gemeld bij de AP. Het is de regel dat een incident, waarbij vermoed wordt dat er sprake is van een datalek, gemeld wordt bij de AP. Omdat vaak niet van tevoren duidelijk is dat er daadwerkelijk een lek is, in de zin dat privacygevoelige gegevens kwijt zijn geraakt. Een groot incident bleek, na analyse met de leverancier die het datalek meldde, achteraf geen lek te zijn. De leverancier heeft de benodigde actie ondernomen. En bij de gemeente heeft het geleid tot aanscherping van de regels op autorisaties en de-autorisaties. Na ieder incident wordt geëvalueerd wat verbeterd kan worden.

De autorisaties op de applicaties worden door de managers van de vakafdelingen bijgehouden. Deze controleert eens per half jaar of de toegangsrechten nog juist zijn. Dat gebeurt door te checken of de medewerker nog in dienst is bij de gemeente, of hij/zij de laatste drie maanden heeft ingelogd en of zich risicovolle activiteiten op dat account plaatsvinden. Bij de afdeling P&O worden de in- en uitdiensttredingen bijgehouden. Is iemand in dienst gekomen, dan volgt een registratie in BREM, waarna de vakafdeling de benodigde autorisaties kan afgeven. Bij een uitdiensttreding wordt de registratie verwijderd en bijgevolg de autorisaties opgeheven. Er is bij sommige respondenten een lichte twijfel of tussentijdse wijzigingen in autorisaties altijd goed geregistreerd worden. Bijvoorbeeld als men van functie verandert. Er is nog geen overall autorisatiebeleid op gemeentelijk niveau aanwezig, met een registratie wie welke rol heeft en tot welke gegevens de medewerker mag geraken. Daar moet nog beleid op ontwikkeld worden. Tijdens de ambtelijke hoor en wederhoor bleek dat het autorisatiebeleid in ontwikkeling is en in het eerste kwartaal van 2018 wordt opgeleverd. De bedoeling is dat de functioneel beheerders de controles op autorisaties gaan uitvoeren.

4.8 Wordt jaarlijks getoetst of de organisatie in control is op het gebied van informatieveiligheid via peer reviews, audits of self assessments (zelf tests)? En wordt over het functioneren van de cyclus van informatieveiligheid gerapporteerd aan de raad?

Norm: 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. [11] *Voor rapportage aan gemeenteraden geeft de BIG geen richtlijnen.*

De gemeente voldoet aan de vereisten inzake de jaarlijkse audits en zelfcontroles op de applicaties. Dat zijn de applicaties die de privacygevoelige gegevens van burgers en bedrijven/instellingen verwerken. Zoals de BRP, PUN, DigID, BAG, BGT en SUWInet, die binnenkort door middel van de single audit van de ENSIA zullen worden gebundeld tot één vragenlijst. De eventuele verbeteracties die uit de audits en zelfevaluaties naar voren komen, worden door de vakafdelingen opgepakt. Voorts voert de accountant een ICT audit uit, die in het accountantsverslag wordt opgenomen. Zoals hiervoor reeds geconstateerd is, is er nog geen ISMS om deze en andere acties te monitoren of over te rapporteren in de P&C-cyclus.

[11] Zie Tactische BIG, item 6.1.8, Beoordeling van informatiebeveiligingsbeleid; 15.2, Naleving van beveiligingsbeleid en –normen en technische naleving.

De gemeenteraad krijgt niet gerapporteerd over de controles op informatiebeveiliging die de organisatie uitvoert, behalve de ICT audit van de accountant. In de BIG is alleen afgesproken dat de raad één keer per jaar in het kader van de P&C-cyclus over informatiebeveiliging wordt geïnformeerd, bij verslag over bedrijfsvoering in de jaarstukken. De gemeenteraad van Zoetermeer wordt in de programmabegroting en in de jaarrekening geïnformeerd over dit onderwerp. Op intranet wordt gemiddeld tweewekelijks een bericht over informatiebeveiliging geplaatst, dat raadsleden ook kunnen bekijken. Volgens een aantal respondenten is dat voldoende, omdat de vrees bestaat dat de discussie over dit complexe onderwerp niet goed met de raad gevoerd kan worden. Volgens het Informatiebeveiligingsbeleid 2015-2017 kan college en/of raad om controles van het beleid vragen. Dat is tot nu toe niet gebeurd, omdat het onderwerp, volgens een aantal respondenten, niet erg leeft. Op basis van het geringe aantal vragen luidt de constatering dat de raad niet erg geïnteresseerd is in het onderwerp en erop vertrouwt dat het college informatiebeveiliging in het kader van de bedrijfsvoering adequaat oppakt. Raadsleden zouden hoogstens naar aanleiding van incidenten elders reageren.

4.9 Zijn de beleidsuitgangspunten nog valide of zijn er interne of externe ontwikkelingen die leiden tot heroverwegingen van de gemeentelijke risico-inschattingen? Indien dit laatste het geval is, wat zijn dan deze ontwikkelingen?

Norm: In de BIG hebben gemeenten afgesproken dat het informatiebeveiligingsbeleid eens in de drie jaar, of zodra zich belangrijke wijzigingen voordoen, wordt geëvalueerd.[12]

De wereld van ICT en beveiliging is continu en turbulent in beweging. De digitale bedreigingen nemen toe en systemen blijken kwetsbaar. Vandaar de eis in de BIG om het beleid voor maximaal drie jaar vast te leggen en te evalueren. Het informatiebeveiligingsbeleid 2015-2017 van Zoetermeer is conform de BIG voor drie jaar opgezet en loopt eind 2017 ten einde. Er is nog geen geheel nieuw beleid geformuleerd, en de verwachting is dat het beleid 2015-2017 met een check op mogelijke aanpassingen wordt gecontinueerd. Reden die daarvoor wordt aangegeven is dat de BIG binnenkort aangepast zou worden.

De BIG is reeds in 2016 op een aantal punten aangepast en er zijn geen aanwijzingen voor verdere aanpassingen op korte termijn. Wel gaan de Baseline Informatiebeveiliging Rijksoverheid (BIR) en de BIG samen op in de Baseline Informatiebeveiliging Overheid (BIO). Dat zal op zijn snelst in twee tot drie jaar gerealiseerd kunnen worden. Vooralsnog geldt de BIG als uitgangspunt voor informatie-beveiliging bij gemeenten.

Voor Zoetermeer ligt het voor de hand om op basis van de GAP-analyse het Informatiebeveiligings-beleid 2015-2017 te evalueren en een beredeneerde afweging te maken het beleid al dan niet aan te passen. Teneinde aan de hand daarvan een jaarplan informatiebeveiliging met de prioriteiten voor 2018 op te stellen.

[12] Zie Tactische BIG, item 5.1.2, Beoordeling van het informatiebeveiligingsbeleid.

4.10 Is er een integrale aanpak voor organisatieleren op het gebied van informatieveiligheid? Hoe houdt de gemeente kennis vast en bouwt zij hierop door?

Norm: In de BIG is afgesproken om te leren van beveiligingsmeldingen met als doel beheersmaatregelen te verbeteren.[13] *Als randvoorwaarde is in de BIG onder andere geformuleerd dat informatieveiligheid een verantwoordelijkheid is van het lijnmanagement en dat kennis en expertise essentieel zijn.*[14]

Zoals eerder gemeld is er geen ISMS aanwezig en is deze niet gekoppeld aan de leercyclus (PDCA). In die zin is er geen integrale of gestructureerde aanpak van organisatieleren op informatiebeveiliging. Dat wil niet zeggen dat er niet geëvalueerd wordt of geleerd wordt van ervaringen.

Respondenten geven aan dat de mens de zwakste schakel in de beveiligingsketen is. Men kan technisch de zaken nog zo goed voor elkaar hebben, "het grootste risico zit tussen scherm en de bureaustoel." Medewerkers zijn zich niet van nature bewust van de risico's, volgens een van de respondenten. Awareness bij de medewerkers wordt als een belangrijk issue gezien. De eerste volledige campagne om risicobewustzijn op informatiebeveiliging te vergroten is in 2016 van start gegaan. Deze is gericht op kennis, houding en gedrag van alle medewerkers gemeente Zoetermeer.

De activiteiten in 2016 waren gericht op de individuele medewerkers, waarbij getracht is aan te haken bij hetgeen men privé meemaakt of wat men in de pers over informatiebeveiliging en bedreigingen kan lezen. Zo zijn medewerkers bijvoorbeeld benaderd met nep spam en phishing mail. De boodschap daarbij is dat iedereen een fout kan maken en op een verkeerde mail of link kan klikken. Daar kan van geleerd worden, met name dat men het meteen meldt bij de leidinggevende, het meldpunt of de coördinator informatiebeveiliging. Om de meldingsbereidheid te stimuleren zijn in 2017 medewerkers die snel een melding deden in het zonnetje gezet met een bloemetje, uitgereikt door de directeur.

De awareness activiteiten in 2017 zijn gericht op de teams. Teneinde de teammanagers mee te krijgen en de medewerkers onderling in gesprek te laten gaan. In het beleid is opgenomen dat de teammanagers jaarlijks gesprekken houden over informatiebeveiliging en risicobewustzijn. De coördinator informatiebeveiliging ondersteunt en adviseert hierbij. Ook gaat de coördinator naar het teamoverleg als zich een incident heeft voorgedaan. Daarnaast wordt getracht het kennisniveau te verhogen door vraagstukken op informatiebeveiliging in spelvorm te behandelen. Volgens een van de respondenten is de achterliggende bedoeling informatiebeveiliging continu bespreekbaar te maken. En om informatiebeveiliging als gesprekselement op te laten nemen in aannameprocedures, teamoverleggen en beoordelingscyclus.

Regelmatig worden diverse testen worden uitgevoerd om te kijken in hoeverre vreemden of kwaadwillenden kunnen binnendringen in de organisatie en in de systemen. Dat zijn de zogenoemde penetratietesten, kortweg pentesten genoemd. Zo hebben studenten van de Haagse Hogeschool, vestiging Zoetermeer, een mystery guest-opdracht uitgevoerd. Zij controleerden hoe ver een

---

[13] Zie Tactische BIG, item 13.2.2, Leren van informatiebeveiligingsincidenten.
[14] Zie Tactische BIG, 1.3, Randvoorwaarden.

vreemde binnen kan komen en bij informatie kan komen. Het versturen van spam en phishing mails en het inhuren van zogenoemde 'ethische hackers' hoort hier ook bij.

Voorts heeft de afdeling I&A een eigen intranetpagina, waarop de nieuwtjes en waarschuwingen zijn te vinden. Er is medio 2016 een communicatieplan opgesteld met betrekking tot algemeen bewustzijn ('overall awareness') op omgang met digitale data naar aanleiding van de wet op datalekken. Zo is er een film op intranet geplaatst om de risico's van onbeveiligde netwerken inzichtelijk te maken. Met name bedoeld voor medewerkers die op locatie of thuis met privacygevoelige gegevens werken, het zogenoemde plaats onafhankelijk werken (POW).

Ter bevordering van de awareness ten aanzien van het plaats onafhankelijk werken met applicaties met privacygevoelige informatie moet een gebruikersovereenkomst gesloten worden. Daartoe vindt een gesprek plaats onder leiding van de teammanager. De coördinator informatiebeveiliging heeft daarin een ondersteunende rol.

De gemeente Zoetermeer heeft voor de bewustwording van de risico's zelf posters vervaardigd. Voor een daarvan heeft de wethouder geposeerd, om het draagvlak in de top van de organisatie voor dit onderwerp te onderstrepen. De posters gaan onder andere over mobiele datadragers, indringers/meelopers in de gebouwen en sterke wachtwoorden. Op deze terreinen is beleid geformuleerd dat ondersteund wordt door communicatiemiddelen. Bijvoorbeeld het wachtwoordbeleid met een autorisatie die op de rol van de medewerker is gebaseerd, met een 'multi-factor' authenticatie die vereist is voor de classificaties 'midden' of 'hoog'. En een zogenoemde 'single sign on' (SSO) wachtwoordenbeleid waarmee op 1 werkplek, met 1 login, alle applicaties aanwezig zijn waar de medewerker mee werkt.

Indringers/meelopers in stadhuis kunnen niet zomaar bij de werkplekken komen en daar informatie ontvreemden. Nog is een tag nodig om bij de werkplekken te komen en er is controle door de beveiligingsdienst. Vanaf eind 2017, met de realisatie van de nieuwbouw, gebouwen en infrastructuur voor diverse gebruikers alleen toegankelijk via poortjes aanwezig. Meelopers zouden dan niet meer kunnen voorkomen.

4.11 Hoe ver is de gemeente gevorderd met de voorbereidingen op implementatie van de Algemene verordening gegevensbescherming (AVG) van de EU?

Norm: Uiterlijk 25 mei 2018 moeten overheden en bedrijven voldoen aan de AVG van de EU. Daartoe behoort onder andere het aanstellen van een Functionaris voor de gegevensbescherming (FG).

Mei 2018 moet de governance en de gegevenshuishouding op het gebied van privacy op orde zijn, bij bedrijven en overheden. Volgens een van de respondenten is voor de implementatie van de AVG geen apart budget vrijgemaakt. De bedoeling is dat dit wordt ingebed in de staande organisatie. De gemeente heeft vanaf oktober 2017 structureel een privacyfunctionaris aangesteld. Deze functie was vanaf 2015 tijdelijk ingevuld. Deze externe kracht is met de applicatiearchitect bezig geweest de structuur voor gegevensbeheer en -huishouding op te zetten.

Boven de privacyfunctionaris komt de (verplichte) functionaris gegevensbescherming (FG). Deze functionaris moet aansluiten bij het Informatie Management Overleg (IMO). Het IMO wordt dan het besluitvormende orgaan voor privacy- en informatiebeveiligingsaangelegenheden.

Voor de transparantie over de wijze waarop de gemeente met privacygevoelige gegevens omgaat is in 2015 het privacyprotocol vastgesteld en gepubliceerd op de intranetsite. Volgens een enkele respondent moet dit protocol geüpdatet worden, omdat het document als te juridisch wordt ervaren en te weinig is gericht op begrijpelijkheid voor de burger. De burger moet erop kunnen vertrouwen dat de gemeente goed met zijn/haar gegevens omgaat, maar moet dat ook zelf kunnen lezen en zien.

De gemeenteraad wordt drie tot vier keer per jaar door middel van een memo geïnformeerd over de voortgang en stand van zaken op privacy en op incidenten. Het onderwerp privacy wordt meegenomen in perspectievennota en geadresseerd in teamgesprekken en personeelsgesprekken enz. Privacy is als onderwerp lastiger dan informatiebeveiliging. Op informatiebeveiliging fungeren de maatregelen uit de BIG als handvat. Dat is voor privacy niet op vergelijkbare wijze vastgelegd.

Bijlage 1. Lijst geïnterviewden en geraadpleegde literatuur

Interviews

- Robin Paalvast, wethouder
- Marc Rosier, wethouder
- Sandra Paulusma, coördinator informatiebeveiliging/CISO
- Jeroen Tomassen, directeur bedrijfsvoering/CISO
- Ingeborg Smit, privacyfunctionaris
- Marc van Gaalen, teammanager I&A
- Daniel van Dijk, security specialist I&A

Geraadpleegde literatuur

- Informatiebeveiligingsbeleid Gemeente Zoetermeer 2015 – 2017, december 2014
- Wachtwoordbeleid. Veilige toegang tot informatie, vs. 1.1, oktober 2016
- Memo Clearpass, 14 juni 2017
- Jaarplan Informatiebeveiliging 2015, vs. 1.0, 4 februari 2015
- Memo ENSIA (Eenduidige Normatiek Single Information Audit), 18 april 2017
- Memo POWbeleid (Plaats onafhankelijk werken) in de praktijk, 24 mei 2017
- Memo SSO (Single Sign On), 14 juni 2017
- Plaats en Onafhankelijk Werken beleid (POW-beleid). Veilig overal werken, vs. 0.7, 9 februari 2017
- Beleid "werken met mobiele apparaten" (beleid WmMA), vs. 0.3, 9 februari 2017
- Beleid Mobiele gegevensdrager USB stick. "Veilig data overdragen", vs. 0.4, 14 juni 2017
- Tokenbeleid. "Veilig overal werken", vs. 0.2, 18 mei 2017. (in ontwikkeling)
- Computer Emergency Response Team (CERT). Reactie, preventie en preparatie, vs. 0.3, 18 april 2017. (in ontwikkeling)
- Evaluatie Jaarplan Informatiebeveiliging 2015 'in één oogopslag', januari 2016.
- Gebruiksvoorwaarden voor Plaats Onafhankelijk Werken (POW) gemeente Zoetermeer team Belastingen inzake de belastingenapplicatie GOUW Belastingen, z.d.
- Risico-analyse, vs. 0.9, z.d.
- Memo risico-analyse, 11 mei 2017.
- Information Security Management System (ISMS)- advies, Aranea, vs. 1.0, 21-12-2016.
- GAP-analyse, vs. 1.01, 12 juni 2014.
- Gap-analyse advies, Aranea, vs. 1.0, 21 december 2016.
- GAP-analyse, externe bijlage, vs. 1.0, 21 december 2016.
- GAP-analyse, resultaten, vs. 1.0, 21 december 2016.
- Handleiding:
    - Beveiliging en privacy (handleiding wachtwoord, phishing, gebruik USB sticks, veilig bestanden delen, opslaan en delen, malware, meldplicht datalekken), z.d.
    - Malware, vs. 1, z.d.
    - Phishing, z.d.
    - USB-gebruik, z.d.
    - Veilig bestanden delen, z.d.

    - Wachtwoorden, z.d.
- Communicatieplan Beveiliging en Privacy, vs. 1, 25 juli 2016.
- Visitatiecommissie Informatieveiligheid VNG:
    - Verslag visitatiecommissie Informatieveiligheid VNMG, 22 maart 2017.
    - Gespreksverslag visitatiecommissie.

Bijlage 2. 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
ACIB	Algemeen Contactpersoon Informatiebeveiliging, ontvangt berichten van algemene aard van de Informatiebeveiligingsdienst voor gemeenten
AP	Autoriteit Persoonsgegevens
Applicatie	Softwareprogramma, zoals de BAG, BRP, SUWInet enz.
BAG	Basisregistratie Adressen en Gebouwen, applicatie met onder andere gegevens over adressen en gebouwen in de gemeente
Berap	Bestuursrapportage, 2 x per jaar
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 2019
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
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
ENSIA	Eenduidige Normatiek Single Information Audit, eenmalige informatieverstrekking en eenmalige IT-audit
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
GBA	Gemeentelijke Basisadministratie
GR	Gemeenschappelijke regeling
IBD	Informatiebeveiligingsdienst voor gemeenten
ICT	Informatie- en communicatietechnologie
IMO	Informatie Management Overleg
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
OWASP	Open Web Application Security Project
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
SSO	Single Sign On, op 1 werkplek via 1 aanmelding toegang krijgen tot alle applicaties waar de gebruiker recht op heeft
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
VPN	Virtueel privé netwerk (versleutelde beveiligde verbinding)