Gemeente **Zeist**

Publiekshal ▪ Het Rond 1, Zeist
Postbus 513, 3700 AM Zeist
Telefoon 14 030 ▪ zeist@zeist.nl

www.zeist.nl ▪ www.twitter.com/gemeentezeist
www.facebook.com/gemeentezeist

Ontv. griffie 06-07-2017
RIB17.095

Gemeente Zeist
Postbus 513
3700 AM ZEIST

Datum	5 juli 2017	**Ons kenmerk**	0221091
Burgerservicenummer		**Uw kenmerk**	Geen
Bijlage(n)	3	**Behandeld door**	mevr. B. Bouwhuis-Willems
Onderwerp	Rekenkamerbrief informatieveiligheid		

Geachte leden van de gemeenteraad en het college,

Digitale communicatie en informatievoorziening nemen in de huidige maatschappij een steeds grotere rol in. Bij deze ontwikkeling speelt ook het vraagstuk van aandacht voor informatieveiligheid. Het onderwerp is niet nieuw maar de maatschappelijke en politieke belangstelling ervoor wel.

De rekenkamer koos er daarom voor het onderwerp informatieveiligheid in het onderzoeksprogramma voor 2017 op te nemen. Allereerst hebben wij het college ter oriëntatie een aantal schriftelijke vragen over informatieveiligheid in Zeist gesteld. De beantwoording van de vragen door het college is terug te vinden in de bijlagen bij deze brief. In deze rekenkamerbrief duiden wij de verkregen informatie.

Algemene indruk: beleid en uitvoering informatieveiligheid goed op orde
Op basis van de beantwoording van de schriftelijke vragen heeft de rekenkamer de indruk gekregen dat de gemeente Zeist het beleid en de uitvoering van informatieveiligheid goed op orde heeft. Landelijke richtlijnen worden goed opgevolgd, er worden duidelijke plannen gemaakt en concrete doelen gesteld en er is sprake van een continue monitoring.

Wij zien dan ook geen aanleiding om verder onderzoek te gaan doen naar het onderwerp informatie-veiligheid. Wij volstaan met het toezenden van deze rekenkamerbrief. Wel willen wij de gemeenteraad en het college wijzen op enkele aandachtspunten in het beleid en uitvoering van informatieveiligheid.

Aandachtspunten

1. Verbetering communicatie.
Wij adviseren de gemeenteraad en het college om zowel binnen de organisatie als naar de samenleving nog meer aandacht te hebben voor communicatie over dit onderwerp. Een zorgvuldige communicatie is van essentieel belang voor het goed laten verlopen van processen. Communicatie is ook een belangrijk middel om te werken aan het vergroten van het bewustzijn. Het college geeft dit ook aan als één van de benoemde speerpunten voor 2017.

2. *Continue aandacht voor bewustwording (inclusief voldoende financiële middelen).*
Zoals ook in het Informatieveiligheidsplan 2017 gesteld wordt onder aandachtsgebied 4, is het belangrijk om continu te blijven werken aan de bewustwording ('bewustwording/awareness') van informatie-veiligheid. Wij sluiten ons hierbij aan en willen het belang hiervan extra benadrukken inclusief het beschikbaar stellen van voldoende middelen daarvoor.

3. *Verbeteringen op het gebied van control*
De gemeente voert sinds enige jaren een actief risicomanagement. Er wordt hierbij zowel gekeken naar externe risico's als naar procesrisico's. Hierbij is er ook aandacht voor risico's die samenhangen met informatieveiligheid. Het college concludeert dat er nog meer aandacht nodig is voor informatieveiligheid. De organisatie wil komen tot een meer gestructureerde aanpak op dit thema. Ook de toename van wet- en regelgeving vraagt hierom. In het interne controleplan 2017 is er aandacht voor de nieuwe ontwikkelingen. Wij adviseren om alle ontwikkelingen op het gebied van informatieveiligheid goed te volgen en hierop zo snel als mogelijk op te anticiperen.

4. *Aandacht voor invulling vacature 'security officer'.*
Informatieveiligheid past als taak niet goed binnen het al bestaande takenpakket van de medewerkers. De omvang van het takenpakket is hiervoor te groot. In de rapportage Informatieveiligheid 2016 wordt de functie van Chief Information Security officer (CISO) genoemd. Wij adviseren u om deze vacature zo spoedig mogelijk te vervullen.

Tot slot
Wij zullen de verdere ontwikkeling rondom informatieveiligheid binnen de gemeente Zeist belangstellend blijven volgen. Mocht u naar aanleiding van deze brief vragen en/of opmerkingen hebben, dan kunt u contact opnemen met het secretariaat van de rekenkamer via rekenkamer@zeist.nl of met Brenda Bouwhuis via 1 4 030.

Bijlagen bij deze brief
- Beantwoording vragen van de rekenkamer door het college
- Jaarplan informatieveiligheid 2017
- Jaarrapportage informatieveiligheid 2016

Met vriendelijke groet,
namens de Rekenkamer Zeist,

Alma Schaafstal
Voorzitter

Bijlage 1.

Rapportage informatieveiligheidsplan 2016

Informatiebeveiliging is geen nieuw thema. Gemeente Zeist geeft al jaren invulling aan dit onderwerp. Wat wel nieuw is, is de maatschappelijke en politieke aandacht voor dit onderwerp. Enerzijds ingegeven door de diverse ontwikkelingen, waaronder de decentralisatie, maar ook een toename, mede door de verdergaande digitalisering, van de bedreigingen op het gebied van continuïteit, betrouwbaarheid en vertrouwelijkheid. Dit maakt Informatieveiligheid tot een thema die zowel de bedrijfsvoering als de persoonlijke leefomgeving raakt. Dit maakt het bij uitstek een thema voor de (lokale) overheid . Overigens een thema dat een vanzelfsprekend onderdeel van het Business Continuity Management van onze gemeente moet zijn.

Tijdens de BALV van de VNG in november 2013 is de resolutie Informatieveiligheid [1] aangenomen. Deze resolutie bevat de gemeentelijke invulling van het begrip verplichtende zelfregulering op Informatieveiligheid. Mede op basis hiervan heeft in december 2013 de gemeente Zeist het strategisch Informatiebeveiligingsbeleid: *"Weerbaarheid als basis, bewustzijn als actieve prikkel"*[2] vastgesteld. In deze beleidsnotitie is de volgende visie opgenomen: Onze beveiliging moet zo georganiseerd zijn, dat we weerbaar zijn en kunnen voldoen aan de beveiligingsverwachtingen van onze klanten, opdrachtgevers en onszelf als overheidsorganisatie, en dus een betrouwbare (digitale) dienstverlening leveren.
De gemeente Zeist geeft vorm aan deze visie en de resolutie door concreet invulling te geven aan het professioneel organiseren en bestuurlijk verankeren van de informatieveiligheid, zoals verwoord in het coalitieakkoord Samen kansen pakken 2014-2015.

Om de weerbaarheid die wij als gemeente nastreven te realiseren dienen er een aantal zaken geregeld te worden. Het opstellen en actueel houden van een jaarlijks informatiebeveiligingsplan is er één van. In 2016 hebben we daarom op basis van de zogeheten zogeheten BIG (Baseline Informatiebeveiliging Gemeenten) een GAP analyse uitgevoerd en op basis hiervan een aantal concrete activiteiten genoemd om de Informatieveiligheid te verhogen en te zorgen dat we als organisatie in control zijn. Dit betekent niet dat alles geregeld is, dit is ook niet realiseerbaar, maar wel dat wij zicht hebben (en houden) op de mate waarin zaken al dan niet zijn geregeld en welke risico's daarbij kunnen optreden.

Doordat de uitvoering van de Jeugdwet, de AWBZ en de wet Participatie vanaf 2015 bij de gemeenten is komen te liggen, hebben de gemeenten vooral een grotere verantwoordelijkheid gekregen voor het goed en zorgvuldig delen van gegevens in het sociale domein. Waarbij het vooral gaat om het vinden van de juiste balans tussen noodzakelijke gegevensverwerking vanuit de maatschappelijke opgave van het sociale domein en het veilig werken waarbij de privacy wordt geborgd.

Een ander risico's is bijvoorbeeld het verkeerd terechtkomen van persoonsgegevens ofwel een datalek (in 2016 is de wet Meldpunt datalek ingevoerd, waarbij je als organisatie dit moet melden bij de Autoriteit persoonsgegevens(AP). Maar ook cybercriminaliteit is een risico dat vanwege nieuwe

---

[1] *Resolutie **Informatieveiligheid: randvoorwaarde voor de professionele gemeente** (BABVI/U201301281)*
[2] *Collegevoorstel **Weerbaarheid als basis, bewustzijn als actieve prikkel** 02-12-2013 (kenmerk 13CV.00471*

technologische technieken steeds grotere vormen aanneemt, waar je als gemeenten maatregelen tegen moet nemen.
Maar los van de diverse technologische en maatschappelijke ontwikkelingen en bedreigingen, ligt de grootste dreiging nog steeds bij het menselijk handelen.

Uitgangspunten van de informatieveiligheid en het plan
Zoals gezegd is de gemeente zelf verantwoordelijk voor het opstellen en/of uitvoeren en/of handhaven van de regels. Hierbij geldt:

- Er is wetgeving waar altijd aan voldaan moet worden (BRP, SUWI, BAG etc.)
- Er is een gemeenschappelijk normenkader als basis; Baseline Informatiebeveiliging Nederlandse Gemeente (BIG);
- De gemeente stelt dit normenkader vast waarbij er ruimte is voor afweging en prioritering op basis van het 'pas toe of leg uit' principe.

De focus en planning voor 2016

Zoals opgenomen in het Informatiebeveiligingsplan 2016 was het speerpunt voor 2016 de daadwerkelijke implementatie van de BIG (Baseline Informatieveiligheid Gemeenten). De BIG geldt als dé minimale set van maatregelen, die gemeente breed ingevoerd moeten worden. Ongeacht het proces of het systeem, de BIG ondersteunt gemeenten en geldt voor alle bedrijfsvoering processen.
Het uitgangspunt is dat 100% veilig niet bestaat en dat incidenten niet zijn te voorkomen, maar door een juist gebruik van de BIG kan wel voorkomen worden dat een incident meer impact krijgt dan nodig is.
Onderstaand

1. Start met de implementatie van een ISMS (Information Security Management Systeem) dat geënt is op de BIG (Baseline Informatiebeveiliging Gemeenten). Dit stelt ons in staat acties uit te zetten en te monitoren, terwijl de verantwoording en benodigde kennis wordt opgeslagen in dit systeem.
   In 2016 is gestart met de implementatie van een ISMS. In 2016 is voor het eerst de zelfaudit BRP hierin opgenomen. Dit heeft geleid tot integrale bewaking en coördinatie op het uitvoeren van de zelfaudit. En is deze informatie ook beschikbaar voor volgende audits.
   In 2017 zal het ISMS verder worden ingericht en gebruikt, o.a. voor wat betreft privacy.

2. Benoemen van rollen en verantwoordelijkheden (CISO: Chief Information Security officer en het Team Informatieveiligheid) en deze aan laten sluiten op de gemeentelijke crisisorganisatie.
   Nog niet alle rollen en verantwoordelijkheden zijn benoemd en belegd. In het college voorstel van 2016 (*Informatieveiligheid en privacy: visie, beleid en actieplan*) is aansluiting op de crisisorganisatie voorgesteld.

3. Implementeren meldpunt Datalekken.
   het meldpunt datalekken is inmiddels geïmplementeerd. Vanaf begin 2016 is er een regieteam die in nauwe samenwerking met onder andere de bestuurder meldingen ontvangt, analyseert, adviseert over de te nemen stappen en uiteindelijk zowel procedureel als inhoudelijk afwikkelt (inclusief eventuele melding bij de AP). Er is inmiddels ook een compacte procedure. Op basis van de opgedane ervaringen in 2016 heeft er ook een evaluatie plaatsgevonden en zijn er aanbevelingen gedaan aan het management, waarbij er aandacht is gevraagd voor het digitaal vaardig zijn en worden van (nieuwe) medewerkers.

4. Starten met bewustwording (awareness)
   We hebben aangesloten bij het programma Landelijk programma Alert-Online, er heeft een actie plaatsgevonden voor wat betreft de schermbeveiliging (rode sticker actie), en is er via posters en Intranet aandacht gevraagd voor het onderwerp Informatieveiligheid. Met een kleine groep is gebrainstormd om een compact bewustwordingsplan te maken dat is gericht op gedragsverandering en wat je daadwerkelijk wil bereiken. Ook is Informatieveiligheid samen met privacy onderdeel gemaakt van het inwerkprogramma. En wordt het onderdeel van de Zeist academie.

5. Audits (o.a. BAG, DigiD en de zelfaudit BRP.
   Met de diverse collega's is er samengewerkt om de diverse audits integraal en uniform te verwerken. Zoals vermeld bij punt 1, is de zelfaudit BRP uitgevoerd in het ISMS.

6. Starten met dataclassificatie van de gebruikte applicaties en beleggen werkzaamheden dataclassificaties bij Control. Prioriteit bij de 30 meest privacy gevoelige systemen.
   In 2016 is gestart met het uitvoeren van dataclassificaties. Op basis van een risicoanalyse zijn de 30 meest risicovolle applicaties geclassificeerd. Deze zijn uitgevoerd door de afdeling Informatievoorziening, overdracht naar Control heeft nog niet plaatsgevonden. Ook is elke nieuwe applicatie geclassificeerd. Bij deze toetsing worden ook gelijk de verwerkingsovereenkomsten meegenomen.
   Voor de komende periode 2017-2018 staat gepland dat alle overige applicaties worden geclassificeerd.

7. Starten met de uitvoering van de Algemene Verordening Gegevensbescherming (AVG).
   Voor wat betreft de AVG is er binnen de regio afstemming geweest over mogelijk samenwerking op dit onderwerp. Onder ander voor wat betreft het aanstellen en delen van een Functionaris Gegevensbescherming (FG), en het formuleren van uniform beleid en regelementen.
   Verder is de AVG in kaart gebracht en is er op hoofdlijnen een plan van aanpak opgesteld. Daarbij is over de AVG ook melding gedaan bij de kadernota.

8. Inventariseren van en adviseren over het SUWI-Net gebruik (zowel intern als in de keten).
   De Suwi-Net aansluiting is na het landelijk onderzoek en een interne analyse, buiten werking gesteld. Bij de samenwerkingsverbanden geldt daar een eigen verantwoordelijkheid voor at betreft het gebruik van Suwi-Net, maar heeft Zeist wel een gecontroleerd of er wordt voldaan aan de regelgeving.

Proces: PDCA cyclus

Om de informatiebeveiliging up-to-date te houden is het belangrijk dat jaarlijks het bestaande informatiebeveiligingsplan wordt geactualiseerd. Zowel toetsing van het bestaande beleid in relatie tot nieuwe ontwikkelingen als planvorming voor de toekomst. Vanuit de resolutie dient informatieveiligheid bestuurlijk en organisatorisch geborgd te worden door aansluiting in de reeds bestaande planning- en control cyclus (Plan – Do- Check – Act). Interne Controle, maakt daarom ook deel uit van het Team Informatieveiligheid.

Bijlage 2.

Jaarplan informatieveiligheid 2017

Het jaarplan 2017 is opgesteld op basis van de bevindingen van een opnieuw uitgevoerde zogeheten BIG (Baseline Informatiebeveiliging Gemeenten) GAP analyse.
Zoals verwoord in onderstaande aandachtsgebieden liggen de aandachtsgebieden op Organisatie van de Informatiebeveiliging, Personele beveiliging en Bedrijfscontinuïteitsbeheer (hoofdstukken 6, 8 en 14 van de BIG.
Daarnaast zijn ook de nog niet (volledig) afgeronde activiteiten uit het jaarplan 2016 meegenomen.

A. Organisatie van de Informatieveiligheid (hoofdstuk 6)

Gericht op de organisatie van de Informatieveiligheid, een gemeente breed aandachtspunt.
Doelstelling: Beheren van de informatiebeveiliging binnen de organisatie.

Voor het jaarplan 2017 worden hierbij de volgende acties benoemd.

1. In de praktijk is gebleken dat het op orde brengen en houden van de informatieveiligheid en privacybescherming teveel inzet vergt om als extra klus door medewerkers naast hun huidige werkzaamheden te kunnen doen. In de wetenschap dat de werkzaamheden op dit gebied alleen nog maar zullen toenemen moet een structurele oplossing gevonden worden. De taken van de CISO en de Privacy Officer moeten daarbij duidelijk omschreven en belegd zijn.
   Naast de voor deze functies benodigde uren moet tevens inzichtelijk worden gemaakt welke taken/activiteiten er nu door medewerkers naast hun reguliere werk worden gedaan om ook hier een structurele oplossing en inbedding te bewerkstelligen.
2. Opstellen van een (tactisch)informatiebeveiligingsplan/beleid, dat gebruikt kan worden als handleiding voor de hieronder bij hoofdstuk 8 genoemde acties gericht op de medewerkers. Alsmede de 10 punten genoemd in de AVG (Algemene Verordening Gegevensbescherming).
3. Inhuren van een zogeheten white had hacker om inzicht te krijgen in de staat van onze beveiliging.

B. Personele beveiliging (hoofdstuk 8)

Gericht op personeel en medewerkers van de organisatie. In eerste instantie aandachtsgebied van P&O.
Doelstelling: Bewerkstelligen dat werknemers, ingehuurd personeel en externe gebruikers hun verantwoordelijkheden begrijpen, en geschikt zijn voor de rollen waarvoor zij worden overwogen, en om het risico van diefstal, fraude of misbruik van faciliteiten te verminderen.

Voor het jaarplan 2017 worden hierbij de volgende acties benoemd.

4. Zorgen dat Bewustwording/Awareness structureel aandacht krijgt enerzijds door gerichte acties uit te voeren, anderzijds door niet vrijblijvende sessies te beleggen voor, in eerste instantie, nieuwe medewerkers van gemeente Zeist, waarbij de informatieveiligheid en het omgaan met privacy gevoelige gegevens de leidraad zijn.
5. Regelen van uniforme afspraken met samenwerkingsverbanden over het uitwisselen van informatie, waaronder het contractmanagement en verwerkersovereenkomsten.

C. Continuïteit (hoofdstuk 14)

Gericht op het voorkomen en beperken van continuïteitsproblemen.
Doelstelling: Op basis van risicoanalyses maatregelen te treffen om het onderbreken van bedrijfsactiviteiten tegen te gaan en kritische bedrijfsprocessen te beschermen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en om tijdig herstel te bewerkstelligen.

Voor het jaarplan 2017 worden hierbij de volgende acties benoemd.

6. Meegaan in de (technologische) ontwikkelingen m.b.t. audits, zoals de ENSIA (Eenduidige Normatiek Single Information Audit).
7. Het door gemeente Zeist in 2016 aangeschafte ISMS (Information Security Management System) Key2control (K2C) inzetten als regiesysteem voor informatieveiligheid en privacy.
8. Continuïteitsplan laten opstellen en uitvoering geven aan de uitwijktesten.
9. Bepalen welke maatregelen moeten worden genomen als leveranciers niet kunnen voldoen aan de door Zeist gestelde eisen van bijvoorbeeld hardening (versiebeheer & autorisaties) bij informatiesystemen.

Proces
In het 1ste kwartaal 2018 zullen we opnieuw een GAP analyse uitvoeren en op basis daarvan het College rapporteren over de in 2017 genomen maatregelen, en een Informatiebeveiligingsplan 2018 opstellen.

Bijlage 3.

Schriftelijke beantwoording vragen rekenkamercommissie informatieveiligheid Zeist

Aanleiding:
Het College heeft uw brief "Vragen rekenkamer Informatieveiligheid" van 29 maart 2017 met als kenmerk: 0221091 ontvangen. Onderstaand is de kern van de brief en de gemaakte opmerkingen opgenomen. Vervolgens treft u per vraag de beantwoording aan. In deze zelfde periode is ook de rapportage over het Informatieveiligheidsplan 2016 opgesteld alsmede het Informatieveiligheidsplan 2017. Dit is de reden dat wij in de beantwoording ook regelmatig verwijzen naar deze stukken.

Gemeenten en informatieveiligheid
Digitale informatie en communicatie neemt een steeds grotere plek in de gemeentelijke organisatie in. Gemeenten zijn zich bewust van het belang van informatieveiligheid en de gevolgen van inbreuken op hierop. Daarom staat het onderwerp informatieveiligheid hoog op de (bestuurlijke) agenda. Het gaat daarbij onder meer om de privacy van inwoners die in het geding kan zijn, maar bijvoorbeeld ook de (digitale) dienstverlening van de gemeente. Gegevens van inwoners, bedrijven en instellingen moeten bij de gemeente veilig zijn. Daarbij geldt wel dat 100% veiligheid niet bestaat. Het draait om het bewust omgaan met (digitale) veiligheidsrisico's.
Bij het verbeteren van de informatieveiligheid bij gemeenten wordt uitgegaan van een 'verplichte zelfregulering'. Dit betekent dat het Rijk heeft vastgelegd dat gemeenten in eerste instantie zelf aan zet zijn. De Informatie Beveiligings Dienst heeft de Baseline Informatiebeveiliging Gemeenten (BIG) opgesteld, waarmee gemeenten een basisnorm voor informatieveiligheid aangereikt krijgen.

Oriëntatie Rekenkamer Zeist
In het onderzoeksprogramma voor 2017 heeft de Rekenkamer Zeist vanwege bovengenoemd belang besloten zich te oriënteren op een onderzoek naar informatieveiligheid binnen de gemeente Zeist.
We hebben een eerste oriëntatie gedaan door een aantal documenten te bekijken en een informeel gesprek te voeren met de senior informatieadviseur. Hieruit blijkt dat er al een aantal stappen is gezet om beleid te ontwikkelen en te implementeren. De gemeenteraad ontving hierover in 2016 een informatiebrief.

Vervolg: schriftelijke vragen aan college
Volgende stap in onze oriëntatie is, in plaats van een uitgebreid onderzoek, u als college een aantal schriftelijke vragen te stellen. Deze vragen zijn opgenomen in bijlage 1. Wij zouden het waarderen wanneer u deze vragen wilt beantwoorden. Kunt u ons aangeven hoeveel tijd u ongeveer voor de beantwoording nodig heeft? Naar aanleiding van uw reactie zal de rekenkamer besluiten of zij verder onderzoek zal verrichten en op welke wijze zij de gemeenteraad over informatieveiligheid zal informeren. Mogelijk plannen wij naar aanleiding van uw beantwoording een toelichtend gesprek in.

Opmerking vooraf van de rekenkamer:

De Rekenkamer Zeist heeft de beschikking gekregen over twee beleidsdocumenten:
- Informatieveiligheid Weerbaar en Bewust, 2016-2018;
- Visie op Privacy, De kunst van het selectief verzamelen en de balans tussen afstand en nabijheid.

Ook ontvingen wij het jaarplan informatieveiligheid voor 2016. De rekenkamer heeft begrepen dat het jaarplan 2017 vertrouwelijk verklaard zal worden. Kunt u bij de beantwoording aangeven in hoeverre deze vertrouwelijk is en blijft? Wij zullen er dan bij het verwerken van de antwoorden rekening mee houden.

Over beleid, visie en managementsturing

1. Kan het college aangeven in hoeverre met de genoemde documenten invulling is gegeven aan de resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' en de implementatie van de BIG? Welke stappen zijn in 2016 gezet en welke stappen moeten nog gemaakt worden vanaf 2017?
   De gemeente Zeist heeft sinds de vaststelling van de resolutie door de BALV in 2014, invulling gegeven aan deze resolutie in haar Informatieveiligheidsbeleid. De BIG wordt als normenkader gebruikt bij de invulling van het Zeister beleid.
   In 2016 zijn de in de BIG genoemde risico's in kaart gebracht dat heeft geleid tot het jaarplan 2016, terwijl tevens een zogeheten ISMS (Information Security Management System) is aangeschaft en ingevoerd om regie te kunnen houden op de betrokken processen.
   Voor de nog te nemen stappen in 2017 wordt verwezen naar Rapportage Jaarplan 2016 & Jaarplan 2017 (zie bijlage 1)

2. In hoeverre zijn de voorgenomen punten in het jaarplan informatieveiligheid 2016 gerealiseerd? Wat zijn redenen voor het wel of niet realiseren van de punten?
   Voor beantwoording van deze vraag verwijzen wij graag naar de Rapportage Jaarplan 2016 & Jaarplan 2017 (zie bijlage 1)

3. Wat zijn de speerpunten voor het informatieveiligheidsplan 2017? En hoe worden gemeenteraad, college en ambtelijke organisatie hierbij betrokken?
   Voor 2017 is de bewustwording (awareness) op alle niveaus het belangrijkste speerpunt. Periodiek wordt het college geïnformeerd over de voortgang van de Informatieveiligheid. Daar waar nodig zal ook de gemeenteraad worden geïnformeerd, bijvoorbeeld ook via WSJG.nl. De ambtelijke organisatie wordt via persoonlijke instructies, bewustwordingsacties, de Zeist Academie en gerichte communicatie betrokken bij dit onderwerp.
   Voor verdere beantwoording van deze vraag verwijzen wij graag naar de Rapportage Jaarplan 2016 & Jaarplan 2017 (zie bijlage 1)

4. Rapporteert en bespreekt de gemeente Zeist het functioneren van de cyclus van informatieveiligheid op management en bestuursniveau (gemeenteraad en/of college)? Zo ja, hoe? Zo nee, waarom niet? Wordt hierover via waarstaatjegemeente.nl gerapporteerd? Waarom wel of niet?
   Sinds 2016 is de Zeister Informatieveiligheid onderdeel van waarstaatjegemeente.nl. Zo is op 18 mei 2017 het onderwerp met de raad besproken in het kader van de toezichtinformatie (zie ook: WSJG.nl).
   Er vindt periodiek (3 wekelijks) overleg plaats met de portefeuillehouder J. Varkevisser. En op 13 september 2016 heeft het College Informatieveiligheid en Privacy in een aparte bijeenkomst besproken, vervolgens het beleid (16cv.00317) vastgesteld en een raadsinformatiebrief gestuurd (16uit03982).
   Hoe en op welke wijze het management structureel te betrekken is onderwerp van gesprek.

5. Hoe vraagt de gemeente Zeist aandacht voor informatieveiligheid bij haar medewerkers (bewustwording)? Welke acties zijn hiervoor gedaan? Tot welke opbrengsten hebben de acties geleid? Gaan deze acties naar tevredenheid? Zijn er verbeteringen mogelijk? Zo ja, welke?
   Zoals gezegd is 2017 bewustwording het belangrijkste speerpunt. Zo heeft een actie plaatsgevonden om medewerkers te wijzen op zogenaamde phishing naar toegangsgegevens. Voor verdere beantwoording van deze vraag verwijzen wij graag naar de Rapportage Jaarplan 2016 & Jaarplan 2017 (zie bijlage 1)

6. Is er een integrale aanpak voor organisatie breed leren over informatieveiligheid? Zo ja, welke? Zo nee, waarom niet? Hoe houdt de gemeente Zeist kennis vast en bouwt zij hierop voort?
   Voor dit onderdeel hebben we een workshop "Ik ben best wel Informatieveilig ;-)....."gecreëerd die onderdeel vormt van de Zeist academie. En heeft er een lunchlezing plaatsgevonden over Identiteitsfraude.

Dienstverlening door de gemeente en de gevolgen van uitval of verstoring

7. Hoe waarborgt de gemeente Zeist de gemeentelijke dienstverlening (continuïteit) in het geval van grootschalige uitval of verstoring van de ICT?
   Er is een dubbel uitgevoerd datacenter, met een deel in Zeist en een deel in Houten. Beide afzonderlijke delen zijn in staat om ieder voor zich de volledige omgeving aan te bieden. Voor het volledig kunnen uitwijken van de gehele gemeentelijke organisatie dienen nog de laatste technische maatregelen gerealiseerd te worden. Dit is voor de zomervakantie geregeld.

8. Heeft de gemeente Zeist intern afspraken gemaakt over de wijze waarop zij handelt bij (ernstige) informatieveiligheidsincidenten? Is hiervoor een werkproces opgesteld? Waarom wel of waarom niet? En welk proces is opgesteld?
   Zeist heeft intern, onder andere met dienstverlening, communicatie en de crisisorganisatie afspraken gemaakt over de wijze van handelen bij informatieveiligheidsincidenten. Het resultaat is een draaiboek Informatie-technische storing.

9. Heeft de gemeente Zeist zicht op de leveranciers en partners waarmee samengewerkt wordt? Toetst de gemeente deze leveranciers op informatieveiligheidsaspecten? Zo ja, hoe dan? Zo nee, waarom niet? M.a.w. hoe is de keten verantwoordelijkheid ingericht?
   De leveranciers die toegang mogen hebben krijgen alleen toegang op verzoek en de werkzaamheden worden gemonitord en gelimiteerd (qua omgeving, qua duur en rechten'. Het beleid is geen toegang tenzij. Het structureel jaarlijks beoordelen van je leveranciers en het indien nodig herijken van je contracten (contractmanagement) is nog een aandachtspunt en daarom ook opgenomen in het jaarplan 2017.

10. Hoeveel incidenten/uitval van ICT hebben zich voorgedaan waarbij de informatieveiligheid in het geding was? Wat heeft de gemeente geleerd van deze incidenten?
    In totaal hebben we in de afgelopen anderhalf jaar 3 incidenten/verstoringen gehad: een keer malware aanval, onderbreking van de bedrijfsvoering gedurende een nacht met vrijwel geen impact voor de organisatie; een stroomstoring overdag met als gevolg verstoring van de bedrijfsvoering gedurende enkele uren en een technische storing bij het uitvoeren van onderhoud op de technische omgeving met als gevolg dat enkele uren geen gebruik van de systemen gemaakt kon worden en er tevens nog een aantal dagen verschillende herstelacties moesten plaatsvinden binnen de bedrijfsapplicaties. Bij het oplossen van de problemen van deze laatste storing heeft geleid tot een draaiboek Informatie-technische storing.

    Daarnaast hebben we een tweetal zogeheten datalekken gemeld bij de AP (Autoriteit Persoonsgegevens). Dit heeft geleid tot een organisatie, die direct kan schakelen in een dergelijk voorval. Standaard vindt evaluatie plaats, waarbij ook de wethouder betrokken wordt en de raad wordt geïnformeerd .

11. Hoe toetst de gemeente Zeist haar systemen en gebouwen op (cyber)aanvallen van buitenaf? Welke noodscenario's zijn er opgesteld? Heeft de gemeente zicht op risico's en zwakke plekken? Is er zicht op hoe gemakkelijk een hacker kan binnenkomen en tot hoe ver deze hacker in de gemeentelijke systemen kan komen?
    Voor wat betreft de systemen is dit tweeledig. Enerzijds vindt er geautomatiseerde monitoring van technische apparatuur plaats, anderzijds wordt door onze security partners, waaronder de IBD (Informatie Beveiligings Dienst) actief gemonitord op de gebruikte systemen.
    Als noodscenario is er vooral gezorgd voor actuele en complete, hoog beschikbare, backups van de volledige omgeving met als doel disaster recovery z.s.m. mogelijk te maken. Daarnaast zorgt de IBD pro actief voor monitoring en informatievoorziening m.b.t. risico's, los hiervan informeert onze securitypartner ons pro actief, terwijl de systeembeheerders ook zelf aan monitoring doen.
    We hebben zicht op de risico's. Door inhuur van externe specialisten worden zogeheten penetratie tests uitgevoerd, waarbij er tevens de mogelijkheid is dat nieuwe risico's worden benoemd. Hierbij wordt tevens inzichtelijk gemaakt hoe diep een hacker in het systeem kan komen. Ook voor 2017 staat dit gepland.
    Wij zijn er ons van bewust dat ondanks alle maatregelen het niet de vraag is of wij gehackt worden, maar wanneer wij gehackt worden. Alles is er echter op gericht om ook dan de schade zoveel als mogelijk te beperken.

Onderstaande vragen 12 t/m 14 zijn beantwoordt door Control.

Control en risico's

12. Wat zijn de belangrijkste risico's die de gemeente loopt?
13. Op welke wijze toetst de gemeentelijke organisatie of zij in control is op het gebied van informatieveiligheid?
14. Hoe toetst de gemeente Zeist of de beleidsuitgangspunten nog valide zijn? Hoe borgt de gemeente Zeist dat nieuwe interne of externe ontwikkelingen die wijzigingen in de gemeentelijke risico-in-schattingen tot gevolg hebben, meegenomen worden in de beleidsuitgangspunten? Is aanpassing van het beleid al voorgekomen? Zo ja, welke aanpassing dan en waarom?

De gemeente voert sinds jaren een actief risicomanagement. Naast inventarisatie van de externe risico's (uitvoeringsrisico's) wordt ook gekeken naar procesrisico's. Vanuit de Verbijzonderde Interne Controle (VIC) worden alle processen op een risicogerichte wijze geaudit. Hierbij is ook aandacht voor risico's m.b.t. informatieveiligheid. Jaarlijks auditen we meerdere processen en onderdelen van processen waarbij er aandacht is voor dit vraagstuk, de risico's worden periodiek geactualiseerd. Naast de jaarlijkse audits wordt iedere nieuwe applicatie onderworpen aan een zogenaamde EDP audit en wordt volop aandacht besteedt aan een goede inrichting van de administratieve organisatie en de interne controle hierop. Ook de accountant toets jaarlijks op onderdelen van de informatieveiligheid (hiervoor heeft onze accountant specialisten in dienst die onze gemeente aan audits onderwerpen).
We merken dat het onderwerp echter meer aandacht verdient. Enerzijds is dit nodig omdat wij als organisatie stappen willen zetten naar een meer gestructureerde aanpak van het thema informatieveiligheid anderzijds zien we een toename in wet- en regelgeving die van invloed is of wordt. Zo is de controle van de accountants de afgelopen jaren flink aangescherpt, dit komt ook tot uiting op het informatieveiligheidvlak. Daarnaast is er een wetsvoorstel in ontwikkeling dat colleges (waarschijnlijk) vanaf 2019 een 'in control statement' aan de raad moeten gaan afgeven, hierdoor zal de rechtmatigheidsverklaring van de accountant waarschijnlijk komen te vervallen. Naar alle waarschijnlijkheid zal het 'in control statement' bestaan uit een aantal belangrijke pijlers, te weten een goed planning en controlsysteem, actief risicomanagement en een goede VIC.
In het 'Interne controleplan 2017', dat de basis vormt voor de VIC, wordt geanticipeerd op deze ontwikkelingen. Zo wordt in het plan expliciet ingegaan op informatieveiligheid, privacy en audits op applicaties, deze zullen vanaf 2017 explicieter onderdeel gaan uitmaken van de Verbijzonderde Interne Controle (VIC). Vervolgens zal er een frauderisico analyse worden opgesteld waarbij de gekeken wordt wat fraudegevoelige functies zijn en welke beheersmaatregelen genomen kunnen worden. Enerzijds zullen dit maatregelen zijn die betrekking hebben op voldoende functiescheiding anderzijds zullen deze maatregelen automatisering technisch van aard zijn.