Rapport

Informatiebeveiliging en privacy Gemeente Zeist

Rekenkamer Zeist

April 2024

Auteur: drs. Etienne Lemmens

Prae Advies en onderzoek, Utrecht

Prae Advies en onderzoek, handelsnaam van BB35 BV, Buys Ballotstraat 35, 3572 ZT Utrecht
E info@prae-advies.nl | W www.prae-advies.nl

“Informatie is één van de voornaamste bedrijfsmiddelen van de gemeente. Het verlies van gegevens, uitval van ICT, of het door onbevoegden kennisnemen of manipuleren van informatie kan ernstige gevolgen hebben voor de bedrijfsvoering en dienstverlening, leiden tot imagoschade en verlies van vertrouwen in de overheid.”

Uit: Bestuurlijke rapportage gemeente Zeist, 2020.

Inhoudsopgave

Samenvatting, conclusies en aanbevelingen

Samenvatting

Inleiding

Eind 2023 heeft de Rekenkamer Zeist onderzoek uitgevoerd naar de informatieveiligheid van de gemeente Zeist.[1] Met het onderzoek wil de rekenkamer de raad in de breedte informeren of de informatieveiligheid bij de gemeente Zeist voldoende is geborgd. Gebleken is dat overheden op het gebied van cybersecurity grote bestuurlijke en financiële risico's lopen, zodanig dat het onderwerp informatieveiligheid meer en meer op de bestuurlijke tafels terecht komt.

De rekenkamer bedankt bestuur, directie en ambtenaren voor de uitstekende samen- en medewerking in dit onderzoek. Dat luisterde nauw vanwege de testen die in het kader van dit onderzoek zijn uitgevoerd.

Techniek, organisatie, mens

Met het onderzoek richt de rekenkamer de aandacht op drie invalshoeken: techniek, organisatie en beleid, mens en gedrag. Daartoe is een bureaustudie uitgevoerd, zijn interviews gehouden en zijn op de systemen testen uitgevoerd, zogenoemde pentesten. Deze samenvatting laat de belangrijkste bevindingen zien. De bevindingen leiden tot conclusies en aanbevelingen aan de gemeenteraad en het college.

Informatiebeveiliging en Privacy

Informatieveiligheid kent twee aspecten. Enerzijds de informatiebeveiliging, waarbij het vooral gaat om de beschikbaarheid, integriteit en vertrouwelijkheid van te verwerken informatie. De norm waaraan gemeenten moeten voldoen is de Baseline Informatieveiligheid Overheid (BIO). Anderzijds gaat het om privacy en dan gaat het met name om namens de gemeente te verwerken persoonsgegevens. De norm hiervoor is de Algemene Verordening Gegevensbescherming (AVG).

Beleid

Volgens de reguliere beleidscyclus op informatieveiligheid wordt eerst via een behoefte- of GAP-analyse[2] geanalyseerd waar de situatie op informatieveiligheid niet voldoet aan de eisen. Daarna worden op basis van een risicoanalyse de geprioriteerde activiteiten in een jaarplan opgenomen. Zeist wijkt hiervan iets af door in 2023 in plaats van met een jaarplan te werken met een Verklaring van Toepasselijkheid (VvT)[3]. De reguliere cyclus van GAP-analyse, risicoanalyse en jaarplan wordt wel weer opgepakt. Zeist volgt daarmee grotendeels de risico-gebaseerde reguliere beleidscyclus ten aanzien van informatieveiligheid en privacy. Wel constateert de

1 Het onderzoek is uitgevoerd door Prae Advies en onderzoek. De testen zijn uitgevoerd door IP4Sure en LBVD.

2 GAP Is de Engelse term voor 'kloof'. Dat betekent hier het verschil tussen de bestaande situatie en de gewenste situatie zoals voorgeschreven door de eisen van de Baseline Informatiebeveiliging Overheid (BIO).

3 De Verklaring van Toepasselijkheid is een document waarin staat welke maatregelen een organisatie heeft genomen om de informatiebeveiliging te waarborgen en wat geactualiseerd dient te worden

rekenkamer dat bij de gemeente Zeist geen integraal risicomanagement is geïmplementeerd, waar informatieveiligheid onderdeel van is.

Het strategische beleid is in Zeist vastgesteld in overeenstemming met de geldende normen. Het beleid is op het 'three lines of defence'-principe[4] geënt en de verantwoordelijkheden zijn conform dat principe in het beleid vastgelegd. De beleids- en visiestukken volgen de mainstream in gemeenteland. Ze getuigen nog niet van een grote ambitie op het gebied van informatieveiligheid en privacy.

Voor de doorvertaling van het strategisch beleid naar het tactisch en met name operationeel niveau heeft de gemeente nog veel stappen te zetten.

De middelen voor informatieveiligheid en privacy zijn niet afgebakend in de begroting en verantwoording, maar als iets nodig is worden de middelen door directie en bestuur ter beschikking gesteld.

Bemensing

De functies op het gebied van informatieveiligheid en privacy zijn voldoende bezet om aan de huidige ambitie te kunnen voldoen. Bij een hogere ambitie past uiteraard meer capaciteit. Dat geldt sterker met het oog op toekomstige ontwikkelingen en eisen die aan de gemeente worden gesteld. De Chief Information Security Officer (CISO) is nu in de lijn gepositioneerd bij de afdeling Informatievoorziening. De IBD (de Informatiebeveiligingsdienst die gemeenten vanuit de VNG ondersteunt) ziet deze rol liever los van de lijn ingevuld. Met de huidige bezetting kan een CISO-functie ingevuld worden die onafhankelijk is van de lijn.

Er zijn voldoende momenten waarop de professionals op informatieveiligheid en privacy elkaar treffen en de aangelegenheden op strategisch, tactisch en operationeel niveau onderling bespreken. Ook directie en bestuur zijn hierbij aangesloten.

Informatie gemeenteraad

De gemeenteraad wordt in de reguliere cyclus gerapporteerd over de vorderingen op het informatieveiligheids- en privacybeleid. Dat gebeurt jaarlijks door middel van de verplichte rapportages op informatieveiligheid (Eenduidige Normatiek Single Information Audit, ENSIA) en sinds kort door het jaarverslag van de Functionaris Gegevensbescherming. Daarbij krijgt de raad wel duiding, maar nog geen dieper inzicht in de risico's die de gemeente op het gebied van informatieveiligheid en privacy loopt. Incidenteel krijgt de raad ook informatie via raadsinformatiebrieven en worden themabijeenkomsten georganiseerd. Er is geen structureel overleg over dit onderwerp tussen college en raad aangetroffen.

Bewustwording

De gesprekspartners vinden het positief dat er meer bewustwording bij de medewerkers is gekomen de laatste jaren. Tegelijk erkennen zij dat het

[4] In het kort zijn er in de 'three lines of defence' drie verdedigingslagen: (lijn)management is primair verantwoordelijk voor strategie en sturing van de organisatie en managen van risico's; de tweede lijn is verantwoordelijk voor de structuur en inrichting van de organisatie; de derde lijn is het (interne en externe) toezicht op de kwaliteit van sturing en beheersing.

gewenste niveau nog niet bereikt is. Het bestuur en directie zetten hier wel op in. Een lerende houding wordt sterk gepropageerd en management en college geven het goede voorbeeld.

Ondanks veel activiteiten, zoals aandacht voor informatieveiligheid en privacy in het inwerkprogramma, e-learning en berichten op intranet, wordt het eigenaarschap bij het lijnmanagement en de eerste lijn van medewerkers nog te weinig beleefd. De gemiddelde score voor taakvolwassenheid op informatieveiligheid wordt in Zeist door de gesprekspartners ingeschat op 2 op de 5 puntsschaal van NOREA.[5]

Bij de phishingmail-test in het kader van het rekenkameronderzoek blijkt dat het klikpercentage onder de steekproef van medewerkers van de gemeente hoger is dan gemiddeld bij vergelijkbare phishing mails. Dat is ook een signaal dat de vereiste bewustwording van de risico's bij de medewerkers nog niet is bereikt.

Datalekken

De gemeente heeft een proces datalekken vastgesteld, waarin de activiteiten en communicatie bij een datalek zijn beschreven. Er is een meldpunt, waarbij onder andere de CISO en Privacyofficer zijn aangesloten. Er zijn weinig 'echte' datalekken gemeld, maar de communicatie met betrokkenen wordt als positief ervaren.

Controle

De gemeente heeft enkele middelen voor het naleven en voorkomen van incidenten op het gebied van informatieveiligheid en privacy tot zijn beschikking. Dat zijn onder andere de accountantscontroles, de Verbijzonderde Interne Controles en de assessments op de verwerking van persoonsgegevens (dpia's). Deze leiden tot verbetermaatregelen. Een van de manieren om die activiteiten te volgen is het managementinformatie-systeem op informatieveiligheid (ISMS). Dat is in Zeist aanwezig, maar wordt niet optimaal benut. Het aantoonbaar vastleggen en borgen van activiteiten behoeft verbetering.

Pentesten

De gemeente voert zelf testen op de systemen uit, de laatste was in 2021. Daarbij zijn risico's aangetroffen (waaronder één kritiek) die in verbeter-plannen zijn opgenomen. De rekenkamer liet in november 2023 door een ethisch hacker de pentesten (penetratietesten) uitvoeren. Hierbij zijn risico's gebleken. Zo wordt op basis van de interne pentest het risico dat de gemeente ten tijde van de test liep als hoog ingeschat. De ethisch hacker vond geen risico's in het wifi-netwerk. Uit de audit op de autorisaties en het wachtwoordenbeleid (Active Directory) komen wel kwetsbaarheden naar voren, die te maken hebben met het niet consequent toepassen van het wachtwoordbeleid. En tot slot liet het bezoek van de mystery guests risico's op een gemiddeld niveau zien.

[5] NOREA is de beroepsorganisatie van IT-auditors, die onder andere een scorekaart voor de volwassenheid op informatiebeveiliging heeft opgesteld (zie bijlage 5).

De resultaten van de testen door de rekenkamer zijn direct gedeeld met de CISO. De ethisch hacker heeft uitleg gegeven over diens bevindingen en mede op basis daarvan heeft de gemeente verbetermaatregelen getroffen.

Toegang tot gevoelige Informatie

De pentesten tonen dat er een kans bestaat op oneigenlijke toegang tot informatie binnen de gemeente. Van buitenaf is de toegang goed beveiligd met firewalls en virusscanners en intern zijn ook drempels opgeworpen. Toegang kan verkregen worden met twee factor authenticatie (2FA). Om verdacht verkeer op de systemen te kunnen monitoren en daarop te kunnen ingrijpen is een hardware matige oplossing gekozen, in afwachting van een geslaagde aanbesteding in VNG-verband van een applicatie (SIEM/SOC).

Logging

Logging betekent het vastleggen in zogenoemde logbestanden van wie toegang heeft gekregen tot informatie uit systemen. Er is een afweging gemaakt van welke applicaties het verkeer gelogd wordt en van welke niet. Die afweging heeft te maken met de beschikbare capaciteit om de loggingbestanden te checken en applicaties waarin veel bijzondere persoonsgegevens worden verwerkt. De controle op de informatie uit de logs en het vastleggen van de activiteiten behoeft verbetering.

Autorisaties

Medewerkers hebben autorisatie nodig om toegang tot informatie en applicaties te krijgen. Er is een proces vastgelegd waarbij de autorisaties worden toegekend en periodiek worden gecontroleerd. Voor een beperkt aantal applicaties is een autorisatiematrix aanwezig, waarmee de toekenning plaatsvindt op basis van rol en functie. De verdere uitrol van een dergelijke matrix staat voor 2024 op de planning. Uit de controles, onder andere van de accountant en in het kader van het rekenkamer-onderzoek, blijkt dat de juistheid van autorisaties een aandachtspunt is.

Conclusies

Voldoende geborgd, maar werk aan de winkel

In het algemeen concludeert de rekenkamer dat in de gemeente Zeist de informatieveiligheid voldoende geborgd is, dat wil zeggen dat het in overeenstemming is met de geldende normen. De situatie is vergelijkbaar met de meeste gemeenten.

Dat wil niet zeggen dat de gemeente Zeist achterover kan leunen. Er is nog werk aan de winkel, al timmert de gemeente op veel deelterreinen hard aan de weg. Op het gebied van informatiebeveiliging en privacy nemen de eisen die aan overheden worden gesteld toe, onder andere omdat de ontwikkelingen en bedreigingen rondom cybersecurity zeer turbulent zijn. Denk aan de toenemende mogelijkheden van Artificiële Intelligentie (AI) en aan geopolitieke actoren die baat kunnen hebben bij ontwrichting van digitale processen bij Nederlandse overheden. Criminelen zitten immers niet stil. Zij blijven zich ontwikkelen, waardoor nieuwe risico’s ontstaan of bestaande risico’s veranderen.

Organisatie voldoet aan de basis	Het beleid ten aanzien van informatieveiligheid en privacy is risicogestuurd en voldoet grotendeels aan de gestelde normen. Wel concludeert de rekenkamer dat een integraal risicomanagement nog niet gerealiseerd is in Zeist. De BIO schrijft een basisset aan normen voor waar overheden aan moeten voldoen. De rekenkamer constateert dat het gemeentelijk beleid ambitieuzer mag en verder mag reiken dan de voorgeschreven normen. De gemeente Zeist is op informatieveiligheid geen voorloper.
Doorvertaling beleid onvoldoende	Het strategisch beleid is geformuleerd. Er is meer inzet nodig bij de doorvertaling van het strategisch beleid naar de protocollen en richtlijnen op tactisch niveau en vooral naar de werkprocessen op operationeel niveau.
Functies voldoende bezet	De functies voor informatieveiligheid en privacy zijn voldoende bezet en er zijn voldoende overlegmomenten onderling en met het management en bestuur om effectief te zijn. De verwachting is dat de eisen die aan de organisatie en de bemensing worden gesteld toe zullen nemen. Gelet op de kwantitatieve en (op specialistische functies) kwalitatieve krapte op de arbeidsmarkt, is het een uitdaging om de juiste competenties binnen te halen en te behouden. Samenwerking met andere gemeenten kan een oplossing zijn. Voor een aantal functies op het gebied van ICT, informatieveiligheid en privacy werken gemeenten al geregeld samen.
Middelen voldoende, maar oncontroleerbaar	Er staan voldoende middelen voor informatieveiligheid ter beschikking voor de benodigde maatregelen. Maar oncontroleerbaar is of deze voldoen aan de norm die de Informatiebeveiligingsdienst (IBD) stelt, namelijk 10% van de middelen die de gemeente aan ICT besteedt.
Managementinformatie niet ten volle benut	De faciliteiten van het managementinformatiesysteem voor informatie-veiligheid (ISMS) worden nog niet ten volle benut. Dat betekent dat er een risico is op ineffectiviteit en inefficiëntie bij het plannen en vastleggen van activiteiten op informatieveiligheid en de onderliggende beleidsleercyclus (PDCA).
Testen laten risico's zien die opgepakt worden	Uit de testen die de rekenkamer heeft laten uitvoeren op de systemen en de fysieke veiligheid van de gemeente komen risico's naar voren. Net als bij de geconstateerde risico's uit eerdere testen (in opdracht van de gemeente zelf uitgevoerd) zijn de risico's vertaald naar verbeterplannen en opgepakt. Gelet op het feit dat er zich steeds nieuwe dreigingen voordoen vereist de BIO jaarlijkse testen op de gemeentelijke systemen.
Autorisaties aandachtspunt	Het werken met autorisaties voor toegang tot systemen en informatie is een aandachtspunt. Met name de uitrol van de tools en de controle op de correctheid van de autorisaties vraagt aandacht. De gemeente is van plan daar in 2024 actie op te ondernemen.
Aandacht voldoende, bewust-wording en taakvolwassen-heid behoeven aandacht	Uit het onderzoek blijkt dat er bij bestuur en management voldoende draagvlak is voor beleid ten aanzien van informatieveiligheid en privacy. Het risicobewustzijn bij de medewerkers en het lijnmanagement (de proces-eigenaren) neemt toe. Maar dat kan altijd beter. Het eigenaarschap ten

aanzien van informatieveiligheid wordt in de gemeentelijke organisatie niet overal gevoeld waar het volgens het beleid zou moeten liggen. De conclusie is dat ingezet moet worden op verhoging van de taakvolwassenheid van de medewerkers.

Gemeenteraad te weinig betrokken

Gelet op het bestuurlijke en financiële belang wordt de gemeenteraad nog te weinig betrokken bij kaderstelling en controle op informatieveiligheid en privacy. College en raad zijn te weinig onderling in gesprek over de risico's en de ambities op informatieveiligheid en de werking van het beleid.

Aanbevelingen

De bovenstaande conclusies leiden tot de volgende aanbevelingen aan het college en de raad.

Aanbevelingen aan het college

1. **Ga verder met activiteiten op het gebied van informatieveiligheid en privacy waar al een begin mee is gemaakt, zoals effectiever gebruik van de functionaliteit van het Informatiemanagementsysteem voor informatieveiligheid (ISMS), uitrol van de autorisatiematrix en logging, het testen van de systemen en de fysieke beveiliging en de aanpak van verbetermaatregelen die daaruit naar voren komen.**
   Blijf ook in de toekomst zorgen voor voldoende capaciteit in de lijn en ondersteuning daarvoor.

2. **Verstevig het investeren in activiteiten om het risicobewustzijn en de taakvolwassenheid van medewerkers te bevorderen.**

3. **Vervolledig het informatieveiligheidsbeleid op tactisch en operationeel niveau:**
   - **vul de nog ontbrekende protocollen en richtlijnen voor informatie-beveiliging en privacy in.** Een integraal continuïteitsplan is bijvoorbeeld een beleidsonderdeel op tactisch niveau dat nog niet is gerealiseerd.
   - **zorg dat protocollen en richtlijnen in de werkprocessen worden ingebed.** Daarmee wordt voldaan aan de BIO en wordt de daadwerkelijke werking van de maatregelen in praktijk bevorderd.

4. **Richt een structuur voor integraal risicomanagement in.**
   Bij Integraal risicomanagement gaat het gemeentebreed om de organisatie van risico-governance, -strategie, -beleid en -beheerprocessen, dus ook ten aanzien van informatieveiligheid en privacy in samenhang met andere terreinen. Dit past in het streven van het college om op termijn een 'in control-statement' af te kunnen geven.

Aanbevelingen aan college en raad

1. **Formuleer samen ambities op informatieveiligheid en privacy.**
   Ga na of het bestuurlijk en financieel haalbaar is een hoger ambitieniveau op informatieveiligheid na te streven, dan te voldoen aan de basis-maatregelen uit de BIO, om op die manier de toenemende risico's sneller aan te kunnen pakken. Concreet bijvoorbeeld: spreek af over welke periode de gemiddelde taakvolwassenheid van de medewerkers op een bepaald niveau moet zijn.

   Het is ook van belang dat er structureel voldoende middelen beschikbaar zijn om de activiteiten op informatiebeveiliging en privacy te financieren. Als richtlijn kan de 10%-norm van de ICT-kosten gelden zoals de IBD die sinds kort stelt. Deze middelen moeten traceerbaar zijn in de jaarrekening.

2. **Zorg ervoor dat de raad regelmatig geïnformeerd wordt over informatie-veiligheid en privacy en spreek af op welke wijze dat gebeurt.**
   Dat kan bijvoorbeeld halfjaarlijks diepgaand in een aparte raadscommissie of een commissie onder een bestaande commissie, naar aanleiding van de ENSIA-rapportages en de rapportages van de FG.[6]

[6] Zo heeft bijvoorbeeld de gemeente Hof van Twente een commissie op ICT onder de auditcommissie die regelmatig wordt gebriefd over de voortgang op de beveiligingsmaatregelen.

1 Inleiding

Gemeenten zijn kwetsbaar

Onder andere door de toegenomen taken in het sociaal domein beheren en verwerken gemeenten meer en meer persoonsgegevens en gevoelige data. Dat doen gemeenten in toenemende mate met behulp van digitale hulpmiddelen. Gemeenten zijn daarbij kwetsbaar gebleken, zoals onder andere blijkt uit datalekken bij gemeenten, zoals Hof van Twente.

Wat gebeurt er bijvoorbeeld als gevoelige informatie op straat komt te liggen of op het dark web[7] wordt aangeboden? Of als de gegevens worden gegijzeld en de digitale dienstverlening aan burgers niet meer mogelijk is?[8] Naast ernstige financiële, juridische en technische gevolgen kunnen deze crises de privacy van burgers en het imago van de gemeente aantasten.[9]

Dat zijn redenen voor de Rekenkamer Zeist geweest om een onderzoek te doen naar de opzet, het bestaan en de werking van het informatie-beveiliging- en privacybeleid in de gemeente Zeist. Dat onderzoek is in november en december 2023 uitgevoerd.

De Rekenkamer bedankt de ambtelijke organisatie, met name de medewerkers van de afdeling Informatievoorziening (IV), voor de medewerking die de onderzoekers tijdens de loop van het onderzoek hebben ervaren.

Hieronder gaan we in op doelstelling en onderzoeksvragen en de aanpak.

Leeswijzer

In hoofdstuk 2 behandelen we de doelstelling, onderzoeksvragen en de aanpak van het onderzoek. De hoofdstukken 3 tot en met 11 bevatten de bevindingen, geordend aan de hand van de onderzoeksvragen. De bevindingen zijn getoetst in het kader van de ambtelijke hoor en wederhoor.

In bijlage 1 zijn de meest gebruikte termen en afkortingen uitgelegd die voorkomen op het gebied van informatiebeveiliging en privacy. Het is nu eenmaal een sector die veel gebruik maakt van voornamelijk Engelstalige termen. In bijlage 2 komen de normen aan bod, gekoppeld aan de

---

7 Het dark web is de diepste en verborgen laag van het internet. Het is onderdeel van het ‘deep web’, omdat het niet toegankelijk is via reguliere zoekmachines. Het staat bekend als een plek waar illegale activiteiten plaatsvinden. Hoewel dit inderdaad gebeurt, bestaat het uit meer dan alleen illegale sites.

8 Ransomware is malware (software met kwaadaardige bedoelingen) die de databestanden van gebruikers versleutelt, met als doel om deze later te ontsleutelen in ruil voor losgeld.

9 Gemeenten hebben in 2013 in VNG-verband afgesproken te voldoen aan de maatregelen van de Baseline Informatiebeveiliging Gemeenten (BIG). De BIG is vanaf 2020 vervangen door de Baseline Informatiebeveiliging Overheid (BIO.) In 2021 hebben gemeenten in VNG-verband afgesproken structureel voldoende middelen voor de weerbaarheid tegen digitale bedreigingen vrij te maken.
Vanaf 25 mei 2016 schrijft de Algemene Verordening Gegevensbescherming (AVG of GDPR) voor dat passende maatregelen getroffen moeten worden om persoonsgegevens te beveiligen, in het belang van de burger en de gemeenten zelf.

onderzoeksvragen. In bijlage 3 is de lijst opgenomen met geraadpleegde stukken en de lijst met functies van de respondenten.

Vervolgens is in bijlage 4 een afbeelding opgenomen van de verschillende richtlijnen en procedures die in het tactische informatiebeveiligings- en privacybeleid worden gehanteerd. In hoofdstuk 5 wordt verwezen naar het volwassenheidsniveau zoals gehanteerd door de beroepsorganisatie van IT-auditors in Nederland (de Nederlandse Organisatie van Register EDP-Auditors, NOREA.). Daarom is deze in een tabel in bijlage 5 opgenomen.

2 Doelstelling en onderzoeksvragen

In dit hoofdstuk gaan we in op de doelstelling, de onderzoeksvragen en de aanpak van het onderzoek. In §2.2 geven we een korte inleiding op het gebied van informatiebeveiliging en privacy.

2.1 Doelstelling en onderzoeksvragen

Hoofdvraag en doelstelling

De rekenkamer wil het onderzoek op drie aspecten richten: techniek, organisatie en beleid, en mens en gedrag. Met het onderzoek wordt de volgende hoofdvraag beantwoord:

''Is de informatieveiligheid bij de gemeente Zeist voldoende gewaarborgd?''

De Rekenkamer wil in de breedte inzicht krijgen in de stand van de informatieveiligheid in de gemeente en daarbij terecht focussen op organisatie/proces, mens en techniek (zie hiervoor de inleiding op informatieveiligheid en privacy in §2.2).

Onderzoeksvragen

Deze hoofdvraag werken we uit, mede op basis van het offerteverzoek, naar de onderzoeksvragen zoals opgenomen in onderstaande tabel 1.

Tabel 1. Onderzoeksvragen

1.	**Heeft de gemeente Zeist op informatieveiligheid de risico's voldoende in kaart gebracht en op basis daarvan beleid geformuleerd?**
2.	**Wordt de gemeenteraad goed geïnformeerd over de risico's en beheersingsmaatregelen?**
3.	**Krijgen medewerkers goede uitleg en ondersteuning om veilig te werken?**
4.	**Hoe communiceert de gemeente met betrokkenen en inwoners over datalekken?**
5.	**Hoe controleert de gemeente op naleving van veilig werken en het voorkomen van beveiligingsincidenten?**
6.	**Welke penetratietesten voerde de gemeente uit? Zo ja, zijn verbeterplannen opgesteld naar aanleiding van de pentesten en zijn deze opgevolgd?**
7.	**Is het mogelijk om oneigenlijke toegang te krijgen tot gevoelige informatie die de gemeente in beheer heeft?**
8.	**In hoeverre wordt in de organisatie van de gemeente Zeist vastgelegd wie wanneer toegang vraagt tot bestanden met gevoelige informatie (het loggen)?**
9.	**Hoe is het autorisatiebeleid vorm gegeven?**
10.	**Welke adviezen zijn te geven aan college, gemeentelijke organisatie en de gemeenteraad?**

Voor de normen die we gebruiken om de antwoorden op bovenstaande vragen te beoordelen verwijzen we naar bijlage 2. De hoofdstukken 3 tot en met 11 bevatten de antwoorden op de onderzoeksvragen 1 tot en met 9. Onderzoeksvraag 10 wordt in de inleidende paragrafen conclusies en aanbevelingen beantwoord.

2.2 Korte inleiding op informatiebeveiliging en privacy

Informatiebeveiliging

Informatiebeveiliging gaat over het geheel aan preventieve, detectieve (opsporings-) en correctieve maatregelen, procedures en processen die de beschikbaarheid, integriteit en vertrouwelijkheid (BIV) van de informatie binnen een organisatie garanderen. Doel is de continuïteit van de informatie en de informatievoorziening of dienstverlening te waarborgen en eventuele gevolgen van (beveiligings)incidenten te beperken. Het beleid dat gemeenten hierop hebben afgesproken is neergelegd in de Baseline Informatiebeveiliging Overheid (BIO).[10] De BIO bevat maatregelen die gemeenten op basis van een risicoanalyse kunnen nemen om aan het basisniveau voor informatiebeveiliging te voldoen. De Network and Information Security Directive 2 (NIS2) is Europese wetgeving die de richtlijnen van de BIO vanaf oktober 2024 verplicht stelt voor overheidsorganisaties, dus ook voor gemeenten.

Gegevensbescherming

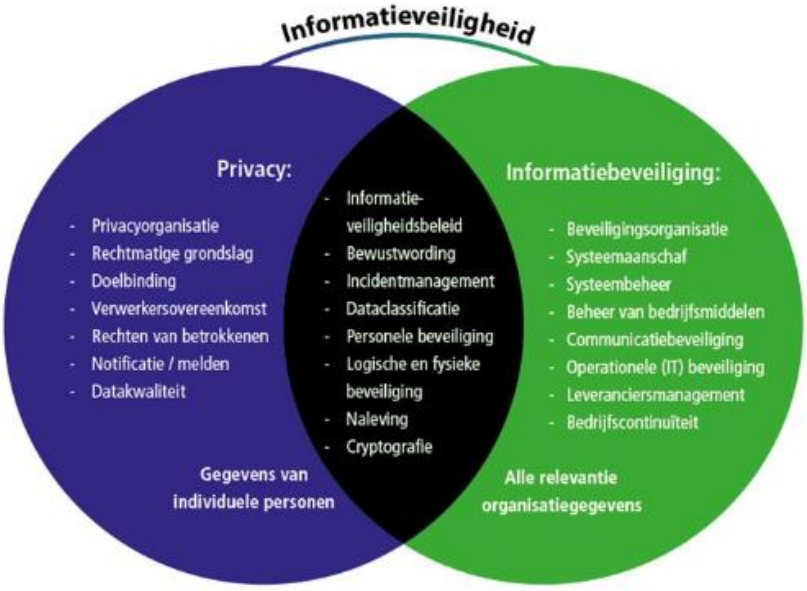
Gegevensbescherming betreft de regels voor de verwerking van persoonsgegevens door bedrijven, instellingen en overheden. Doel is de privacy van burgers op een adequate manier te beschermen. De Europese General Data Protection Regulation (GDPR), in Nederland bekend als de Algemene Verordening Gegevensbescherming (AVG), is sinds mei 2018 van kracht.

Informatieveiligheid

De AVG schrijft onder andere voor dat passende maatregelen getroffen moeten worden om persoonsgegevens te beveiligen, in het belang van de burger en de gemeenten zelf. De twee onderwerpen informatiebeveiliging en gegevensbescherming (privacy) hebben dus onderling een grote overlap. Een deel van de protocollen en procedures op beide terreinen komt met elkaar overeen. Overkoepelend wordt vaak de term informatieveiligheid gebruikt, zie onderstaand afbeelding 2.1.

[10] Gemeenten hebben in 2013 in VNG-verband afgesproken te voldoen aan de maatregelen van de Baseline Informatie-beveiliging Gemeenten (BIG). De BIG is vanaf 2020 vervangen door de Baseline Informatiebeveiliging Overheid (BIO). De baseline is gebaseerd op de kwaliteitsnormen NEN-ISO/IEC 27001:2017 en de NEN-ISO/IEC 27002:2017.

Afbeelding 2.1. Informatieveiligheid met privacy en informatiebeveiliging.

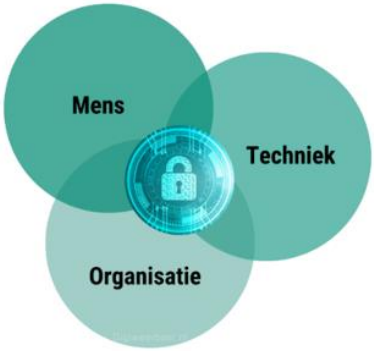


Bron: Rekenkamer Utrecht, 2021.

In dit onderzoek komen beide onderwerpen (informatiebeveiliging en privacy) aan bod. In bijlage 4 is visueel gemaakt hoe de richtlijnen en protocollen op informatiebeveiliging en privacy onderling samenhangen.

Mens, techniek, organisatie

Informatieveiligheid wordt vaak nog enkel vanuit een technische invalshoek benaderd. De ervaring leert evenwel dat technische oplossingen te organiseren zijn, hoewel deze natuurlijk ook de praktische (pen)testen moeten doorstaan ("the proof of the pudding is in the eating"). Naast techniek zijn mens en organisatie essentieel bij informatiebeveiliging en privacy. Cruciale factoren die de informatieveiligheid bepalen zijn houding en gedrag van de menselijke actor, kortom bewustwording op risico's bij medewerkers en lijnmanagement. Ook moeten de organisatorische rand-voorwaarden gecreëerd zijn om techniek en mens te ondersteunen. Beleid en protocollen moeten daarvoor opgesteld en vastgesteld zijn (voor een gedeeltelijk overzicht van de protocollen op informatiebeveiliging en privacy zie afbeelding 3.1) en in de praktijk worden toegepast. Om dat optimaal te laten slagen moet beleid op informatiebeveiliging en privacy gedragen en uitgedragen worden door bestuur en directie van de gemeente.



2.3 Aanpak

Methoden

De onderzoeksvragen worden beantwoord door middel van een analyse van documenten in deskresearch, interviewverslagen en pentesten. De documenten bevatten beleid en rapportages van de gemeente. De

documenten die zijn bestudeerd zijn in bijlage 3 opgenomen, evenals de functies van de bestuurders en functionarissen van de gemeente Zeist die zijn geïnterviewd. De deskresearch vond plaats in de periode oktober-november 2023. De interviews zijn in november 2023 afgenomen.

Pentesten

In oktober en november 2023 zijn in het kader van het rekenkamer-onderzoek verschillende pentesten uitgevoerd op de systemen.[11] Door de gemeente zijn eerder pentesten uitgevoerd, de laatste in 2021. De resultaten van deze test zijn gedeeld met de rekenkamer.

In een vroeg stadium is door de rekenkamer en de onderzoeker overleg gevoerd met ambtenaren over de scope van de testen in het kader van het rekenkameronderzoek. Besloten is een interne netwerk test, een wifi netwerk test, een Active Directory (AD) audit en een inlooptest met mystery guests uit te voeren. Daartoe is besloten, deels omdat deze testen nog niet of lang geleden zijn uitgevoerd, deels deze een goed beeld geven van de veiligheid van de systemen. Voor een nadere uitleg van deze testen en de resultaten zie §8.1.

Ook zijn in het kader van het rekenkameronderzoek phishing mails verstuurd naar medewerkers van de gemeente.[12] De laatste phishing mail simulatie in opdracht van de gemeente zelf is uit 2022. Voor een uitleg van deze test en de resultaten zie §5.1.

De nota van bevindingen is in maart 2024 voor de ambtelijke hoor en wederhoor (feitencheck) aangeboden. Het definitieve rapport is op 16 april 2024 voor de bestuurlijke hoor en wederhoor aan het College van B&W aangeboden.

[11] Een pentest of penetratietest is een toets van een of meer computersystemen op kwetsbaarheden, waarbij deze kwetsbaarheden gebruikt kunnen worden om in deze systemen in te breken.

[12] Phishing is een vorm van internet oplichting en fraude, door middel van een vals e-mail bericht 'hengelen' naar inlog- of andere persoonsgegevens.

3 Risico in beeld en in beleid

Onderzoeksvraag 1	Heeft de gemeente Zeist op informatieveiligheid de risico's voldoende in kaart gebracht en op basis daarvan beleid geformuleerd?

BIO

In dit hoofdstuk gaan we in op het beleid op informatieveiligheid van de gemeente Zeist. Daarbij gaan we ook in op het beleid op gegevens-bescherming of privacy. De Baseline Informatiebeveiliging Gemeenten (BIG) legde tot en met 2019 de basis onder het informatieveiligheidsbeleid van gemeenten met een aantal beheersmaatregelen. De Baseline Informatie-beveiliging Overheid (BIO) is vanaf 2020 de geldende baseline voor de gehele overheid. De BIO is meer dan diens voorganger gebaseerd op risicomanagement. Daarvoor worden GAP-analyses[13] gehouden om te bepalen in hoeverre de gemeente voldoet aan de maatregelen in de BIO. Als er maatregelen ontbreken dient een risicoanalyse te worden uitgevoerd om te bepalen welke maatregelen met prioriteit worden opgepakt en welke risico's vooralsnog geaccepteerd worden.

Samenwerking op ICT met

De gemeente Zeist werkt met Nieuwegein samen op ICT-gebied. Zeist heeft zich niet aangesloten bij RID-Utrecht, de regionale ICT-dienstverlener, waarbij zes gemeenten en één sociale dienst zijn aangesloten. Zeist en Nieuwegein hebben een gezamenlijk datacenter in gebruik genomen, met een wederzijdse uitwijk, mochten de systemen van een van de gemeenten het begeven. De beide serverparken zijn van elkaar gescheiden en worden onderhouden door een externe partij. Zoals omschreven in de woorden van een van de respondenten is de gemeente nog een klassieke ICT-organisatie, die zoals meer gemeentelijke overheden de ambitie heeft om naar de 'cloud' te migreren.[14]

Beleidscyclus

Het informatieveiligheidsbeleid van de gemeente moet risicogestuurd zijn, zoals de BIO voorschrijft. De beleidscyclus van een gemeente ziet er als volgt uit. Overkoepelend is er het strategische informatieveiligheidsbeleid, waarin de doelen, rollen en functies op informatieveiligheid zijn beschreven. Dit beleid wordt om de 3 tot 4 jaar vastgesteld door het College van B&W. Daaronder ligt het tactische informatieveiligheidsbeleid, dat een groot aantal richtlijnen en protocollen bevat op informatie-veiligheid. Deze worden in samenhang met andere beleidsterreinen opgesteld, zoals het privacy- of gegevensbeschermingsbeleid. De overlap op richtlijnen en protocollen met dat terrein is inzichtelijk in afbeelding 2.1 en

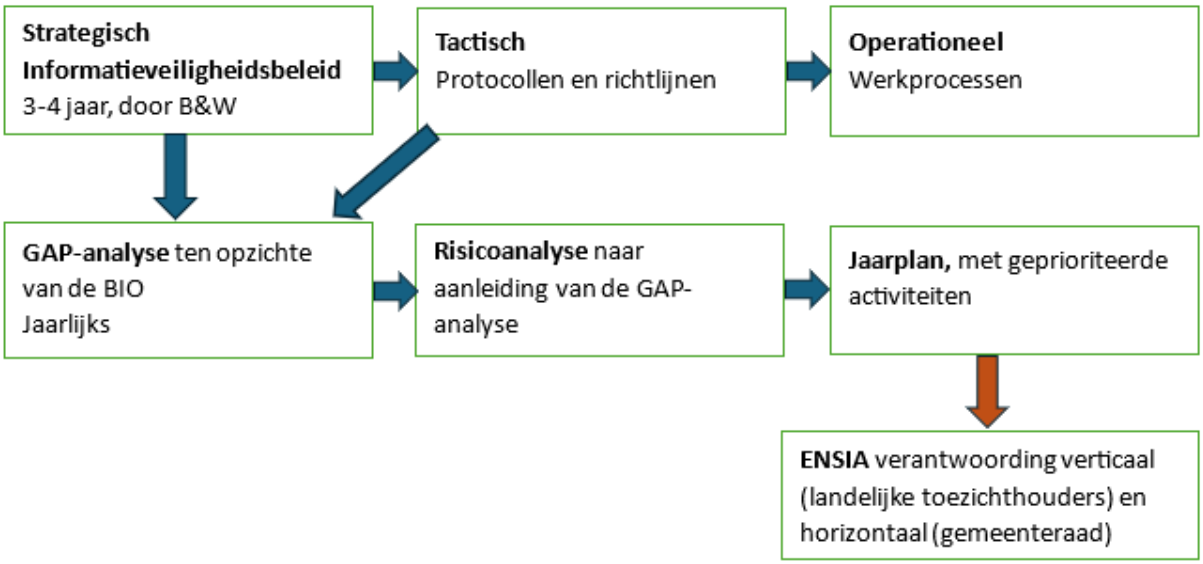
[13] GAP is de Engelse term voor 'kloof'. Dat betekent hier het verschil tussen de bestaande situatie en de gewenste situatie. GAP-analyse is de check of en in welke mate de maatregelen uit de BIO geïmplementeerd zijn.

[14] Bij migratie naar de cloud worden applicaties en gegevens van de ene locatie naar de servers van een provider van een cloud op internet verplaatst. De voordelen van cloudmigratie zijn het verminderen van de IT-kosten, maar ook op het gebied van onder andere beveiliging biedt het voordelen.

de afbeelding in bijlage 4. Tot slot moeten de verschillende protocollen en richtlijnen in procesbeschrijvingen hun neerslag krijgen en daarmee op operationeel niveau geborgd worden.

Concrete jaarplannen dienen te worden opgesteld naar aanleiding van een analyse van de kloof tussen wat er onder andere aan protocollen, richtlijnen en activiteiten aanwezig is en wat er aanwezig zou moeten zijn (een GAP-analyse). Het MT stelt de jaarplannen vast. Een risicoanalyse bepaalt de urgentie van de in het jaarplan op te nemen activiteiten en welke risico's voorlopig geaccepteerd worden. Over de uitvoering wordt door het College door middel van ENSIA (de Eenduidige Normatiek Single Information Audit) jaarlijks gerapporteerd aan de raad en de landelijke toezichthouders, zie daarvoor hoofdstuk 4.

Schema 3.1. Beleidscyclus Informatieveiligheid.



3.1 Beleid

Strategisch beleid

Het strategisch informatieveiligheidsbeleid van de gemeente Zeist voor de periode 2022-2026 is op 8-12-2022 door het College van B&W vastgesteld. Tegelijk is het privacybeleid voor dezelfde periode vastgesteld. De strategische stukken verwijzen naar dezelfde uitgangspunten, vooruitlopend op de in 2023 geformuleerde beleidsstukken in 'Een goed leven in Zeist – ook digitaal' en de ICT-visie 2030. De ambitie uit het informatieveiligheidsbeleid is als volgt weer te geven: voortdurend verbeteren, een goed en betrouwbaar functionerende informatievoorziening en een hoog volwassenheidsniveau dat niet op elk proces even hoog hoeft te zijn. Met betrouwbaar wordt bedoeld dat gegevens en informatie die de gemeente verwerkt beschikbaar (continuïteit van bedrijfsvoering), integer (juist en volledig) en vertrouwelijk (alleen geautoriseerd gebruik) is.

Strategische doelen

In het strategische beleidsstuk wordt gerefereerd aan de 10 bestuurlijke principes voor informatieveiligheid en het dreigingsbeeld van de Informatiebeveiligingsdienst Dienst (IBD). De strategische doelen van het beleid zijn als volgt geformuleerd:

- het managen van de Informatieveiligheid;
- adequate bescherming van bedrijfsmiddelen;
- het minimaliseren van risico's van menselijk gedrag;
- het voorkomen van ongeautoriseerde toegang;
- het garanderen van correcte en veilige informatievoorzieningen;
- het beheersen van de toegang tot informatiesystemen;
- het waarborgen van veilige informatiesystemen;
- het adequaat reageren op incidenten;
- het beschermen van kritieke bedrijfsprocessen;
- het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers;
- transparantie over incidenten; [15]
- het waarborgen van de naleving van dit beleid.

Grondslag en ambities

Aan het beleid en de ambities liggen verschillende beleids-, visie- en ambitiestukken ten grondslag over informatieveiligheid en privacy. Dat is een doorgaand proces, dat niet ophoudt op het moment dat het strategische beleid eenmaal is vastgesteld. Daarvoor verandert de omgeving op informatieveiligheid te onstuimig en er komen steeds nieuwe bedreigingen bij. Maar ook nieuwe kansen en mogelijkheden om de bedreigingen het hoofd te bieden. Tot de beleids- en visiestukken behoren onder andere de Bestuurlijke rapportage informatieveiligheid 2020, "Weerbaarder verder... Beleid Informatieveiligheid & privacy" 2020, 'Het goede leven in Zeist – ook digitaal' 2023 en een nog vast te stellen 'ICT-visie 2030'. Het laatste visiestuk is niet bestudeerd door de rekenkamer. De ambities in de bestudeerde stukken zijn grotendeels het volgen van het landelijke beleid. Terwijl in de interviews hogere ambities worden uitgesproken, zoals als gemeente op gebied van informatieveiligheid en privacy voorloper willen zijn. Die ambitie heeft zich nog niet vertaald naar het geformuleerde beleid.

Uitgangspunt

Uitgangspunten van het informatieveiligheidsbeleid in Zeist zijn de sturing op risico's, verdeling van verantwoordelijkheden en rollen op basis van het RASCI-model en het 3-lijnenmodel ('3-lines of defence'). RASCI verdeelt de verantwoordelijkheden en rollen naar

- verantwoordelijk (Responsible) >
- eindverantwoordelijk (Accountable) >
- ondersteunend (Supportive) >
- toezicht (Consulted) >
- geïnformeerd (Informed)

[15] Het betreft transparantie en open communicatie met betrekking tot cybersecurity-incidenten.

Binnen het 3-lijnenmodel wordt kortweg onderscheid gemaakt tussen operationeel niveau, ondersteuning en toezicht. De eerste lijn van verdediging tegen bedreigingen bestaat uit de proceseigenaren/-lijnmanagement en de medewerkers verantwoordelijken in de lijn (Responsible) en de eindverantwoordelijken (Accountable). In het verlengde van deze lijn zijn er de externe uitvoeringsorganisaties. De tweede lijn bestaat uit de professionals die de eerste lijn ondersteunen op informatieveiligheid en privacy. Tot slot bestaat de derde lijn uit het toezicht, waaronder de Functionaris Gegevensbescherming. In het model dat Zeist hanteert is een vierde lijn ingebracht, 'Informed', met onder andere inwoners, gemeenteraad, accountant en de Autoriteit Persoons-gegevens. Deze rolverdeling en toewijzing van verantwoordelijkheden ook in het visiestuk 'Het goede leven in Zeist – ook digitaal' opgenomen.

Tabel 3.1. Verantwoordelijkheden belegd op basis van RASCI-model en 3-lijnenmodel

RASCI	3 Lines of Defence (LoD)	Rolverdeling
R – Responsible (operationeel verantwoordelijk)	1e lijn	- Proceseigenaren - Medewerkers - Uitvoeringsorganisaties ('verwerkers')
A – Accountable (bestuurlijk eindverantwoordelijk)	1e lijn	- Het college (verwerkingsverantwoordelijke)
S – Supportive (ondersteunend)	2e lijn	- Team Veilig werken, ICT, informatieveiligheid, Inkoop, JZ, risk- en kwaliteitsmanagement
C – Consulted / Toezicht (Iemand die geraadpleegd wordt)	3e lijn	- Functionaris Gegevensbescherming (FG) (in samenwerking met audit)
I – Informed (Iemand die geïnformeerd wordt)	4e lijn	- Inwoners, De raad, Accountant; - Autoriteit Persoonsgegevens (AP)

In het strategisch beleid is op praktisch niveau de volgende lijn vastgelegd: een borging in het de PDCA-cyclus (Plan-Do-Check-Act) met een risico-beheersing op basis van achtereenvolgens een GAP-analyse, een impact analyse en prioritering van actiepunten/activiteiten/maatregelen.[16]

Tactisch beleid nog niet geheel volledig

Onder het strategische beleid ligt het beleid op tactisch niveau, waarin de strategische uitgangspunten in richtlijnen en protocollen op de verschillende deelterreinen van informatieveiligheid en privacy zijn uitgewerkt. Daarbij is te denken aan een uitgeschreven wachtwoorden-beleid, encryptiebeleid,[17] wijzigingsmanagement, leveranciersmanagement,

16 GAP is de Engelse term voor 'kloof'. Dat betekent hier het verschil tussen de bestaande situatie en de gewenste situatie. GAP-analyse is de check of en in welke mate de maatregelen uit de BIO geïmplementeerd zijn.

17 Encryptie of versleuteling is een methode om gegevens te coderen.

devicemanagement enz. Bijlage 4 geeft een gedeeltelijk overzicht van de in de BIO voorgeschreven richtlijnen en protocollen.

Zo schrijft de BIO voor dat er een integraal bedrijfscontinuïteitsplan moet worden opgesteld. Er is een continuïteitsplan aanwezig, maar dat is vooral vanuit de afdeling Informatievoorziening (IV) opgesteld. Continuïteit in de breedte is er niet, met bijvoorbeeld personele richtlijnen bij een calamiteit en afspraken met de Veiligheidsregio. Zo zijn er nog lacunes in het arsenaal aan tactische beleidsstukken, waar de organisatie mee aan de slag is om aan de eisen van de BIO te voldoen.

Doorvertaling naar operationeel gebied nog onvolledig

Op operationeel gebied ontbreekt het aan procesbeschrijvingen waarin de verschillende stappen waar aspecten op informatieveiligheid en privacy meespelen zijn opgenomen. In 2022 heeft de gemeente een consultant ingehuurd om de verschillende processen op het gebied van gegevensbescherming (privacy) te beschrijven en eventuele lacunes vast te stellen. Eind 2023 was een aantal processen in conceptversie met hoofd van de afdeling Informatievoorziening en de betreffende proceseigenaar besproken. De borging van deze processen staat voor 2024 in de planning.

In 2023 is een kwaliteitsmedewerker aangenomen die hetzelfde moet doen op het gebied van informatieveiligheid. De ambitie is dat dit in het tweede kwartaal van 2024 gerealiseerd is. Uit de stukken en de interviews blijkt dat de doorvertaling van het strategische naar tactisch en operationeel niveau nog niet volledig is.

Dat betekent dat nog niet alle activiteiten op informatieveiligheid en gegevensbescherming vastliggen in procesbeschrijvingen voor de werkvloer. Dat kan verstoringen in werkprocessen tot gevolg hebben. Bijvoorbeeld als tijdens de laatste fase van een proces duidelijk wordt dat stappen zijn overgeslagen, bijvoorbeeld de uitvoering van een data protection impact assessment (dpia)[18] op een verwerkingsproces. Bijkomend risico is dat activiteiten niet goed vastgelegd of geborgd worden. Daarop zijn nog stappen te zetten door de gemeente.

Jaarplannen zijn aanwezig

Het beleid van de gemeente Zeist is risicogestuurd, zoals de BIO voorschrijft. Voor 2021-2022 heeft de gemeente naar aanleiding van de ENSIA 2020 een risicoanalyse uitgevoerd. Onderzocht wordt in welke mate de gemeente de BIO-maatregelen heeft geïmplementeerd. De beheersmaatregelen die daaruit met prioriteit naar voren kwamen zijn in het Jaarplan 2021-2022 opgenomen. Daartoe behoren onder andere de implementatie van een wachtwoordkluis, professionalisering van het wijzigingenbeheer, monitoring op het netwerkverkeer (SIEM/SOC [19]) en continuïteitsmanagement.

[18] Data protection impact assessment (dpia) is een analyse op risico's in verband met privacy en gegevensbescherming bij verwerkingsprocessen. Onder de AVG verplicht bij gegevensverwerking met waarschijnlijk een hoog privacy risico.

[19] Zie ook §8.3.

In januari 2023 is naast een jaarplan een Verklaring van toepasselijkheid (VVT) opgesteld, bedoeld voor het bestuur, directie, lijn- en stafmanagers, auditors en externe toezichthouders. Deze verklaring geeft inzicht in hoeverre de BIO-normen zijn geïmplementeerd. Het is daarmee min of meer gelijk aan een risicoanalyse, en gesteld wordt dat de VVT door de proceseigenaren geactualiseerd moet worden. Uit een van de interviews blijkt dat de vastlegging van de activiteiten niet geheel voldoet aan de verwachtingen, in tegenstelling tot een jaarplan. De bedoeling is weer terug te keren naar de systematiek van risicoanalyse en op basis daarvan activiteiten opnemen in een jaarplan.

Middelen beschikbaar als noodzaak is aangetoond

Onderdeel van het informatieveiligheidsbeleid is uiteraard ook de middelen die ermee gemoeid zijn. Investeren in informatieveiligheid is vaak een lastig discussiepunt, het wordt nooit helemaal duidelijk of de gedane investeringen effectief of efficiënt zijn. Het enige dat vaak achteraf geconstateerd kan worden is dat de investering te laag is geweest als blijkt dat een ransomware aanval succesvol is geweest. De IBD gaat uit van de vuistregel van een investering in informatiebeveiliging van ongeveer 10% van de ICT-kosten.

Die middelen gaan aan allerlei verschillende posten op, van personeel tot en met trainingen en pentesten. Dat is niet afgebakend uit de begroting of jaarverslagen te destilleren en de respondenten hebben ook niet een dergelijk overzicht. Wel geven respondenten aan dat de middelen beschikbaar worden gemaakt als zij de noodzaak van te nemen maatregelen aantonen. Ook uit het bestuurlijke ‘peer to peer’ gesprek onder leiding van de VNG blijkt dat het College nooit geaarzeld heeft middelen vrij te maken voor ICT en bedrijfscontinuïteit.

3.2 Functionarissen

In het strategisch beleid zijn de rollen en verantwoordelijkheden op informatieveiligheid en privacy beschreven. Hieronder gaan we in op de bezetting van de functies op de twee terreinen.

Chief Information Security Officer (CISO)

Op informatieveiligheid vervult de fulltime strategisch informatieadviseur CISO-taken (Chief Information Security Officer) en lis gepositioneerd bij de afdeling Informatievoorziening (IV). Als aandachtsgebied heeft deze strategisch informatieadviseur Informatieveiligheid, Gegevensbescherming en Cybersecurity. De inzet als CISO op informatieveiligheid is wisselend en niet afgebakend. Het is moeilijk in te schatten hoeveel tijd van de fulltime functie aan informatieveiligheid wordt besteed. Tot de taken van de informatieadviseur horen het opstellen van visiedocumenten op informatieveiligheid en gegevensbescherming, ondersteuning aan de proceseigenaren, deelname aan overleggen op

strategisch en tactisch niveau. De CISO is voorzitter van het Meldpunt Datalekken.

De Informatiebeveiligingsdienst van de VNG (IBD) stelt dat de CISO een belangrijke en onafhankelijk van de lijn te positioneren functie heeft. De CISO valt onder de afdeling IV en zou via de hiërarchische lijn moeten communiceren met de portefeuillehouder en gemeentesecretaris. Uit de interviews blijkt dat dit spanningsveld nauwelijks aanwezig is. De CISO pakt de eigen rol op en heeft een directe eigen lijn naar het hoogste bestuurlijk en directieniveau. Zie ook de volgende paragraaf, §3.3.

Privacyofficer (PO)

De Privacyofficer (PO) vormt een brug tussen informatieveiligheid en privacy. Deze is werkzaam bij de afdeling Informatievoorziening (IV), sinds kort fulltime. De taken van de PO omvat de ondersteuning aan proceseigenaren, bijhouden van het verwerkingsregister en check op verwerkingsovereenkomsten en het uitvoeren van quick scans op verwerkingsprocessen[20]. De PO is net als de CISO aangesloten op het Meldpunt Datalekken (zie ook hoofdstuk 6 'Communicatie over datalekken').

Coördinator

Bij de afdeling Informatievoorziening (IV) is fulltime een coördinator werkzaam op functioneel beheer, technisch beheer en veilig werken op informatieveiligheid en privacy. Hij is tevens de coördinator van de rapportages in het kader van de Eenduidige Normatiek Single Information Audit (ENSIA, zie ook hoofdstuk 4). Dat zijn de jaarlijkse rapportages op informatieveiligheid en gegevensbescherming aan de landelijke toezichthouders en de gemeenteraad.

Functionaris gegevens-bescherming (FG)

Sinds vorig jaar is de Functionaris gegevensbescherming (FG) extern ingehuurd. Het is gebruikelijk bij gemeenten dat deze functie extern wordt ingevuld. De FG toetst steekproefsgewijs het beleid, de procedures en de maatregelen op gegevensbescherming. Jaarlijks rapporteert de FG aan college en de raad over opzet, bestaan en werking van het beleid.

Chief Information Officer (CIO)

Vanaf begin 2024 is het hoofd van de afdeling Informatievoorziening (IV) als Chief Information Officer (CIO) toegevoegd als lid van het directieteam (DT). Daarmee is vanuit informatievoorziening een directe link naar het DT gerealiseerd.

Informatieadviseur IV

Bij de afdeling IV zijn drie informatieadviseurs werkzaam. Eén van de strategische adviseurs heeft de rol van CISO (zie hiervoor). Een ander is gericht op ICT-infrastructuur en werkplekken, en heeft de rol van technisch adviseur security. Deze is onder andere verantwoordelijk voor beveiligings-maatregelen naar aanleiding van adviezen of incidenten en ondersteuning en advies op informatiebeveiliging en gegevensverwerking. De derde heeft als aandachtsgebied informatiemanagement.

[20] Quick scans zijn bedoeld om het risiconiveau van verwerkingsprocessen te bepalen en te bezien of een data protection impact assessment (dpia) uitgevoerd moet worden (zie ook hoofdstuk 7).

Kwaliteitsmedewerker AVG

Voor onder andere de procesbeschrijvingen op informatieveiligheid en privacy is sinds kort een kwaliteitsmedewerker AVG (Algemene Verordening Gegevensbescherming)[21] werkzaam. Deze is fulltime aan de slag, in samenwerking met lijnmanagement en medewerkers, met de vertaling van strategisch beleid naar tactisch en operationeel niveau.

Daarmee zijn de belangrijkste functionarissen op informatieveiligheid en gegevensbescherming, in de tweede en derde lijn volgens het 3 lijnen-model, in beeld gebracht. Volgens de respondenten voldoet de bezetting aan de eisen en de ambities die de gemeente heeft. Tegelijkertijd geven respondenten aan dat als er meer formatie zou zijn, meer aandacht naar bijvoorbeeld de doorvertaling van beleid op strategisch naar tactisch en operationeel niveau en de borging van processen zou kunnen gaan. De verwachting in algemene zin is ook dat de omgeving zich snel en turbulent ontwikkelt, met name op informatieveiligheid, waardoor de eisen aan personeel in de nabije toekomst hoger worden.

3.3 Overleggen op informatieveiligheid en privacy

Informatieveiligheid en privacy komen als onderwerpen langs in veel interne en enkele externe overleggen, op de verschillende niveaus in de gemeentelijke organisatie. Hieronder passeren deze de revue.

Strategisch informatie-veiligheidsoverleg

Hierin overleggen de CISO, hoofd afdeling Informatievoorziening (IV) en de informatieadviseur tweemaandelijks met elkaar over de grote lijnen en hoe de portefeuillehouder, gemeentesecretaris en DT geïnformeerd gaan worden. Zo wordt onder andere de ICT-visie 2030 besproken. De FG kan bij dit overleg aansluiten, indien nodig of gewenst.

Overleg met portefeuille-houder

Op strategisch niveau heeft de portefeuillehouder twee keer per jaar overleg over informatieveiligheid met de CISO, het hoofd van de afdeling IV, en de gemeentesecretaris (SIVO). Daarnaast heeft de CISO tweewekelijks een 1-op-1 overleg met de portefeuillehouder en sinds kort een structureel periodiek overleg met de gemeentesecretaris. De FG overlegt twee keer per jaar met de portefeuillehouder. Het hoofd van de afdeling IV heeft vanuit zijn bredere rol ook een tweewekelijks overleg met de portefeuillehouder en de CISO, waarin informatieveiligheid en privacy ook ter sprake komen.

Subopgaven afdeling IV

Binnen de afdeling hebben de functionarissen op informatieveiligheid en privacy elke twee tot drie weken overleg op tactisch niveau, subopgave ‘Veilig Werken’. Daarin bespreken zij de jaarplannen en de voortgang op de implementatie van de maatregelen die daarin zijn opgenomen. Daarnaast is er de subopgave ‘ICT in control’ met de systeembeheerder, informatie-adviseur en de helpdesk. Deze subopgave is meer op de techniek gericht, zoals het inrichten van wijzigingsbeheer (changemanagement).

[21] Algemene Verordening Gegevensbescherming (AVG), is Europese regelgeving die vanaf 2018 de privacyregels in de Europese lidstaten harmoniseert. Ook bekend onder de naam General Data Protection Regulation (GDPR).

Team Informatie en privacy

Met de medewerkers van de teams Sociaal Domein en Basisregistratie Personen was tot voor kort een regulier overleg met de CISO en Privacy-officer over informatievoorziening en gegevensbescherming. Juist met deze afdelingen omdat zij veel (bijzondere) persoonsgegevens verwerken en het risico op incidenten navenant groot is. Uit de interviews blijkt dat dit overleg in de toekomst anders wordt vormgegeven, hoe is nog niet duidelijk.

De CISO en de PO hebben met enige regelmaat overleg met de medewerker die de procesbeschrijvingen op operationeel niveau op informatieveiligheid en privacy bijwerkt.

Regionaal

In Zuidoost Utrecht hebben de CISO's en de privacyofficers elke twee weken een regionaal overleg, om onderling af te stemmen, uit te wisselen en van elkaar te leren. Indien nodig worden de CISO's bij de gemeen-schappelijke regelingen daarbij betrokken.

Crisisteam

Het operationeel crisisteam (OT) is niet zozeer een overlegorgaan, maar een team dat in tijden van een calamiteit daadkrachtig moet kunnen opereren, zoals bijvoorbeeld bij het lek Log4J in december 2021. Het hoofd van de afdeling Informatievoorziening (IV), de CISO, hoofd Dienstverlening, hoofd Communicatie vormen de kern van het crisisteam, onder leiding van een directielid. Een medewerker van het domein Veiligheid, die contact onderhoudt met de Veiligheidsregio, wordt altijd geïnformeerd en sluit op ad hoc basis aan.

Checklist cybercrisis

Door adviesbureau BCM is een checklist opgesteld met 6 activiteiten. Eén van de activiteiten is in de preventiesfeer, namelijk een jaarlijkse oefening in samenwerking met de Veiligheidsregio. De andere vijf betreffen activiteiten die in geval van een crisis moet worden ondernomen. Zoals inschakelen van de Informatiebeveiligingsdienst (IBD) van de VNG in de rol van Computer Emergency Response Team (CERT) en het activeren van het voornoemde operationeel crisisteam (OT).

Samenvatting

De beleidscyclus op informatieveiligheid en privacy wordt grotendeels gevolgd door de gemeente Zeist en is risicogebaseerd. Het strategische beleid is in overeenstemming met de geldende normen vastgesteld. Het beleid is op basis van het 'three lines of defence'-principe geënt en de verantwoordelijkheden zijn conform dat principe in het beleid vastgelegd. De beleids- en visiestukken volgen de mainstream in gemeenteland en getuigen nog niet van een grote ambitie op het gebied van informatie-veiligheid en privacy.

Met de Verklaring van Toepasselijkheid (VvT) in plaats van een jaarplan is tijdelijk de beleidscyclus niet gevolgd. Aangegeven wordt dat de cyclus van GAP-, risicoanalyse en jaarplan wordt weer opgepakt.

Op de doorvertaling van het strategisch beleid naar het tactisch en met name operationeel niveau heeft de gemeente nog veel stappen te zetten.

De middelen voor informatieveiligheid en privacy zijn niet afgebakend in begroting en verantwoording, maar als iets nodig is worden de middelen door directie en bestuur ter beschikking gesteld.

De functies op informatieveiligheid en privacy zijn voldoende bezet om aan de huidige ambitie te kunnen voldoen. Bij een hogere ambitie past uiteraard meer capaciteit en dat geldt sterker met het oog op toekomstige ontwikkelingen en eisen die aan de gemeente worden gesteld. De CISO is nu in de lijn gepositioneerd bij de afdeling Informatievoorziening, hoewel de IBD deze bij voorkeur los van de lijn ingevuld ziet. Met de huidige bezetting kan een van de lijn onafhankelijke CISO-functie ingevuld worden.

Er zijn voldoende momenten binnen de gemeente waarop de professionals op informatieveiligheid en privacy elkaar treffen en de aangelegenheden op strategisch, tactisch en operationeel niveau onderling bespreken. Ook directie en bestuur is hierop aangesloten.

4 Informatie gemeenteraad

Onderzoeksvraag 2	Wordt de gemeenteraad goed geïnformeerd over de risico's en beheersingsmaatregelen?

In de BIO is vastgelegd dat de raad in het kader van de P&C-cyclus minimaal een keer per jaar wordt geïnformeerd over de stand van zaken met betrekking tot informatieveiligheid. Over gegevensbescherming en privacy zijn geen nadere bepalingen. In het RASCI-model is de raad als een partij aangemerkt die geïnformeerd moet of kan worden, net als inwoners, accountant en de Autoriteit Persoonsgegevens. Het kanaal dat jaarlijks gebruikt wordt om de raad te informeren is de ENSIA-rapportage.

ENSIA

De jaarlijkse ENSIA-rapportage ziet toe op interne en externe audits op applicaties zoals Basisregistratie Personen (BRP) en Reisdocumenten, Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basis-registratie Ondergrond (BRO), Waardering Onroerende Zaken (WOZ) en de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet). Over deze applicaties moet de gemeente door middel van ENSIA verantwoording afleggen richting landelijke toezichthouders. Met name aan DigiD en Suwinet worden hoge eisen met betrekking tot veiligheid gesteld. Het college rapporteert hierover met een assurance-statement van een extern bureau. Daarin meldt het college onder andere in hoeverre voldaan wordt aan de eisen van de landelijke toezichthouders en of verbetermaatregelen van toepassing zijn.

Daarnaast dient via ENSIA aan de gemeenteraad te worden gerapporteerd over de vorderingen op informatiebeveiliging, dat wil zeggen de vorderingen van de gemeente ten opzichte van de maatregelen die de BIO voorschrijft. In de ENSIA-rapportages aan de raad wordt ingegaan op de audits van Suwinet en DigiD en de (zelf)audits op de bovengenoemde applicaties. In de ENSIA rapportage 2021 is opgenomen dat DigiD en Suwinet aan de normen voldoen. Maar de WOZ die toen voor het eerst werd geaudit niet. De te nemen maatregelen zijn door de Belastingsamenwerking gemeenten en hoogheemraadschap Utrecht (BghU) in een verbeterplan opgenomen en worden door de samenwerkende partijen (gemeenten en hoogheemraadschap) gemonitord. In de ENSIA 2022 is gemeld dat DigiD aan de normen voldoet, maar Suwinet niet.[22] Door het college wordt aangegeven dat een verbeterplan is opgesteld en de in de

[22] Het kan voorkomen dat Suwinet in een jaar voldoet aan de normen en een jaar later niet. De gehanteerde normen op informatieveiligheid worden soms aangescherpt.

Regionale Sociale Dienst Kromme Rijn Heuvelrug (RSD-KRH) deelnemende gemeenten de sociale dienst daarop zullen gaan monitoren.

Raad krijgt duiding, maar geen inzicht in risico's

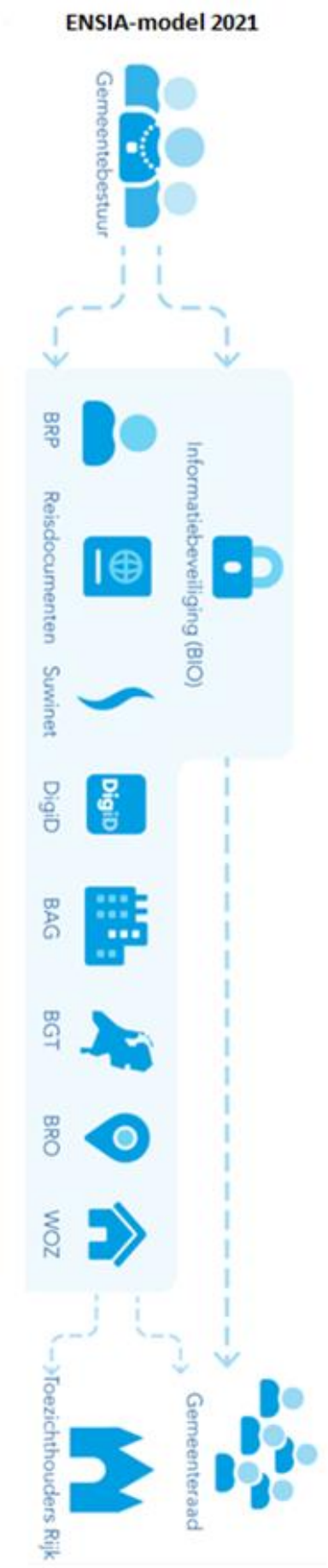
Volgens respondenten kreeg de raad tot en met 2023 een duiding van de resultaten van de audits in het kader van ENSIA en de stand van zaken met betrekking tot de maatregelen van de BIO. Dat gebeurde in de vorm van een jaarplan met activiteiten. De raad krijgt tegenwoordig bij ENSIA een korte duiding van de bevindingen. De vorderingen op de volledige breedte van de maatregelen in de BIO komen in ENSIA niet aan bod. De raad krijgt daarmee geen inzicht in de risico's of de beheersingsmaatregelen op alle aspecten van informatieveiligheid. Wel wordt er in het algemeen gemeld of er naar aanleiding van de geconstateerde verbeterpunten maatregelen worden getroffen.

Via Raadsinformatiebrieven (RIB) geïnformeerd

Via raadsinformatiebrieven (RIB) wordt de raad geïnformeerd over het beleid op informatieveiligheid en privacy. In december 2022 krijgt de raad de informatiebrief dat het strategische informatieveiligheids- en privacybeleid zijn vastgesteld door het college. Daarin wordt een themabijeenkomst aangekondigd over onder andere het ambitiedocument 'Een goed leven in Zeist – ook digitaal'. Met de RIB van juli 2023 krijgt de raad het genoemde ambitiedocument en het jaarverslag van de FG toegestuurd.

Jaarverslag FG: Rapportcijfer 7

In het jaarverslag gaat de FG in op de stand van zaken met betrekking tot beleid en maatregelen op privacy en gegevensbescherming. De stand van zaken op de naleving van de AVG wordt beoordeeld met het rapportcijfer 7. Op 10 speerpunten gaat de FG in op opzet, bestaan en werking van onder andere



beleid, regie, toezicht, informatieveiligheid en budget. Ook geeft de FG een drietal actiepunten mee, zoals vaststellen van het bijgeleverde visie-document ‘Een goed leven in Zeist – ook digitaal’, opstellen van jaarplan 2023-2024 met prioriteiten en verantwoording afleggen via jaar-rapportages. Onder de prioriteiten staat onder andere de invoering van het 3-lijnenmodel, zoals ook in het strategisch beleid 2022-2026 op informatie-veiligheid en privacy is beschreven. Daarmee aangevend dat het strategisch beleid nog niet volledig is geïmplementeerd.

Themabijeenkomsten waarin de raad geïnformeerd wordt

Voorts wordt de raad bij grotere incidenten, zoals grote datalekken, geïnformeerd. De raad wordt met enige regelmaat door de CISO en de strategisch adviseur ICT bijgepraat in themabijeenkomsten of een raadsinformatiebijeenkomst. In 2021 krijgt de raad een presentatie over veilig werken, naar aanleiding van vragen van raadsleden in december 2020 over de hack in Hof van Twente. Uitgelegd is hoe onder andere de back-up systemen werken.

In 2023 gaven de CISO en FG een workshop aan het college over het visie- en borgingsdocument ‘Het goede leven in Zeist – ook digitaal’. Het beschrijft hoe de gemeente het (digitale) bewustzijn en de (digitale) weerbaarheid kan verhogen en de dilemma’s die daarbij spelen. Dezelfde workshop is voor de raad in een raadsinformatiebrief aangekondigd.

Aandacht vanuit de raad als laag ervaren

Enkele respondenten geven aan het te jammer te vinden dat een van de sessies die gepland is voor de raad niet goed door de raadsleden werd bezocht. Ondanks het gegeven dat de raad bij de accountant informatie-veiligheid als speerpunt heeft aangegeven (zie hoofdstuk 6), wordt de bestuurlijke aandacht vanuit de raad voor het onderwerp niet altijd als hoog ervaren. Als er vragen vanuit de raad komen, zijn ze vaak ingegeven door incidenten elders, zoals de aanval met ransomware bij Hof van Twente. De meeste raadsleden gebruiken niet de mailboxen van de gemeente Zeist, maar de eigen privé-mailboxen. Dat wordt als een aandachtspunt vanuit informatieveiligheid gezien, als de raadsleden onvoldoende de risico’s doorgronden en het mailverkeer niet goed beveiligen. Raadsleden beschikken ook over vertrouwelijke en gevoelige persoonsgegevens. De FG wijst erop dat de raad zelf ook verwerkings-verantwoordelijke is.

Samenvatting

De krijgt in de reguliere cyclus gerapporteerd over de vorderingen op het informatieveiligheids- en privacybeleid. Dat gebeurt jaarlijks door middel van de ENSIA-rapportages, en sinds kort het jaarverslag van de Functionaris Gegevensbescherming. Daarbij krijgt de raad wel duiding, maar geen dieper inzicht in de risico’s die de gemeente loopt. Incidenteel wordt de raad geïnformeerd via raadsinformatiebrieven en worden themabijeenkomsten georganiseerd. Er is geen structureel overleg tussen college en raad op het gebied van informatieveiligheid en privacy aangetroffen.

5 Bewustwording

Onderzoeksvraag 3	Krijgen medewerkers goede uitleg en ondersteuning om veilig te werken?

Risicobewustzijn

Bewustwording van medewerkers over de risico's van informatieveiligheid is uitermate belangrijk. De meeste respondenten melden op de vraag wat er goed gaat op het gebied van informatieveiligheid en privacy dat de bewustwording hiervan in de gemeentelijke organisatie is toegenomen. Tegelijk melden de respondenten dat het gewenste niveau nog niet bereikt is en het altijd beter kan. Bekend uit onderzoek bij gemeenten in het algemeen is dat bij afdelingen en teams die al langer met (bijzondere) persoonsgegevens werken, zoals burgerzaken, sociaal domein, salaris-administratie en HR, de medewerkers redelijk risicobewust zijn. Maar er zijn ook medewerkers van afdelingen die daar minder bij stil staan. Voor een aantal medewerkers is aandacht voor informatieveiligheid iets dat afleidt en naast het dagelijkse werk erbij komt.

Inwerkprogramma en Zeist Academie

Veilig (en integer) werken en bewustwording van de risico's is volgens de gemeentelijke beleidsstukken een continu proces. Dat geldt voor nieuw aangenomen en zittend personeel en externe inhuur. Sinds 2021 is informatieveiligheid onderdeel van het inwerkprogramma (onboarding) voor nieuwe medewerkers. De CISO en de informatieadviseur geven binnen het inwerkprogramma van nieuwe medewerkers (de zogenoemde 'onboarding') de workshop "ik ben best wel Informatieveilig". Daarin leren medewerkers onder andere phishing mails te herkennen en hoe om te gaan met informatieveiligheid. De e-learning module 'Holmes' vanuit de Zeist Academie is voor nieuwe medewerkers een verplicht onderdeel van de onboarding. De zittende medewerkers worden voor de e-learning uitgenodigd en deelname wordt aangemoedigd, maar deelname is niet verplicht. Een enkele respondent geeft aan dat het voornemen is om deelname van alle medewerkers te monitoren en daarover te rapporteren aan de directie.

Externen

Externen die bij samenwerkingspartners werkzaam zijn, krijgen niet dezelfde onboarding als de medewerkers van de gemeente. Bijvoorbeeld de consulenten in het sociaal domein die bij andere organisaties in dienst zijn. Dat is een risico, met name in een terrein waar veel persoonsgegevens worden verwerkt. Dat gaat in de loop van 2024 veranderen. De consulenten komen in dienst van de gemeente en krijgen vanaf dan dezelfde onboarding.

Diverse activiteiten

Er zijn onder andere bijeenkomsten georganiseerd voor medewerkers om de bewustwording op risico's op informatieveiligheid en privacy te vergroten. Zoals de 'AVG on tour' over gegevensbescherming langs de

teams. Voorts is een training verzorgd, specifiek voor de medewerkers van het sociaal domein, omdat zij veel bijzondere persoonsgegevens in groepen (kwetsbare) inwoners verwerken. Medewerkers die het scherm bij afwezigheid niet op slot hebben, gezet zijn met ludieke acties 'bestookt'.

Beveiligd werken

Uit de interviews bij twee afdelingen die veel persoonsgegevens verwerken blijkt dat de medewerkers zich zeer bewust zijn van de risico's. Mails met persoonsgegevens gaan over beveiligde verbindingen. Of met behulp van Smartlockr, waarmee men via een vinkje de mail met persoonsgegevens beveiligt. Helemaal uitsluiten dat er persoonsgegevens in mailmappen aanwezig zijn kunnen de respondenten niet, maar de middelen om veilig gegevens te delen en op te slaan zijn wel aanwezig. Ook wordt in het kader van gegevensbescherming gelet op dataminimalisatie, zo min mogelijk persoonsgegevens verwerken die nodig zijn voor de gestelde taak. Respondenten melden dat het werken met deze uitgangspunten van de AVG nog niet bij alle afdelingen vanzelfsprekend is. Met name bij de afdelingen die weinig persoonsgegevens verwerken.

Intranet

Online wordt informatie en tips over informatieveiligheid en privacy gepubliceerd op het onderdeel 'Weten en regelen'. Informatie over verwerkingsovereenkomsten, zodat medewerkers met vragen hierover antwoorden kunnen vinden en voor een groot deel zelf aan de slag kunnen. Die informatievoorziening verzorgt het team Veilig werken samen met het team Communicatie.

Eigenaarschap nog te veel bij afdeling IV

Ondanks dat het bewustzijn is toegenomen wordt door respondenten gemeld dat het eigenaarschap op informatieveiligheid en privacy nog te veel bij het team Informatievoorziening wordt gelegd, terwijl volgens het 3-lines-of-defence model het eigenaarschap thuishoort bij de proces-eigenaren, ofwel de teammanagers, zou moeten liggen. De werking van het beleid en de borging van de processen staat volgens een aantal respondenten nog in de kinderschoenen. Daarin is onder andere het hiervoor geconstateerde gemis merkbaar van een deel van de protocollen en richtlijnen op tactisch en operationeel niveau. Daarop wordt sinds kort ingezet met een kwaliteitsmedewerker die zich bezig houdt met het doorvertalen van het strategische en tactische beleid naar het operationele niveau (zie ook §3.2).

Functionarissen op informatieveiligheid en privacy geven aan dat de medewerkers hen meer en meer weten te vinden en te betrekken aan de voorkant van processen waar informatieveiligheid en privacy een rol spelen. Dat besef is gegroeid, maar nog niet bij alle teams aanwezig. Mogelijk omdat medewerkers het niet weten, het nog niet in protocollen is opgenomen of als er tijdsdruk aanwezig is, kan het zijn dat aspecten op informatieveiligheid en privacy niet aan de voorkant meegenomen worden. Dan bestaat de kans dat delen van het proces overgedaan moeten worden, wat over en weer aanleiding kan geven tot frustraties.

'Tone at the top' wordt als goed ervaren

Om bewustwording en eigenaarschap in de organisatie goed te laten landen is het nodig dat van hogerhand het goede voorbeeld wordt gegeven. Het college en directieteam moeten doordrongen zijn van de noodzaak daartoe. Zo krijgt het college geregeld een presentatie over de stand van zaken, onder andere naar aanleiding van de ENSIA-rapportage (zie ook §4.1). Ook is de noodzaak voor bewustwording aan de orde gekomen bij het college in een door de VNG georganiseerde bestuurlijk gesprek ('peer to peer'-sessie onder leiding van de gemeente Veere). Bij het directieteam komt ook met enige regelmaat informatieveiligheid en privacy als agendapunt langs. Samen hebben college en directie eind 2023 een cyberoefening gehad, voorafgegaan door een scenariosessie. Alle respondenten ervaren een goed voorbeeldgedrag aan de top.

Taakvolwassenheid rond 2 op 5-puntschaal

Zoals eerder opgemerkt is in beleid vastgelegd dat informatiebeveiliging en privacy niet iets van de gespecialiseerde functionarissen is, maar een verantwoordelijkheid van de medewerkers en het lijnmanagement. De taakvolwassenheid van lijnmanagement en medewerkers op informatie-veiligheid, dat wil zeggen de mate waarin zij bekend zijn met de protocollen en procedures en deze in de praktijk brengen, wordt vaak op een 5 punts-schaal weergegeven. NOREA, de beroepsvereniging voor IT auditors, onderdeel van de Koninklijke Nederlandse Beroepsorganisatie van Accountants (NBA), gebruikt de schaal zoals in bijlage 5 is opgenomen.

Uit de interviews blijkt dat de gemiddelde volwassenheid van de organisatie in Zeist op informatiebeveiliging rond 2 scoort. Dat wil zeggen dat er wel procedures zijn, maar onvolledig. En dat deze inconsistent en ad hoc worden uitgevoerd.

Er zijn geen landelijke benchmarks op volwassenheidsniveau van medewerkers bij gemeenten. Uit diverse onderzoeken naar bewustwording bij gemeenten komt naar voren dat het gemiddelde niveau tussen niveau 2 en 3 ligt. Algemeen gesteld wordt dat een organisatie vanaf niveau 3 'in control' is. Vanaf dat niveau zijn beheersingsmaatregelen gedocumenteerd en worden ze gestructureerd, geformaliseerd en aanwijsbaar uitgevoerd.

Uit de interviews blijkt dat er vooruitgang wordt geboekt, maar dat veel proceseigenaren nog ondersteund moeten worden door de functionarissen op informatieveiligheid en privacy. Alertheid wanneer in processen aspecten hierop aan de orde zijn en de notie om de professionals tijdig te betrekken is niet altijd en overal aanwezig. Zeker niet als bijvoorbeeld gegevensverwerking maar een klein onderdeel van het proces vormt. Dan is het risicomanagement vaak beperkt tot de financiële risico's en zitten de proceseigenaren niet te wachten op input die misschien vertragende invloed zal hebben op de planning. Uit de interviews blijkt dat het vaak niet om weerstand gaat, maar dat men er niet tijdig bij stil heeft gestaan. Dat verschilt overigens per afdeling: zoals eerder geconstateerd zijn er

afdelingen die al langer gewend zijn veilig te werken en hoger zullen scoren op taakvolwassenheid hierop.

Lerende houding

Voorkomen van fouten is uiteraard het best. De houding van de directie is dat fouten niet altijd te voorkomen zijn en uitgedragen wordt dat medewerkers fouten open moeten kunnen melden. Uit de interviews blijkt dat een lerende houding aangemoedigd wordt. Aangegeven wordt dat medewerkers bij geconstateerde tekortkomingen worden benaderd door de servicedesk om uit te leggen wat er fout ging, wat het belang is van ieders individuele actie op systemen en hoe men dit kan voorkomen in de toekomst.

5.1 Phishing simulatie

Phishing mail test 2022

Cybercriminelen gebruiken met phishing verschillende methodes om gevoelige informatie te verkrijgen. Dit is een reële dreiging voor bedrijven en overheidsorganisaties. Met behulp van phishing-simulaties kunnen medewerkers bewust(er) gemaakt worden van gevaren van de digitale wereld. Hoe hoger het bewustzijn en de weerbaarheid van de medewerkers, hoe kleiner de kans op financiële- en imago schade. De gemeente laat phishing mail testen uitvoeren In 2022 is een phishing mail simulatie uitgevoerd. Daarbij heeft 77% van de medewerkers geklikt op een link uit een verdachte mail en uiteindelijk zijn van 23 medewerkers inloggegevens ‘gephisht’.

Phishing mail test 2023

In het kader van het rekenkameronderzoek kreeg selectie van 200 medewerkers op 24 oktober een phishing mail, zogenaamd van de Afdeling HR van de gemeente Zeist.[23] Het dringende verzoek was om op een link naar het salarisportaal te klikken om eventuele fouten in de salarisadministratie te corrigeren. Er is een aantal kenmerken in de phishing -simulatie aangebracht waardoor deze herkenbaar is als phishing mail:

- De afzender was niet afkomstig van gemeente Zeist
- De aanhef was onpersoonlijk (‘Beste collega’)
- De link verwees niet naar een URL van de gemeente Zeist
- In de mail werd tijdsdruk geënsceneerd
- De mail was niet persoonlijk ondertekend, maar algemeen door Afdeling HR, Gemeente Zeist

De phishing simulatie is een week lang actief geweest. De ICT regisseurs zijn van tevoren ingeseind dat de phishing simulatie plaats zou vinden, zodat zij niet technisch zouden ingrijpen na een melding. Nadat de medewerker van de helpdesk na ongeveer 10 minuten de ICT regisseurs ging informeren

[23] Om ervoor te zorgen dat de nep phishing mail niet door de virusscanner of firewall tegengehouden zou worden, is het domein waar vanaf de phishing mail is gestuurd ‘gewhitelist’. Dat wil zeggen dat de gemeente ingesteld heeft dat mails van dat domein vertrouwd kunnen worden.

over een mogelijke phishing aanval, hebben zij hem geïnformeerd over de test en verzocht niet in te grijpen en hier geen ruchtbaarheid aan te geven.

De eerste dag heeft een alerte medewerker via een mailbericht collega's op de hoogte gesteld, en hebben meerdere medewerkers de phishing mail bij de melddesk gemeld. Op de eerste dag heeft 29% van de medewerkers in de testpopulatie op de link geklikt. Dat percentage liep in de week doorlooptijd op tot 39%. De medewerkers die op de link hebben geklikt kwamen op een landingspagina waarop uitleg werd gegeven over de phishing simulatie en waaraan ze in het vervolg phishing mails kunnen herkennen.

Samenvatting

Door respondenten wordt als positief ervaren dat de bewustwording bij de medewerkers de laatste jaren groter is geworden. Tegelijk wordt erkend dat het gewenste niveau nog niet bereikt is. Vanuit bestuur en directie wordt hier op ingezet. Een lerende houding wordt sterk gepropageerd en de 'tone at the top' levert een voorbeeldfunctie. Ondanks de vele activiteiten, zoals aandacht voor informatieveiligheid en privacy in de onboarding, e-learning, berichten op intranet, wordt het eigenaarschap bij de 1e lijn van medewerkers en lijnmanagement te weinig beleefd. De gemiddelde taakvolwassenheid op informatieveiligheid wordt in de interviews rond de 2 op een 5 puntsschaal geschat.

Bij de phishingmail test in het kader van het rekenkameronderzoek blijkt het klikpercentage onder de steekproef van medewerkers van de gemeente hoger is dan gemiddeld bij vergelijkbare phishing mails.[24] Dat is mede een signaal dat het vereiste bewustwording bij de medewerkers nog niet is bereikt.

[24] De phishing mail test is bij meerdere vergelijkbare organisaties uitgevoerd, en dan is het gemiddelde klikpercentage circa 35%.

6 Communicatie over datalekken

Onderzoeksvraag 4	Hoe communiceert de gemeente met betrokkenen en inwoners over datalekken?

Proces	De gemeente heeft in het strategisch beleidsplan Privacy een proces vastgesteld voor het melden van en omgaan met datalekken. De gemeente onderscheidt drie categorieën datalekken, namelijk een inbreuk op de beschikbaarheid [25], inbreuk op de vertrouwelijkheid [26] en inbreuk op de integriteit [27] van persoonsgegevens (BVI). Er is door de gemeente een meldpunt datalekken ingesteld.
Meldpunt datalekken	Bij het meldpunt datalekken kunnen medewerkers terecht voor het melden van een (potentieel) datalek. Het meldpunt wordt beheerd door de CISO en de Privacy Officer. Verder zijn bij een (potentieel) datalek de Service Desk, het kernteam Datalekken en Beveiligingsincidenten en de portefeuille-houder betrokken. In het kernteam Datalekken zijn de CISO, Privacy Officer, Privacy Jurist, Security Officer en de FG vertegenwoordigd. De gemeente-secretaris en de bestuurder worden door de CISO geïnformeerd over het (potentiële) datalek. Een datalek moet in principe ook gemeld worden bij de Autoriteit Persoons-gegevens (AP). Ook moeten de betrokkenen wier gegevens het betreft geïnformeerd worden. Evenwel is niet elke inbreuk op de beschikbaarheid, vertrouwelijkheid of integriteit van persoonsgegevens die door de gemeente worden verwerkt is een datalek. Dat hangt af van de mate waarin het datalek een risico oplevert voor de rechten en vrijheden van de betrokkenen. Als er een hoog risico is wordt de melding bij de AP gedaan en worden de betrokkenen geïnformeerd.
Terugkoppeling	Uit de bestuurlijke rapportage Informatieveiligheid blijkt dat de melder en de betrokkenen waarderen en het prettig vinden dat zij persoonlijk geïnformeerd worden over het lek en de afwikkeling. Ook wordt indien nodig de Raad geïnformeerd, volgens de procedure. De bekendheid van het meldpunt datalekken en de meldingsbereidheid bij medewerkers om een datalek te melden is groot, volgens respondenten. De meldingen worden onderzocht, geanalyseerd en geregistreerd. De meeste meldingen zijn te classificeren als fouten zoals door de AP ook de meeste

[25] Inbreuk op de beschikbaarheid betekent dat de organisatie waar het datalek is (geweest) niet meer bij de persoons-gegevens kan komen. Of de gegevens zijn vernietigd. Dit is gebeurd door iemand die daartoe niet bevoegd is. Of dit is per ongeluk gebeurd (bron: AP).

[26] Inbreuk op de vertrouwelijkheid betreft persoonsgegevens die openbaar zijn gemaakt of er is toegang geweest tot persoonsgegevens. Dit is gebeurd door iemand die daartoe niet bevoegd is. Of dit is per ongeluk gebeurd (bron: AP).

[27] Inbreuk op de integriteit betreft persoonsgegevens die zijn gewijzigd door iemand die daartoe niet bevoegd is. Of dit is per ongeluk gebeurd (bron: AP).

worden gecategoriseerd, namelijk het gebruiken van een verkeerd email-adres, een verkeerde bijlage in een envelop, het niet gebruiken van de BCC of het verkeerd anonimiseren van stukken. De analyse van het proces is er op gericht ervan te leren zodat er niet opnieuw een datalek kan ontstaan.

Rapportage

Er is geen overzicht van datalekken aangetroffen en er wordt niet over gerapporteerd in de jaarstukken. Bij navraag zijn er in 2022 en 2023 respectievelijk 12 en 18 potentiële datalekken gemeld bij de Melddesk Datalekken. Daarvan hoefde er geen gemeld hoeven te worden bij de Autoriteit Persoonsgegevens, omdat het uiteindelijk geen datalek betrof of tijdig gemitigeerd kon worden. Daarnaast is één datalek via de gemeenschappelijke regeling die het betrof daadwerkelijk als datalek bij de AP gemeld.

Samenvatting

De gemeente heeft een proces datalekken vastgesteld, waarin de activiteiten en communicatie bij een datalek zijn beschreven. Er is een meldpunt, waarbij onder andere de CISO en Privacyofficer zijn aangesloten. Er zijn weinig ‘echte’ datalekken te melden, maar de communicatie met betrokkenen wordt als positief ervaren.

7 Controle op naleving en voorkomen

Onderzoeksvraag 5	Hoe controleert de gemeente op naleving van veilig werken en het voorkomen van beveiligingsincidenten?

Veel van de manieren waarop de gemeente controleert op de naleving van veilig werken en het voorkomen van incidenten zijn hiervoor de revue gepasseerd. Zoals de verschillende overleggen waarin aspecten van informatieveiligheid en privacy worden geagendeerd, bewustwordings-activiteiten en de phishing simulatie, de (zelf)audits en rapportages naar aanleiding van de audits. Hieronder gaan we in op de aanvullende maatregelen die de gemeente inzet op controle en preventie.

Accountant

De accountant stelt, in opdracht van de auditcommissie van de raad, onder eigen verantwoordelijkheid een controleplan op. De raad kan speerpunten meegeven. Vorig jaar heeft de raad, naast het strategisch huisvestingsplan, informatieveiligheid als speerpunt aangegeven. Los daarvan heeft de accountant in eerdere jaren ook al gekeken naar algemene IT-controls, maar dan vooral gericht op de financiële rechtmatigheid. Vanuit de afdeling Control wordt met behulp van de Verbijzonderde Interne Controles (VIC) input aan de accountantscontrole gegeven.

Zo gaf de accountant eind 2021 de volgende aanbevelingen:

- verdere formalisering en implementatie van rollen, verantwoordelijkheden en General IT Control processen;
- opzetten en bijhouden van een actueel overzicht van de systeemarchitectuur waaronder voor de situatie rond Unit4 Financials en haar bronsystemen;
- opzetten, beschrijven en invoeren van IT werkprocessen;
- opstellen en invoeren van beleid en maatregelen ter voorkoming gebruik non personal accounts (NPA) voor beheer database van Unit4 Financials.

Informatiemanagement aanwezig, niet optimaal gebruikt

Zoals hiervoor geconstateerd is het strategische beleid aanwezig, en deels op tactisch en operationeel gebied. Uit de interviews en de verschillende controles en audits blijkt dat het aantoonbaar vastleggen van activiteiten en beheersmaatregelen op informatieveiligheid en privacy nog aandacht verdient.[28] De gemeente beschikt al 5-6 jaar over een Information Security

[28] Dat bleek niet alleen ten aanzien van informatieveiligheid en privacy, maar in 2021 ook bij de audit op de implementatie van het financiële systeem AFAS bleken tekortkomingen: Op 1) beheer en de inrichting van AFAS voor de aansturing van de financiële transactieverwerking 2) de interne controles op het personeelsdata en salaris verwerkende proces, 3) de door de projectorganisatie ingevoerde processen voor beheer en doorontwikkeling van het systeem en 4) de projectacceptatie en dechargeverlening. Risico's die werden geconstateerd waren incorrecte financiële boekingen. Ook werd geconstateerd dat er onterechte autorisaties waren en te veel personen met een account met te veel rechten. Volgens de afdeling HR worden de autorisaties nu 2x per jaar gecontroleerd.

Management System (ISMS) waarmee de PDCA-cyclus[29] op informatie-veiligheid vormgegeven kan worden. Met een dergelijk systeem kan de organisatie de vinger aan de pols houden of de afgesproken activiteiten en de beheersmaatregelen op informatieveiligheid worden opgevolgd. De activiteiten in het kader van informatieveiligheid kunnen daarmee worden geformaliseerd en geborgd. In de interviews wordt aangegeven dat het systeem beter gevuld en gebruikt moet gaan worden. Dat ligt enerzijds aan de capaciteit om het systeem te vullen, anderzijds aan de gebrekkige taakvolwassenheid van de lijn die met het systeem in de praktijk aan de slag moet. Het ISMS blijft daarmee vooral alleen een tool van de afdeling IV. In principe is de aandacht voor de PDCA-cyclus en de intentie om te leren aanwezig, evenals het instrument. Maar het niet optimaal gebruik staat verdere professionalisering in de weg.

Streven naar 'In control statement'

Uit de interviews blijkt dat de PDCA-cyclus vanaf begin 2024 vorm zal worden gegeven, vanuit de afdeling IV samen met de afdeling Control. Deze samenwerking met Control is mede ingegeven door het streven van de ambtelijke en bestuurlijke top om op termijn een 'in control statement' af te kunnen geven. Tot nu toe concentreerde Control met de interne controles op de financiële rechtmatigheid. Bij een 'in control statement' moet dat verbreed worden naar kwaliteitsaspecten van de gehele organisatie, waarbij informatieveiligheid ook betrokken is.

Interne controle

Naar aanleiding daarvan heeft de afdeling Control in 2022 op IT een relatief beperkt onderzoek uitgevoerd, namelijk op de governance, informatie-beveiliging en de beheersmaatregelen in de IT-processen. Daaruit werd de conclusie getrokken dat de beheersmaatregelen voldoen, behalve op onder andere systeemarchitectuur, beheersing van de uitbestedingen en informatiebeveiliging. Bij dat laatste werd geconstateerd dat informatie-beveiliging nog geen integraal onderdeel uitmaakt van de overall risico-managementcyclus[30]. Het geschetste risico is dat de CISO niet over alle relevante informatie beschikt voor de uitvoering van het informatieveilig-heidsbeleid. De CISO krijgt sinds 2023 de op informatieveiligheid betrekking hebbende rapportages van de afdeling Control.

Bij de monitoring van de verbetermaatregelen naar aanleiding van de bevindingen van de accountant en de interne controle zijn in 2023 verbeteringen geconstateerd ten aanzien van de aansluiting van informatie-beveiliging op de risicomanagementcyclus, het proces rond wijzigings-beheer, het proces rond toekennen, wijzigen en intrekken van rechten en de minimalisering van de generieke accounts. Ten aanzien van de andere bevindingen van de accountant en interne controle zijn verbeteracties nodig, zoals de systeemarchitectuur, de implementatie van systemen en opdrachtverlening aan leveranciers van IT-systemen. Maar ook op de

[29] PDCA-cyclus is de beleidsleercyclus: Plan-Do-Check-Act.
[30] Dat is onder andere nodig om naar een 'in control statement' te groeien.

punten waarop verbetering is geconstateerd, is nog verdere vooruitgang te boeken, zoals blijkt uit de interviews en de pentesten (zie §8.2).

Dpia's

Dataprotection impact assessments (dpia's) moeten in het kader van de AVG uitgevoerd worden op processen waar veel (bijzondere) persoonsgegevens worden verwerkt. Uit de interviews en een inventarisatie blijkt dat de gemeente Zeist vanaf de introductie van de AVG in 2018 dpia's uitvoert. In totaal zijn 10 belangrijke verwerkingsprocessen die aan de criteria voldoen zijn geaudit en elk nieuw proces of nieuwe applicatie wordt in dat kader opgepakt. Er rekening mee houdend dat een gemeente gemiddeld tientallen verwerkingsprocessen heeft die mogelijk in aanmerking komen voor een dpia, blijft er nog een caseload liggen.

Een volledige dpia kost namelijk de nodige tijd om uit te voeren en moet door de Privacyofficer gecontroleerd worden. De Privacyofficer voerde voorheen de dpia's uit. Uit de interviews blijkt dat de proceseigenaren in de lijn nog wel ondersteuning nodig hebben, maar meer en meer hun verantwoordelijkheid hiervoor nemen. Zij kunnen met een quickscan of predpia bepalen of een volledige dpia uitgevoerd moet worden, afhankelijk van het risiconiveau. In totaal zijn 22 quick scans en 10 audits uitgevoerd. Zo is in het sociaal domein voor het gebruik van Zorgnet in de regio een quick scan uitgevoerd, maar nog geen volledig assessment. Dat gaat in regionaal verband uitgevoerd worden. Voor het regionaal aanbestede jeugdvolgsysteem is bijvoorbeeld wel al een volledige dpia uitgevoerd.

Gemeenschappelijke regelingen

De verantwoordelijkheid voor de uitvoering van processen op informatieveiligheid en privacy bij gemeenschappelijke regelingen ligt uiteindelijk bij de deelnemende gemeenten. Daarop moeten de bestuursleden in de regelingen en accountmanagers alert zijn, bijgestaan door onder andere de CISO en Privacyofficer of FG. Zo worden bijvoorbeeld delen van Suwinet uitgevoerd door de Regionale Sociale Dienst Kromme Rijn Heuvelrug (RSD-KRH), daarbij ondersteund door Centric als IT-bedrijf. Daaraan liggen verwerkingsovereenkomsten en zogenoemde Third Party Memoranda (TPM)[31] ten grondslag. De gemeenten krijgen auditrapporten over de uitvoering van de processen op informatieveiligheid en privacy bij de gemeenschappelijke regelingen. Deze werden achteraf gecontroleerd door de CISO. Dat proces is verbeterd doordat de CISO vooraf voor advies wordt betrokken. Zo kon de CISO naar aanleiding van het auditrapport van de RSD-KRH constateren dat een aantal jaren achter elkaar niets werd gedaan met steeds dezelfde bevinding en aanbeveling op informatieveiligheid.

[31] Third Party Memorandum (TPM). Verklaring dat de derde partij, die gegevens voor de gemeente verwerkt, voldoet aan de geldende richtlijnen over informatiebeveiliging.

Samenvatting

De gemeente heeft enkele middelen op naleving en voorkomen van incidenten op informatieveiligheid en privacy tot zijn beschikking. In dit hoofdstuk zijn de accountantscontroles, de Verbijzonderde Interne Controles en de assessments op de verwerking van persoonsgegevens (dpia's) aan de orde gekomen. Deze leiden tot verbetermaatregelen die gevolgd kunnen worden. Een van de manieren om die activiteiten te volgen is het managementinformatiesysteem op informatieveiligheid (ISMS). Dat is aanwezig, maar wordt niet optimaal benut. Het aantoonbaar vastleggen en borgen van activiteiten behoeft verbetering.

8 Toegang tot gevoelige informatie

In dit hoofdstuk behandelen we drie onderzoeksvragen die met elkaar samenhangen, namelijk de vragen 6 tot en met 8.

Onderzoeksvraag 6	Welke penetratietesten voerde de gemeente uit? Zijn verbeterplannen opgesteld naar aanleiding van de pentesten en zijn deze opgevolgd?
Onderzoeksvraag 7	Is het mogelijk om oneigenlijke toegang te krijgen tot gevoelige informatie die de gemeente in beheer heeft?
Onderzoeksvraag 8	In hoeverre wordt in de organisatie van de gemeente Zeist vastgelegd wie wanneer toegang vraagt tot bestanden met gevoelige informatie (het loggen)?

8.1 Pentesten gemeente Zeist

Open source intelligence onderzoek (Osint)

De gemeente Zeist geeft periodiek opdracht tot het testen van de systemen en de bewustwording van de medewerkers (voor deze laatste testen, de phishingmail testen zie §5.1.) Het jaarlijks uitvoeren van testen, op systemen en op bewustwording van medewerkers, is een van de maatregelen in de BIO. In 2021 heeft de gemeente een zogenoemd Open source intelligence onderzoek (Osint) laten uitvoeren op de systemen. Totaalscore was een 3,0 op een 5-puntschaal.[32] Naar aanleiding van de geconstateerde risico's zijn onder andere de volgende verbetermaatregelen in een verbeterplan opgenomen en opgepakt: vervanging van verouderde software en een apart ingerichte ontwikkel- en testomgeving van applicaties.[33]

8.2 Pentesten rekenkamer

Pentesten

In november 2023 zijn in het kader van het rekenkameronderzoek enkele pentesten uitgevoerd op de systemen. Met pentesten wordt de effectiviteit van de door de gemeente genomen beveiligingsmaatregelen getest. Ook zijn phishing mails verstuurd naar medewerkers van de gemeente. Deze zijn bedoeld om het risicobewustzijn bij medewerkers te testen.[34]

De rekenkamer besloot een interne netwerk- en wifi-test, een Active Directory (AD) audit, een inlooptest en een phishing mail test uit te

[32] De in de test geconstateerde risico's waren als volgt gecategoriseerd: 1 kritiek, 1 hoog, 6 gemiddeld, 11 laag en 2 informatief. Hoewel naar aanleiding van de resultaten van de pentest verbetermaatregelen zijn genomen gaan we in deze rapportage niet nader in op de specifieke risico's. Om kwaadwillenden niet in de verleiding te brengen.

[33] De applicaties die gemeenten aanschaffen en/of ontwikkelen zijn uiteraard getest, maar niet getest in de specifieke systeemconfiguratie van elke gemeente. De eis is dan ook om de applicaties in een aparte omgeving te testen of te ontwikkelen, zodat incompatibiliteiten met andere systemen voorkomen kunnen worden.

[34] Een pentest of penetratietest is een toets van een of meer computersystemen op kwetsbaarheden, waarbij deze kwetsbaarheden gebruikt kunnen worden om in deze systemen in te breken.

voeren.[35] Om mogelijke dubbelingen te voorkomen is vooraf overleg geweest met de CISO, informatieadviseur en directielid welke testen de rekenkamer zou uit gaan voeren. Hieronder gaan we in op de resultaten van de testen.

In opdracht van de rekenkamer is door ethisch hackers getest op een beperkt aantal doelen, dat wil zeggen dat de reikwijdte of scope van het onderzoek beperkt is.[36] Daarvoor is in samenspraak tussen de rekenkamer, de gemeente en de onderzoekers een testplan opgesteld. De pentesten zijn in oktober en november 2023 uitgevoerd. Getest is op doelen met een zekere risicoclassificatie. Deze risicoclassificatie is in de onderstaande tabel weergegeven.

Tabel 7.1. Risicoclassificatie pentesten.

Risicoclassificatie	Toelichting
Kritisch (9-10)	Extreem hoge kans dat de beveiligingsmaatregelen niet voldoende zijn of omzeild kunnen worden en dat hierdoor de kwetsbaarheid misbruikt kan worden met als gevolg catastrofale financiële verliezen.
Hoog (7,9-8,9)	Hoge kans dat de beveiligingsmaatregelen niet voldoende zijn of omzeild kunnen worden en dat hierdoor de kwetsbaarheid misbruikt kan worden met als gevolg enorme financiële verliezen.
Gemiddeld (4,0-6,9)	Aannemelijke kans dat beveiligingsmaatregelen niet voldoende zijn of omzeild kunnen worden en dat hierdoor de kwetsbaarheid misbruikt kan worden met als gevolg financiële verliezen.
Laag (0,1-3,9)	Mogelijke kans dat beveiligingsmaatregelen niet voldoende zijn of omzeild kunnen worden en dat hierdoor de kwetsbaarheid misbruikt kan worden met als gevolg gelimiteerde financiële verliezen.
Best Practice	Deze bevinding bevat geen direct aanvalsscenario met negatieve gevolgen. Echter duidt een bevinding met deze classificatie wel aan dat er een beveiligingsmaatregel niet voldoet aan security best practices. Het ontbreken van deze beveiligingsmaatregel kan het uitvoeren van andere aanvallen vergemakkelijken.

Disclaimer

Algemene disclaimer is dat pentesten een momentopname zijn van de stand van zaken van de beveiligingsmaatregelen. De ontwikkelingen aan de kant van de bedreigingen gaan razendsnel, onder andere door kunstmatige intelligentie (AI). Kwaadwillende hackers hebben de tijd om diep te graven in mogelijkheden om schade aan te richten. Terwijl middelen en tijd voor ethische hackers beperkt zijn en de scope van de pentesten navenant beperkt is. Daardoor bieden de resultaten van de pentesten geen garantie voor de toekomst. Ze kunnen wel zicht geven op de risico's die de organisatie op dat moment loopt.

[35] Phishing is een vorm van internet oplichting en fraude, door middel van een vals e-mail bericht 'hengelen' naar inlog- of andere persoonsgegevens.

[36] Een ethisch hacker is een computerspecialist die beveiligingssystemen en netwerken test op een positieve manier. Zijn doel is om door middel van hacken fouten en veiligheidslekken op te sporen in de systemen en netwerken om deze daarna te melden aan de bedrijven of instanties waarmee ze samenwerken.

Afspraak: kritiek risico's meteen melden

Afgesproken is dat kritieke risico's meteen gemeld zouden worden aan de CISO. Dat is op één punt gebeurd tijdens de pentesten. Daarop heeft de organisatie meteen geacteerd en de benodigde verbetermaatregelen geïmplementeerd. Daarnaast heeft de CISO na de testen vertrouwelijk de technische rapportages van de pentesten intern besproken. Daarbij zijn de technische verbetermaatregelen die de ethisch hacker aanraadt aan de orde gekomen.

Hieronder gaan we nader in op de technische pentesten zelf en op hoofdlijnen op daarbij gesignaleerde risico's. De test met phishing mails is al in §4.1 behandeld, omdat deze test met name gericht is op de 'awareness' en niet zozeer op de techniek.

8.2.1 Interne en wifi-netwerk pentest

Interne en wifi-netwerk pentest

Deze pentest is uitgevoerd in week 43 van 2023 en bedoeld om de kwetsbaarheden van het wifi- en interne netwerk in kaart te brengen. Hiermee wordt de effectiviteit van de genomen beveiligingsmaatregelen getest die ervoor moeten zorgen dat de schade die een kwaadwillende in het netwerk kan aanrichten zoveel mogelijk beperkt wordt. Die kwaadwillende kan iemand zijn die van buiten in het netwerk is doorgedrongen of over inloggegevens op het netwerk beschikt. Voor de volledigheid zij vermeld dat in het kader van het rekenkameronderzoek niet getracht is van buitenaf het netwerk binnen te komen.[37]

Wifi-netwerk: geen risico

Tijdens de pentest is het de ethisch hacker niet gelukt het wifi-netwerk te exploiteren. Uit die test is geen risico naar voren gekomen. Wel kan een verbetering, een zogenoemde 'best practice', de veiligheid van het wifi-netwerk verder verbeteren.

Interne netwerk pentest: kritische risico's

Een ander onderdeel van deze pentest betrof het interne netwerk op basis van "grey-box" test.[38] Hierbij wordt aan de ethisch hacker een netwerk-account verstrekt door de organisatie, zodat ook het netwerk "van binnenuit" getest kan worden op eventuele kwetsbaarheden. De scope van deze test betrof 4 doelen, 2 van kritisch en 2 van hoog niveau. De ethische hacker slaagde erin de doelen te behalen. Daarbij zijn 13 risico's geconstateerd, waarvan 3 kritisch, 2 hoog en 8 van gemiddeld niveau. Daarnaast zijn vier verbeteringen van de veiligheid geconstateerd op basis van 'best practice'. In deze rapportage wordt niet dieper ingegaan op de inhoud van de risico's en de 'best practices', om kwaadwillenden niet op een spoor te zetten.

---

37 Meestal zijn de netwerken van buitenaf met een 'zerotolerance' beleid goed beveiligd, met firewalls en virusscanners. Daarnaast is in 2021 het netwerk getest op basis van een Open source intelligence onderzoek (Osint).

38 Een grey-box test is een teststrategie waarbij de ethische hackers beperkte kennis hebben van de technische infrastructuur en systemen en met behulp van die kennis technische zwakheden trachten op te sporen. Bij een black-box test hebben de hackers vooraf geen kennis van de systemen. Bij een white-box test hebben de hackers veel kennis van de systemen.

Zoals eerder aangegeven zijn de risico's van kritiek niveau meteen gedeeld met de CISO en zijn deze door de organisatie meteen aangepakt en gemitigeerd. De andere kwetsbaarheden zijn vertrouwelijk met de CISO gedeeld en met de afdeling IV in overleg met de ethisch hackers besproken. Naar aanleiding van dat overleg zijn enkele verbetermaatregelen meteen genomen en andere in een verbeterplan opgenomen.[39]

Ten aanzien van de pentesten zij opgemerkt dat de ethisch hacker in het kader van de grey-box aanpak een netwerkaccount had en met een eigen laptop toegelaten werd tot de systemen.[40] De opdracht aan de ethisch hacker was op zoek te gaan naar kwetsbaarheden in de systemen. De ethisch hacker is niet extra voorzichtig te werk gegaan om bijvoorbeeld niet opgemerkt te worden of sporen achter te laten. Gedurende de tijd dat de hacker actief was zijn diens handelingen door de detectiesystemen en de ICT-medewerkers opgemerkt. Met die meldingen is niets gedaan, zoals afgesproken om de ethisch hacker zijn opdracht te laten vervullen. De opdracht van de ethisch hacker was namelijk niet om de detectiesystemen te testen. Dat zou een andere en meer voorzichtige aanpak vergen om de inbraakpoging van een malafide hacker te simuleren. Kortom, de kwetsbaarheden die de ethisch hacker, in het kader van de pentesten in opdracht van de rekenkamer, heeft gevonden zijn reëel en kunnen door een malafide hacker geëxploiteerd worden als deze niet opgemerkt wordt.

Activiteiten hacker wel opgemerkt

Op basis van de interne pentest wordt het risico dat de gemeente ten tijde van de test liepen als hoog ingeschat. Dat wil zeggen dat de gemeente kwetsbaar is voor een aanval met grote financiële en andere nadelige effecten tot gevolg.

8.2.2 AD audit

AD audit

De Active Directory (AD) audit is op 22 mei 2023 uitgevoerd. Een AD staat beheerders toe om het beleid met betrekking tot rechten van medewerkers en instellingen in het netwerk van een organisatie te beheren. De AD-audit test met name op risico's in verband met de uitvoering van het wachtwoordenbeleid, kwetsbaarheden met betrekking tot de inrichting van de Active Directory en op accounts en wachtwoorden die bekend zijn op internet.[41]

De AD-audit checkt onder andere op kwetsbare en zwakke wachtwoorden. Deze worden gecheckt op de vereiste complexiteitsgraad en vergeleken

[39] Uit de ambtelijke hoor en wederhoor blijkt dat de afdeling I&A inmiddels is begonnen met de top-10 van deze kwetsbaarheden te mitigeren. Acht hiervan zijn gemitigeerd. De andere twee bestaan uit kwetsbare applicaties waarvoor inmiddels een vervangingstraject loopt voor het uitfaseren.

[40] De ethisch hacker heeft in het kader van het rekenkameronderzoek niet de beveiligingslaag van de van de standaard laptop werkplek getest, noch de firewall.

[41] Accounts en wachtwoorden die bekend zijn op internet betekent dat deze bij eerdere hacks of phishing mails zijn buitgemaakt en gepubliceerd worden op het dark web.

met een lijst op internet met wachtwoorden die in relatie gebracht kunnen worden met de gemeente. In totaal zijn 2.018 gebruiker accounts gescand.

Van de 2.018 gebruikersaccounts zijn er 2 aangetroffen met een zwak wachtwoord dat niet voldoet aan de veiligheidseisen. 322 accounts hebben een wachtwoord van een jaar of ouder. In totaal zijn 154 niet unieke wachtwoorden aangetroffen, dat wil zeggen wachtwoorden die vaker worden gebruikt. Daaronder zijn ook service accounts, die hogere rechten hebben dan reguliere gebruikersaccounts. Van 142 accounts verloopt het wachtwoord nooit en van 9 accounts is de optie 'password not required' ingeschakeld. Verder zijn er 8 accounts zonder versleuteling (missende AES-sleutels).[42]

Daarnaast zijn in de groep 'Administrators'-accounts losse accounts en groepen aangetroffen waarvan de rechten 'door elkaar lopen'. Daardoor kunnen accounts op verschillende manieren dezelfde rechten verkrijgen, dat is ongewenst. Van 28 accounts met admin-rechten zijn 16 met een wachtwoord dat ouder is dan een jaar. 6 admin accounts zijn langer dan een jaar niet gebruikt, maar kunnen nog wel actief gebruikt worden. Tot slot zijn 9 serviceaccounts lid van een beheerdersgroep en dat is ook ongewenst.

Voorts is in het kader van de AD audit een aantal testen uitgevoerd op de inrichting en configuratie van de Active Directory. Daarbij zijn risico's gevonden waarvan 9 van een hoog niveau zijn, 6 gemiddeld.

Niet consequent toepassen wachtwoordbeleid

Er zijn bij deze AD audit kritische kwetsbaarheden gevonden. Een aantal van deze kwetsbaarheden lijkt voort te komen uit het niet consequent toepassen van het wachtwoord beleid.

8.2.3 Inlooptest/Mystery guest

Inlooptest/Mystery guest

In landelijke richtlijnen is opgenomen dat er toegangsbeveiliging aanwezig is op de werk-, server- en technische ruimten van overheidsgebouwen. Dit geldt ook voor de ruimtes in gemeenten waar reisdocumenten zich bevinden en waar persoonsgegevens worden verwerkt. Op 12 oktober 2023 is in het kader van het rekenkameronderzoek een inlooptest met behulp van mystery guests uitgevoerd in het gemeentehuis van Zeist. Getracht is ongeautoriseerd toegang te krijgen toegang te krijgen tot verdiepingen en ruimtes die gesloten zijn voor onbevoegden en om ongestoord werkzaamheden op een (eigen/onbewaakt) computersysteem uit te voeren.

Kritisch risico-doel niet behaald

Het doel dat vooraf beoordeeld is als een risico met hoge impact is niet behaald, namelijk toegang te krijgen tot de serverruimte. Eén van de doelen met een gemiddeld risico is ook niet behaald, namelijk toegang krijgen tot

[42] Advanced Encryption Standard (AES) is een (cryptografische) versleutelingstechniek.

de raadzaal. Wel behaald zijn twee doelen met hoog risico-, twee met een gemiddeld risico- en een met een laag risiconiveau. Daarmee hebben de mystery guests onder andere ongeoorloofd toegang gekregen tot verdiepingen die gesloten zijn voor onbevoegden en technische ruimtes.

Vrijwaringsverklaring laten zien

In één ruimte zijn de mystery guests kritisch aangesproken door een medewerker van de IT-afdeling. Zij waren daardoor genoodzaakt de vrijwaringsverklaring te laten zien.[43]

Het is de mystery guests gelukt om met personeel mee te lopen naar de niet-publieke ruimte zonder aangesproken te worden. Vanuit deze ruimte kon er vrij rondgelopen worden zonder aangesproken te worden. Wel maakte de open uitstraling van het pand en de omgeving het lastig voor de mystery guests zich ergens echt op hun gemak te voelen.

Verder zijn de mystery guests niet aangesproken op hun aanwezigheid en het niet zichtbaar hebben van een bezoekerspas. Enkel bij het actief vragen naar toegang tot de kamer van de burgemeester is kort het ontbreken van de bezoekerspas ter sprake gekomen. Dit heeft verder geen gevolgen gehad waarna de mystery guests toegang hebben gekregen tot de burgemeesters-kamer. De mystery guests hadden diverse keren toegang tot deuren, waarbij een toegangscontrole aanwezig was, maar deze niet nodig bleek om door te kunnen lopen.

Ook zijn tijdens het bezoek werkplekken gecontroleerd op onbeheerde badges, documenten of ontgrendelde computers. Er is één werkplek gevonden met documenten en één onbeheerde werkplek die niet vergrendeld was. Toegang tot technische ruimtes is vrijwel nergens verkregen, behalve bij de technische ruimte voor de lucht/warmte voorziening. Hier stond ook een ingeschakelde vaste computer. Dit zou bij uitstek een plek zijn waar ongezien voor langere tijd hardware, ten behoeve van spionage, gebruikt zou kunnen worden. De organisatie is naar aanleiding van de rapportage van de testen daarop geattendeerd.

De mystery guests waren in staat zonder aangesproken of gestopt te worden het gemeentehuis te verlaten. Naar aanleiding van de test zijn verbeterpunten geconstateerd op de fysieke beveiliging en het risico-bewustzijn van de medewerkers. Op basis van de resultaten van de inlooptest met mystery guests wordt het risico op gemiddeld ingeschat.

Samenvatting pentesten

De gemeente voert zelf testen op de systemen uit, de laatste was in 2021. Daarbij zijn risico's aangetroffen, waaronder één kritiek risico, die in verbeterplannen zijn geadresseerd. Uit de pentesten, uitgevoerd in november 2023 door een ethisch hacker in opdracht van de rekenkamer, zijn ook risico's gebleken. De ethisch hacker vond geen risico's in het wifi-netwerk. Op basis van de interne pentest wordt het risico dat de gemeente

[43] Een beperkt aantal medewerkers is op de hoogte van het bezoek van de mystery guests, om de test zo realistisch mogelijk te laten zijn. Om escalatie te voorkomen hebben de mystery guests een vrijwaringsverklaring die uitleg geeft over de test en contactgegevens van de medewerkers die op de hoogte zijn van de test.

ten tijde van de test liepen als hoog ingeschat. In de Active Directory audit zijn kwetsbaarheden gebleken die te maken hebben met het niet consequent toepassen van het wachtwoordbeleid. En voorts blijkt uit het bezoek van de mystery guests het risico op gemiddeld.

De resultaten van de testen zijn gedeeld met de CISO. De ethisch hacker heeft uitleg gegeven over diens bevindingen en mede op basis daarvan heeft de gemeente verbetermaatregelen getroffen.

8.3 Toegang tot gevoelige informatie

De vraag of het mogelijk is om oneigenlijke toegang te krijgen tot gevoelige informatie die de gemeente Zeist in beheer heeft is deels met de boven-genoemde pentesten beantwoord. Met de testen is aangetoond dat de gemeente hierop risico's loopt. Uit de interviews, die afgenomen zijn na afronding van de pentesten, blijkt dat de medewerkers van afdeling IV zich ervan bewust zijn dat ze het nodige te doen hebben om de systemen veilig te houden. De met de tests aangetoonde risico's zijn intern met de ethisch hacker besproken en de te nemen maatregelen zijn geprioriteerd in een verbeterplan opgenomen.

0-tolerance

Op het gebied van informatiebeveiliging is het zaak om intern en extern op de systemen een 'zerotolerance'-beleid te hanteren. In principe is alle verkeer van buiten verdacht, behalve als die kan aantonen te vertrouwen te zijn. De poort is meestal goed beveiligd met een firewall en virusscanners. En als een medewerker inlogt op het systeem kan deze dat alleen met gebruik van gebruikersnaam en bijbehorend wachtwoord, versterkt met een extra authenticatie (2FA of MFA).[44]

De ingelogde medewerker heeft ook alleen toegang tot de systemen zover als de autorisaties die zijn toegekend toelaten. Intern is er een zero-tolerance beleid, zodat er drempels voor het interne verkeer tussen de verschillende segmenten van het systeem zijn opgeworpen. Een hacker die binnen is gekomen kan niet zonder de benodigde autorisaties die drempels nemen. Daarom is minimalisatie van uitgebreide autorisaties belangrijk.

Intern wordt ook een systeem van Microsoft gebruikt dat afwijkend verkeer van een ingelogde laptop of computer kan detecteren. Die aansluiting wordt dan door de afdeling Informatievoorziening (IV) uit het netwerk gehaald. Soms is dat onterecht, en dan kan de medewerker even niet werken.

Monitoring

In de ICT-samenwerking met Nieuwegein is in eerste instantie een firewall buiten de scope van de contracten gehouden. Uiteindelijk is deze toch gezamenlijk extern aanbesteed als onderdeel van de ICT-infrastructuur. De

[44] Multi factor authenticatie (MFA) is een authenticatie of verificatie methode waarbij twee of meer stappen succesvol doorlopen moeten zijn om ergens toegang toe te krijgen, zoals naast het gebruik van een wachtwoord het gebruik van een token of biometrisch gegeven.

instellingen van de firewall worden door de gemeente bepaald, de externe partij monitort. Het is niet alleen noodzaak oneigenlijke gebruik proberen tegen te gaan, het is ook nodig verdacht verkeer zo vroeg mogelijk te detecteren en maatregelen te nemen. Daarvoor zijn hulpmiddelen zoals een SIEM/SOC [45] beschikbaar. In VNG-verband is getracht een aanbesteding voor een dergelijke oplossing te organiseren. Dat is helaas mislukt en daar hebben veel gemeenten veel last van. De VNG is bezig een nieuwe aanbestedingsprocedure voor een SIEM/SOC op te starten. Ondertussen hebben de gemeenten Zeist en Nieuwegein een hardwarematige tussenoplossing geïmplementeerd. Een vraagstuk is evenwel hoe de gemeente de monitoring en de response 24/7 adequaat kan borgen. Een van de meer robuuste ingrepen bij een hackaanval is de hoofdstekker eruit te trekken. Daar is het hoofd van de afdeling IV toe gerechtigd, los van de hiërarchische lijn.

Samenvatting

De pentesten geven al een beeld van de mogelijkheid tot oneigenlijke toegang tot informatie. Van buitenaf is de toegang goed beveiligd met firewalls en virusscanners en intern zijn ook drempel opgeworpen. Toegang kan verkregen worden met twee factor authenticatie (2FA). Om verdacht verkeer te monitoren en daarop in te kunnen grijpen is een hardeware-matige oplossing gekozen, in afwachting van een geslaagde aanbesteding in VNG-verband van een applicatie (SIEM/SOC).

8.4 Logging

Het geautomatiseerd registreren van gegevens bedoeld om bij te houden welke gebeurtenissen of handelingen op een systeem hebben plaats-gevonden heet logging. In de AVG is dit niet expliciet als verplichting opgenomen, maar het is een noodzakelijke maatregel om bewijslast te hebben bij oneigenlijke toegang tot gegevens.

In Zeist zijn de belangrijkste applicaties, de ‘kroonjuwelen’, gedefinieerd en wordt het verkeer op die applicaties in logbestanden bijgehouden. Dat geldt voor de Suwinet en DigiD, waarop landelijke toezichthouders in het kader van ENSIA zwaar op controleren. Ook op de systemen met een financiële impact wordt logging bijgehouden. Dus niet op alle systemen staat logging standaard aangevinkt, maar gelet op de aanwezige capaciteit is een afweging gemaakt welke belangrijke systemen en applicaties wel worden gelogd.

Controle op logging

Controle van de loggingbestanden vindt beperkt plaats, omdat de benodigde capaciteit daarvoor ontbreekt. De functioneel beheerder de loggingbestanden 1 tot 2 keer per jaar of wanneer zich een afwijking voordoet. Hierboven is al gerefereerd aan een systeem dat het netwerk- en

[45] Security Information & Event Management (SIEM) en Security Operations Center (SOC) is software die computerdreigingen en verdacht verkeer op systemen detecteert en monitort.

werkplekverkeer monitort op verdacht verkeer. Uit de logging komen grote bestanden die het verkeer op de systemen inzichtelijk maken. Volgens respondenten kan het controleren van de loggingbestanden, daarop acteren en vastleggen beter. Dat is een kwestie van capaciteit om de systemen wat betreft logging bij te houden.

Samenvatting

Er is een afweging gemaakt op welke applicaties het verkeer gelogd wordt en op welke niet. Die afweging heeft te maken met de beschikbare capaciteit om de loggingbestanden te checken en applicaties waarin veel bijzondere persoonsgegevens worden verwerkt. Het controleren, reageren en vastleggen behoeft verbetering.

9 Autorisatiebeleid

Onderzoeksvraag 9	Hoe is het autorisatiebeleid vorm gegeven?

Toekennen van rechten	Het autorisatiebeleid met betrekking tot toegang tot applicaties en gegevens is geregeld in het in- en uitdienstproces, waarvan HRM proceseigenaar is. Voor het toekennen van rechten bij de belangrijkste applicaties is volgens respondenten een autorisatiematrix aanwezig. Dat is bijvoorbeeld bij het financiële systeem AFAS en de Gemeentelijke Basisadministratie (GBA). De toedeling van de rechten gebeurt door de functioneel beheerder, na toekenning door het afdelings- of teamhoofd. Daarna moet de applicatiebeheerder van de afdeling Informatievoorziening (IV) de rechten daadwerkelijk aanzetten, na een melding in Topdesk.
Instroom	Bij instroom van een nieuwe medewerker wordt het proces meestal correct doorlopen, daar de nieuwe medewerker met de rechten in een nieuwe functie aan de slag moet. Soms gaat dat niet goed, volgens een van de respondenten. In een enkel geval wordt een medewerker of externe aangenomen zonder dat de afdeling IV daarvan op de hoogte is.
Door- en uitstroom	Bij doorstroom van een medewerker naar een andere functie of bij uitstroom uit de gemeentelijke organisatie moeten de toegekende autorisaties verwijderd worden. Bij doorstroom moet het nieuwe teamhoofd nieuwe autorisaties goedkeuren. En er moet een signaal naar Topdesk en afdeling IV voor het daadwerkelijk toekennen van de rechten en naar personeelszaken bijvoorbeeld om te checken of voor de nieuwe functie een (nieuwe/andere) VOG nodig is. Het kan voorkomen dat de aanwezige autorisaties na-ijlen op de daadwerkelijke situatie. In die gevallen betekent het dat er rechten zijn toegekend die medewerkers gezien hun functie/rol niet meer zouden mogen hebben.
Controle	Er hoort een periodieke controle te zijn op toegekende autorisaties. Dat gebeurt bij Suwinet en DigiD, de twee applicaties die in het kader van ENSIA door landelijke toezichthouders strikt worden gecontroleerd. Volgens respondenten gebeurt dat bij andere belangrijke applicaties vier keer per jaar, bij andere applicaties 2 of 1 keer per jaar. Bij de applicaties waar een autorisatiematrix aanwezig is moeten de daadwerkelijke autorisaties vergeleken worden met de rollen/functies van de medewerkers. Zoals begin 2023 omschreven in een interne audit op het Zaaksysteem subsidieproces zijn de aandachtspunten bij de controle: - alle medewerkers met autorisaties zijn actief in dienst van de gemeente of hebben rechten op basis van een met de leverancier vastgelegde afspraak; - de werkelijke aanwezige rechten horen bij de functie zoals vastgelegd in de autorisatiematrix.

- de genoemde functiescheidingen zijn niet doorbroken.
- afwijkingen worden gedocumenteerd en opgevolgd door een verzoek tot wijziging van autorisaties (bijvoorbeeld door het aanmaken van een Topdesk ticket).

Toch laten controles zien dat het proces van toekennen en afmelden van autorisaties niet vlekkeloos verloopt.

Accountantscontrole

Zo blijkt onder andere uit de controles door de accountant (zie daarvoor ook hoofdstuk 7). Bij de interimcontrole 2022 constateerde deze dat de autorisaties niet altijd in overeenstemming zijn met het mandaat. De accountant constateert verbeterpunten op het gebied van gebruikers-beheer, onder andere het formaliseren van de procedures over toekennen, wijzigen en intrekken van gebruikersrechten. "… functioneel beheer en technisch beheer [zijn] in dit proces afhankelijk … van de teams voor het doorgeven van wijzigingen en uitdienstmeldingen en dat dit niet altijd tijdig gebeurt."

Ook constateerde de accountant een verbeterpunt met betrekking tot het aantal 'generieke' accounts met uitgebreide rechten. Dat is in overeenstemming met de bevindingen uit de AD audit die in opdracht van de rekenkamer is uitgevoerd (zie §8.1.2). De accountant stelde dan ook dat de uitvoering van de controles op de juistheid van de autorisaties een aandachtspunt is.

Samenvatting

Medewerkers moeten geautoriseerd worden om toegang tot informatie en applicaties te krijgen. Er is een proces vastgelegd waarbij de autorisaties worden toegekend en periodiek dienen te worden gecontroleerd. Op een beperkt aantal applicaties is een autorisatiematrix aanwezig, waarmee de toekenning op basis van rol en functie geschiedt. De verdere uitrol van een dergelijke matrix staat voor 2024 op de rit. Uit de controles, onder andere van de accountant en in het kader van het rekenkameronderzoek, blijkt dat de juistheid van autorisaties een aandachtspunt is.

Bijlage 1. Gebruikte termen en afkortingen

2FA	Zie MFA
Applicatie	Softwareprogramma, zoals SUWInet
AVG (GDPR)	Algemene Verordening Gegevensbescherming, Europese regelgeving die de privacyregels in de Europese lidstaten harmoniseert
BIG	Baseline Informatiebeveiliging Gemeenten, maatregelen voor de informatiebeveiliging bij gemeenten, in 2013 als standaard afgesproken in VNG-verband. Deze is in 2019 vervangen door de Baseline Informatiebeveiliging Overheid (BIO)
BIO	Baseline Informatiebeveiliging Overheid
BIV	Beschikbaarheid – Integriteit – Vertrouwelijkheid. Termen waarop de beveiligingsrisico's van de informatie/applicaties zijn geënt
Blackbox pentest	Zie Pentest
CERT	Computer Emergency Response Team, multidisciplinair samengesteld team dat kan acteren op incidenten en crises
CIO	Chief Information Officer
CISO	Chief Information Security Officer
Cloud	De cloud staat voor een netwerk van computers die een soort 'wolk van computers' vormt, waarbij de eindgebruiker niet weet op hoeveel of welke computer(s) de software draait of waar die computers precies staan
Dataclassificatie	Betekent inzicht krijgen in de beschikbaarheid, de integriteit en de vertrouwelijkheid van de door of namens de organisatie beheerde en verwerkte informatie (BIV)
DigiD	Digitale Identiteit
DPIA	Data protection impact assessment, analyse op risico's in verband met privacy en gegevensbescherming bij verwerkingsprocessen. Onder de AVG verplicht bij gegevensverwerking met waarschijnlijk een hoog privacy risico.
ENSIA	Eenduidige Normatiek Single Information Audit, eenmalige informatieverstrekking en eenmalige IT-audit voor de horizontale (richting gemeenteraad als toezichthouder) en verticale verantwoording (richting landelijke toezichthouders)
FG	Functionaris gegevensbescherming, verplicht voor overheden.
GAP	Is de Engelse term voor 'kloof'. Dat betekent hier het verschil tussen de bestaande situatie en de gewenste situatie
GAP-analyse	Controle of en in welke mate de maatregelen uit de BIO geïmplementeerd zijn
GDPR	General Data Protection Regulation (zie ook AVG)
GR	Gemeenschappelijke regeling
GRC	Tool om de Governance, Risk and Compliance (GRC) op informatiebeveiliging en privacy te monitoren
Greybox pentest	Zie Pentest
IAM	Zie Identity and Access management
IBD	Informatiebeveiligingsdienst voor gemeenten
ICT	Informatie- en communicatietechnologie
Identity and Access management (IAM)	IAM regelt dat de juiste medewerkers het juiste toegangsniveau hebben tot de netwerken en de daarin opgeslagen of verwerkte gegevens. Gebruikersrollen en toegangsrechten worden via een IAM-systeem gedefinieerd en beheerd.
ISMS	Information Security Management System
Logging	In bestanden vastleggen welk dataverkeer over een netwerk gaat. Zo wordt onder andere vastgelegd wie toegang had tot welke persoonsgegevens.
MFA	Multi factor authenticatie is een authenticatie of verificatie methode waarbij twee of meer stappen succesvol doorlopen moeten zijn om ergens toegang tot te krijgen, zoals naast het gebruik van een wachtwoord het gebruik van een token of biometrisch gegeven
NBA	De koninklijke Nederlandse Beroepsorganisatie van Accountants
NOREA	De Nederlandse Organisatie van Register EDP-Auditors

Open source intelligence onderzoek (Osint)	Osint is een techniek om online sporen die op het eerste gezicht verborgen lijken naar de oppervlakte te halen. De techniek maakt gebruik van openbare bronnen.
P&C-cyclus	Planning & Control cyclus
PDCA	Plan-Do-Check-Act beleidsleercyclus
Pentest	Een pentest of penetratietest is een toets van een of meer computersystemen op kwetsbaarheden, waarbij deze kwetsbaarheden gebruikt kunnen worden om in deze systemen in te breken. Een whitebox test is een teststrategie waarbij de ethische hackers kennis hebben van de technische infrastructuur en systemen en met behulp van die kennis technische zwakheden trachten op te sporen. Dit in tegenstelling tot black- of greybox testen, waarbij de hackers vooraf respectievelijk geen of beperkte kennis hebben van de systemen
Phishing mail	Vorm van internet oplichting en fraude, door middel van een vals e-mail bericht 'hengelen' naar inlog- of andere persoonsgegevens
PO	Privacy officer
Role based access control (Rbac)	Concept waarmee toegang tot gegevens en systemen geschiedt op basis van rollen en functies van de medewerkers. Dat is het concept waarmee Identity Access Management (IAM) wordt uitgevoerd.
SAAS	Software-as-a-Service, is een model waarbij softwaretoepassingen via internet worden aangeleverd.
SIEM/SOC	Security Information & Event Management (SIEM) en Security Operations Center (SOC) is software die computerdreigingen en verdacht verkeer op systemen detecteert en monitort.
Suwinet	Gemeenschappelijke elektronische Voorziening Suwi (Wet structuur uitvoering werk en inkomen), of GeVS, ook wel Suwinet genoemd. Is een digitale infrastructuur die is ontwikkeld om ervoor te zorgen dat de Suwipartijen (UWV, SVB en gemeenten) gegevens met elkaar kunnen uitwisselen
TISO	Technical Information Security Officer
TPM	Third Party Memorandum. Verklaring dat een derde partij, die de gegevens voor de gemeente verwerkt, voldoet aan de geldende richtlijnen over informatieveiligheid
Verwerkingsregister	Register waarin de gemeente bijhoudt welke persoonsgegevens de gemeente en de verwerkers die deze inschakelt verwerkt
VNG	Vereniging Nederlandse Gemeenten
VNG Realisatie	Kwaliteitsinstituut van de VNG (voorheen KING)
Whitebox pentest	Zie pentest

Bijlage 2. Onderzoeksvragen en normen

De onderstaande normen zijn opgesteld op basis van de normen van de BIO (inclusief de 10 bestuurlijke principes informatiebeveiliging), AVG, Agenda Digitale Veiligheid 2020-2024 VNG. Mogelijk kunnen de gemeentelijke beleidsplannen aanvullende normen opleveren, waaraan de uitvoering van het informatiebeveiligings- en privacybeleid getoetst wordt.

Onderzoeksvragen	Normen
1. Heeft de gemeente Zeist op informatie-veiligheid de risico's voldoende in kaart gebracht en op basis daarvan beleid geformuleerd?	- Er worden met voldoende frequentie GAP- en risicoanalyses uitgevoerd. In de risicoanalyses zijn de belangrijkste risico's geïdentificeerd. - De gemeente beschikt over een actueel overkoepelend informatiebeveiligingsbeleid dat op onderdelen is uitgewerkt in specifieke procedures en/of richtlijnen. De inhoud van het informatiebeveiligingsbeleid sluit aan op good practices, zoals de BIO en relevante wet- en regelgeving (zoals de AVG). - De gemeente beschikt over een actueel informatie-beveiligingsplan met concrete activiteiten om nader invulling te geven aan diverse onderdelen van het informatie-beveiligingsbeleid. Op basis van de activiteiten is er een urenraming en budget opgesteld. - De gemeente besteedt 10% van het ICT-budget aan maatregelen ter bevordering van informatieveiligheid. - Taken en verantwoordelijkheden rond informatiebeveiliging en de bescherming van (bijzondere) persoonsgegevens zijn duidelijk belegd in de organisatie. - De functionarissen op informatiebeveiliging en privacy zijn goed gepositioneerd om hun rol te kunnen vervullen.
2. Wordt de gemeenteraad goed geïnformeerd over de risico's en beheersingsmaatregelen?	- Het college legt verantwoording af over het informatiebeveiligingsbeleid, de gemaakte afspraken en geplande activiteiten, volgens de BIO. - De raad kan zijn kaderstellende en controlerende rol invullen op basis van de aangereikte informatie.
3. Krijgen medewerkers goede uitleg en ondersteuning om veilig te werken?	- De gemeente heeft een bewustwordingsprogramma opgezet voor medewerkers, in vaste dienst en externe inhuur. - In het inwerkprogramma voor nieuwe medewerkers wordt aandacht besteed aan informatiebeveiliging en privacy. - Informatie en protocollen/richtlijnen over informatie-beveiliging en privacy zijn makkelijk toegankelijk. - De functionarissen op informatiebeveiliging en privacy zijn bereikbaar voor medewerkers.
4. Hoe communiceert de gemeente met betrokkenen en inwoners over datalekken?	- De gemeente heeft een protocol datalekken opgesteld dat voldoet aan de eisen van de AVG; - De gemeente rapporteert in het kader van de P&C-cyclus over datalekken.
5. Hoe controleert de gemeente op naleving van veilig werken en het voorkomen van beveiligingsincidenten?	- In het informatiebeveiligingsbeleid is beschreven hoe invulling wordt gegeven aan de PDCA-cyclus rond informatiebeveiliging en privacy.
6. Welke penetratietesten voerde de gemeente uit? Zo ja, zijn verbeterplannen opgesteld naar aanleiding van de pentesten en zijn deze opgevolgd?	- De gemeente laat jaarlijks testen en audits uitvoeren om de beveiliging van de systemen te testen - De gemeente stelt op basis van de resultaten uit de pentesten concrete verbeterplannen op en volgt deze op.

7. Is het mogelijk om oneigenlijke toegang te krijgen tot gevoelige informatie die de gemeente in beheer heeft?	- Het totaal aan beveiligingsmaatregelen geeft voldoende waarborgen voor een goede bescherming van de (bijzondere) persoonsgegevens die de gemeente in beheer heeft - De gemeente heeft afdoende technische maatregelen getroffen om ongeautoriseerde interne en externe toegang te voorkomen.
8. In hoeverre wordt in de organisatie van de gemeente Zeist vastgelegd wie wanneer toegang vraagt tot bestanden met gevoelige informatie (het loggen)?	- Op de systemen waarin (bijzondere) persoonsgegevens worden verwerkt is logging aanwezig. - De gemeente heeft de capaciteit om de loggingbestanden regelmatig te controleren.
9. Hoe is het autorisatiebeleid vorm gegeven?	- De gemeente werkt met een autorisatiematrix, of vergelijkbaar Identity Access Managementsysteem (IAM) waarin toegang tot informatie op basis van rollen wordt toegekend. - Bij in-, door- en uitstroom van medewerkers worden de autorisaties aangepast. - De autorisaties worden regelmatig op juistheid gecontroleerd.
10. Welke adviezen zijn te geven aan college, gemeentelijke organisatie en de gemeenteraad?	Geen normen.

Bijlage 3. Lijst van geraadpleegde stukken en respondenten

Geraadpleegde stukken

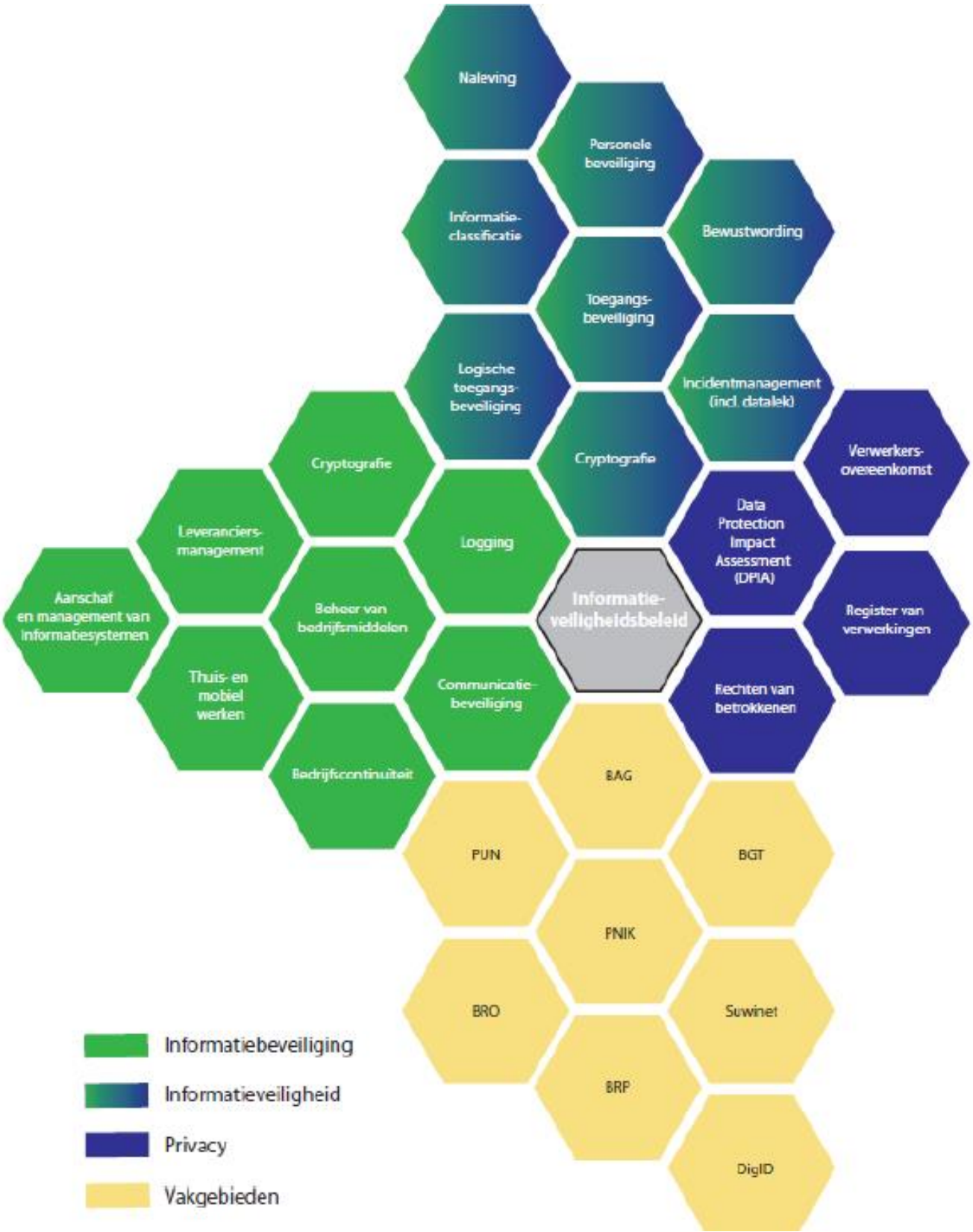
- Accountantsverslag 2022 Gemeente Zeist Concept 25-05-2023
- Analyse Holmes Gemeente Zeist april 2022
- Bijlage 1. Managementletter Zeist 2022
- Beleidsnotitie Bedrijfs Continuïteits Management BCM
- Bestuurlijke rapportage Informatieveiligheid 2020, Jaarplan informatieveiligheid 2021-2022
- Bijlage 2 BCM Crisisstructuur en opschaling
- Bijlage beleidsnotitie BCM Checklist cybercrisis
- Collegevoorstel ENSIA 2022 inzake informatieveiligheid
- Coordinated Vulnerability Disclosure 2023
- CV BCM Cybersecurity
- CV Beleid Informatieveiligheid en privacy
- CV ENSIA rapportage 2021
- CV Visiedocument Een goed leven in Zeist - ook digitaal _ Jaarverslag FG
- Deelnemersverslag peer to peer gesprek digitale veiligheid tussen Veere en Zeist
- Def Rapport AFAS Zeist V1.0
- Def Rapport Subsidieproces Zeist
- Definitief Rapport Audit ITGC
- DigiD aansluitbeleid - Beveiligingsplan Zeist 2022
- ENSIA Collegeverklaring 2022 - Gemeente Zeist
- FG-verslag_GZST_2022-2023
- Gemeente Zeist - ENSIA 2021 compleet
- Informatieveilig 2030 – De juiste dingen goed doen! 10-11-2023
- Monitoring bevindingen VIC en Accountant 2021 + KB
- Rapportage - pentest Blackbox external threat v0.1
- RIB Visiedocument Een goed leven in Zeist - ook digitaal _ Jaarverslag FG
- Strategisch Informatieveiligheidsbeleid Zeist 2022-2026
- Strategisch Privacybeleid Zeist 2022-2026
- V 1.0 Proceskaart Proces 7 Proces VWO's (Verwerkingsovereenkomsten)
- V 1.0 Processtroom Proces 7 VWO's
- V 1.0 Toelichting processtappen Proces 7 VWO's
- V1.0 Proceskaart Proces 11 Proces Melden Datalekken en Beveiligingsincidenten
- V1.0 Processchema Proces 11 Proces Melden Datalekken en Beveiligingsincidenten
- V1.0 Toelichting Processtappen Proces 11 Proces Melden Datalekken en Beveiligingsincidenten
- vastgesteld voorstel 29 maart 2022
- Veilig werken onboardingsweek
- Verklaring van toepasselijkheid januari 2023
- Visie en missie subopgave veilig werken 2021

- Visiedocument Een goed leven in Zeist - ook digitaal 2023

Respondenten

- Bedrijfskundig adviseur
- Chief Information Security Officer en strategisch adviseur
- Coördinator functioneel beheer
- Functionaris gegevensbescherming
- Informatieadviseur
- Kwaliteitsmedewerker HR
- Kwaliteitsmedewerker Sociaal Domein
- Privacyofficer
- Proces- en informatiebeheerder Informatieveiligheid
- Teamleider Sociaal Domein
- Teammanager Control en concerncontroller
- Teammanager Informatieveiligheid
- Teammanager P&O

Bijlage 4. Richtlijnen/procedures voor Informatiebeveiliging en privacy



Bijlage 5. Volwassenheidsniveau NOREA

Bron: Handreiking bij Volwassenheidsmodel Informatiebeveiliging, januari 2019, Nederlandse Nederlandse Beroepsorganisatie van Accountants.

Niveau	Naam	Omschrijving	Indicatieve criteria
1	Initieel	Beheersingsmaatregelen zijn niet of gedeeltelijk gedefinieerd en/of worden op inconsistente wijze uitgevoerd. Grote afhankelijkheid van individuen.	• Geen of beperkte controls geïmplementeerd. • Niet of ad-hoc uitgevoerd. • Niet /deels gedocumenteerd. • Wijze van uitvoering afhankelijk van individu.
2	Herhaalbaar	Beheersingsmaatregelen zijn aanwezig en worden op consistente en gestructureerde, maar op informele wijze uitgevoerd.	• Control is geïmplementeerd. • Uitvoering is consistent en standaard. • Informeel en grotendeels gedocumenteerd.
3	Gedefinieerd	Beheersingsmaatregelen zijn gedocumenteerd en worden op gestructureerde en geformaliseerde wijze uitgevoerd. De uitvoering is aantoonbaar en wordt getoetst.	• Control gedefinieerd o.b.v. risico assessment. • Gedocumenteerd en geformaliseerd. • Verantwoordelijkheden en taken eenduidig toegewezen. • Opzet, bestaan en effectieve werking aantoonbaar. • Rapportage van uitvoering van beheersingsmaatregel aan management. • Effectieve werking van controls wordt periodiek getoetst, gebaseerd op het risicoprofiel van de organisatie. • De toetsing toont aan dat de control effectief is.
4	Beheerst en meetbaar	De effectiviteit van de beheersingsmaatregelen wordt periodiek geëvalueerd.	• Periodieke (control) evaluatie en opvolging vindt plaats. • Evaluatie is gedocumenteerd en geformaliseerd. • Frequentie waarop wordt geëvalueerd is gebaseerd op het risicoprofiel van de onderneming en is minimaal jaarlijks. • Rapportage van de evaluatie aan management.
5	Continu verbeteren	De beheersingsmaatregelen zijn verankerd in het integrale risicomanagement raamwerk, waarbij continu gezocht wordt naar verbetering.	• Continu evalueren van de beheersingsmaatregelen om de effectiviteit te verbeteren. Gebruik makend van resultaten uit Self-assessment, gap en root cause analyses. • De getroffen beheersingsmaatregelen worden gebenchmarkt en zijn 'Best Practice' in vergelijking met andere organisaties. • Real time monitoring. • Inzet automated tooling.