- Rapport –

Informatiebeveiliging en privacy Gemeente Zutphen

Rekenkamercommissie Zutphen

16 augustus 2023

Auteur: drs. Etienne Lemmens

Prae Advies en onderzoek, Utrecht

Prae BV, Buys Ballotstraat 35, 3572 ZT Utrecht | T 06-11226755 | E info@prae-advies.nl | W www.prae-advies.nl
KvK 321 249 60 | BTW NL8182.21.227 | IBAN: NL93 INGB 0004 9860 86

Inhoudsopgave

Samenvatting, conclusies en aanbevelingen

Samenvatting

Inleiding

Gemeenten verwerken in ICT-systemen veel gegevens en na de decentralisaties met name van grote kwetsbare groepen inwoners. Door toenemende bedreigingen blijken gemeenten kwetsbaar op het gebied van informatiebeveiliging en gegevensbescherming, zoals bleek uit hacks en datalekken bij overheden en bedrijven/instellingen. Gemeenteraden, verantwoordelijk voor kaderstelling en controle van het beleid, zien het onderwerp informatieveiligheid steeds meer op de agenda komen. Dat is een van de redenen dat de Rekenkamercommissie Zutphen (rekenkamercommissie) in 2022 informatiebeveiliging en privacy heeft laten onderzoeken.

De rekenkamercommissie vindt dat informatiebeveiliging en privacy belangrijk is. De rekenkamercommissie realiseert zich tegelijkertijd dat dit een nogal technisch onderwerp is wat voor alle raadsleden niet altijd even toegankelijk is. Het betreft een onderwerp met veel technische termen en veelal een eigen jargon. De rekenkamercommissie heeft getracht dit onderwerp op een zo toegankelijk mogelijk wijze in dit rapport tot uitdrukking te brengen. Verder heeft de REKENKAMERCOMMISSIE technische termen toegelicht in een voetnoot en in bijlage 1 is een verklarende woordenlijst opgenomen.

Informatiebeveiliging

Informatiebeveiliging gaat over het geheel aan preventieve, detectieve 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).[1] De BIO bevat maatregelen die gemeenten op basis van een risicoanalyse kunnen nemen om aan het basisniveau voor informatiebeveiliging te voldoen.

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

[1] 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). De baseline is gebaseerd op de kwaliteitsnormen NEN-ISO/IEC 27001:2017 en de NEN-ISO/IEC 27002:2017.

Algemene Verordening Gegevensbescherming (AVG), is sinds mei 2018 van kracht.

Onderzoeksvraag

Met dit rapport wil de rekenkamercommissie de gemeenteraad van Zutphen inzicht geven in de stand van zaken met betrekking tot beleid en uitvoering van informatiebeveiliging en privacy. De volgende vraag staat in dit onderzoek centraal:

> *Heeft de gemeente Zutphen de informatiebeveiliging en gegevens-bescherming op orde?*

Het belang en de urgentie van Informatiebeveiliging en privacy (IB&P) neemt steeds meer toe. De gemeente Zutphen, zo heeft de rekenkamer-commissie ervaren in dit onderzoek, is zich hiervan bewust. De gemeente komt van ver, mede omdat in de afgelopen jaren bezuinigd is op middelen en mensen onder andere op deze terreinen. De gemeente heeft wat betreft beleid en uitvoering nog zeer veel te doen en stelt het nodige in het werk om aan leidinggevenden en medewerkers aandacht voor deze onder-werpen te vragen. Uitvoering van informatiebeveiligingsbeleid is nooit af, de dreigingen nemen toe en kwaadwillenden vinden steeds nieuwere manieren om ongeoorloofd toegang te krijgen tot informatie. Met dit rapport verwacht de rekenkamercommissie de raad te ondersteunen, zodat deze inzicht krijgt in de stand van zaken en kan bijdragen aan de verdere ontwikkeling van informatiebeveiliging en privacy in de gemeente Zutphen.

De rekenkamercommissie zal de bevindingen, conclusies en aanbevelingen uit dit onderzoek uitwerken aan de hand van de volgende vier onderzoeksvragen:

1. In hoeverre beschikt de gemeente Zutphen over een adequaat informatiebeveiligings- en privacybeleid?
2. Hoe wordt het beleid uitgevoerd en hoe wordt de uitvoering gemonitord?
3. In hoeverre zijn gegevens bij de gemeente beschermd tegen de toegang door onbevoegden?
4. Hoe wordt de gemeenteraad betrokken bij het informatiebeveiligingsbeleid?

Dit hoofdstuk wordt afgesloten met conclusies, aanbevelingen (punten waar extra aandacht voor gevraagd wordt) en aansporingen (punten waarop de gemeente aangespoord wordt om daar op te blijven inzetten.)

Onderzoeksvraag 1. In hoeverre beschikt de gemeente Zutphen over een adequaat informatiebeveiligings- en privacybeleid?

Strategisch Informatie

Strategisch informatiebeveiligingsbeleid is in 2020 vastgesteld voor de periode 2020-2024. Gezien de snelle ontwikkelingen is dat een te lange

Beveiligingsbeleid

periode en de gemeente is bezig met een update. De doelen, ambitie en verantwoordelijkheden en de ambitie zijn in het beleid geformuleerd. Ambitie is te voldoen aan de BIO, dat is de basisset aan maatregelen voor informatiebeveiliging. De analyse voor het jaarplan met activiteiten op informatiebeveiliging om te voldoen aan de BIO is uitgevoerd, maar ten tijde van het onderzoek nog niet vastgesteld. De gemeente heeft de laatste jaren moeten bezuinigen en geconstateerd is dat er nog veel te doen is en scherpe prioriteiten gesteld moeten worden.

Privacybeleid

Op gegevensbescherming is in 2018 een 0-meting gehouden. Met behulp van een extern bureau is het privacybeleid opgesteld. Dat is nog niet geüpdatet en door externe en interne organisatorische ontwikkelingen is het beleid verouderd. Jaarlijks wordt een jaarrapportage opgesteld met activiteiten op privacy voor het volgende jaar. Specifiek en alleen voor het sociaal domein is een handreiking privacy opgesteld.

Actieplan

Op informatiebeveiliging en privacy is begin 2022 het actieplan 'Actieplan Informatiebeveiliging en privacybescherming' opgesteld, met de bedoeling het niveau hierop in de gemeente te verhogen. Onder andere vanwege de constatering dat veel activiteiten uit het privacyplan uit 2018 niet waren gerealiseerd. De interim CISO [2] heeft medio 2022 een update opgesteld. In het actieplan zijn activiteiten opgenomen om te voldoen aan de ambitie, namelijk voldoen aan de normen van de BIO en AVG. De activiteiten worden gecoördineerd door de functionarissen op informatiebeveiliging en privacy (zie hierna bij 'Functies en positionering').

Een van de activiteiten met prioriteit in het Actieplan is het vergroten van bewustzijn en kennis bij medewerkers door trainingen.

Protocollen/richtlijnen

Ook in het Actieplan opgenomen is het op niveau brengen van de protocollen en richtlijnen die in het kader van informatiebeveiliging zijn voorgeschreven. Geconstateerd wordt dat er een deel van de noodzakelijke protocollen en richtlijnen beschikbaar is, maar een belangrijk deel ook niet. Zoals een volledig en integraal continuïteitsplan en een autorisatiebeleid. En de protocollen en richtlijnen die er zijn moeten deels ook geüpdatet moet worden. Een goed overzicht hierop was nog niet voorhanden tijdens het onderzoek. Met betrekking tot de AVG zij de meeste protocollen aanwezig en mist op onderdelen nog een element.

Functies en positionering

In het beleid zijn de rollen van de functionarissen op informatiebeveiliging en privacy beschreven en zij staan op intranet gepubliceerd. Recent zijn, mede vanwege de eerder genoemde bezuinigingen een adjunct bedrijfsvoering (CIO), teamleider I&A en een strategisch adviseur I&A gestart. De CISO wordt momenteel voor 0,6 fte interim ingevuld en deze is strategisch en onafhankelijk van de lijnorganisatie ingevuld, zoals

[2] CISO: Chief Information Security Officer

gebruikelijk. Het lag in de bedoeling de functie naar 0,7 fte uit te breiden. Ondanks de strategische positionering is de CISO nog ook op tactisch en operationeel niveau bezig.

Vanaf 2018 is voltijds een FG [3] aanwezig, die vanaf 1-1-2023 voor 0,8 fte werkzaam is. De FG is, evenals de CISO, strategisch en onafhankelijk van de lijn gepositioneerd. Op tactisch niveau wordt de FG bijgestaan door een privacy officer (PO) voor 0,45 fte en adviseur privacy voor 0,53 fte. Zij werken organisatiebreed, hoewel de adviseur privacy in eerste instantie gericht is op privacy in het sociaal domein. Ter ondersteuning van gegevensbescherming wordt erover gedacht om privacy ambassadeurs op te leiden en uren toe te wijzen.

Getracht wordt een aantal functies, met name de éénpitters zoals de CISO en FG, gezamenlijk met buurgemeenten in te vullen, zodat kennis gedeeld kan worden.

Overleggen

De PO en de adviseur privacy vormen samen het Team Privacy. De FG maakt daar overigens geen deel van uit. Driewekelijks is er een functionarissenoverleg waar de CISO, PO en adviseur privacy aan deelnemen. Daarnaast is een tweewekelijks overleg over informatiebeveiliging met de CIO, CISO, teamleider I&A en strategisch adviseur I&A. Dit overleg is de opvolger van de projectgroep 'Versterken privacybescherming en informatieveiligheid' die het Actieplan heeft opgesteld. Tevens is er een maandelijks overleg tussen CISO, teammanager I&A en de portefeuillehouder. De portefeuillehouder heeft geen structureel overleg met de FG. In urgente gevallen hebben de FG en de CISO een directe lijn naar de portefeuillehouder.

Bij een crisis kan ad hoc snel een crisisteam worden geformeerd. Afhankelijk van de situatie is dat met de CIO, teammanager I&S en systeembeheerders en eventueel benodigde functionarissen.

Rapportages

De FG stelt de verplichte jaarlijkse rapportage over gegevensbescherming op, gericht aan gemeentesecretaris en college. Dit verslag wordt evenwel niet mede gericht aan de privacy officer en adviseur privacy. Tevens rapporteert de FG indien nodig over lopende zaken. De CISO rapporteert op basis van de ENSIA[4]-rapportage aan college en via deze aan de raad over informatiebeveiliging en privacy.

Onderzoeksvraag 2. Hoe wordt het beleid uitgevoerd en wordt de uitvoering gemonitord?

Na het vaststellen van het beleid volgt de volgende stap, implementeren en uitvoeren van het beleid. Voor informatiebeveiliging en privacy is het

[3] FG: Functionaris Gegevensbescherming
[4] ENSIA staat voor Eenduidige Normatiek Single Information Audit

essentieel dat beleid en uitvoering gemonitord en getoetst worden, om te controleren of het afgesproken beleid daadwerkelijk in de praktijk werkt.

Draagvlak

Een van de bestuurlijke principes in het strategisch informatiebeveiligingsbeleid is dat het gemeentebestuur het belang van informatiebeveiliging uitdraagt. Draagvlak bij het bestuur voor informatiebeveiliging en privacy is groeiende, na tijden van bezuinigingen en mindere aandacht voor deze beleidsvelden. De portefeuilles op enerzijds informatiebeveiliging en privacy en anderzijds bedrijfsvoering en ICT zijn momenteel belegd bij twee collegeleden. En er is relatief recent een adjunct-directeur bedrijfsvoering aangetreden die specifieker aandacht heeft voor de onderwerpen informatiebeveiliging en privacy.

Bewustwording

Zoals aangegeven is bewustwording op de risico's bij medewerkers een van de geprioriteerde activiteiten in het Actieplan. Activiteiten zoals modules op e-learning en test phishing mails worden sinds 2022 aangeboden. Voor nieuwe medewerkers is een informatieboek met onder andere informatiebeveiliging en privacy als onderwerp. Vaak wordt aandacht voor informatiebeveiliging en privacy als een extra taak erbij ervaren, die afleidt van het 'echte' werk, mede omdat deze onderwerpen niet standaard als onderdeel van werkprocessen wordt meegenomen. Teams die al langer met persoonsgegevens werken zijn vaak meer risicobewust dan andere teams. Dat blijkt onder andere uit de casebeschrijving over het sociaal domein. Geconstateerd wordt dat het bij de teamleiders vaak nog ontbreekt aan een gevoel van urgentie die bewustwording te bevorderen.

Autorisaties

Het autorisatieproces, dat de toegang regelt van medewerkers tot informatie die zij nodig hebben voor hun werkzaamheden, en bijgevolg de toegang beperkt tot gegevens die zij niet in mogen zien. Dit proces is gekoppeld aan de in-, door- en uitstroom van medewerkers. Geconstateerd is dat op dit proces verbeteringen mogelijk zijn, zoals ook de accountant dat in het verleden constateerde. Er zijn verbeteringen aangebracht, maar de controle op de autorisaties kan nog verbeteren. Er staat om 2023 een structurele aanpak van het autorisatieproces op stapel, op basis van rollen/functies.

Derden en leveranciers

Elke verwerking van persoonsgegevens hoort in het verwerkingsregister te zijn opgenomen. En onder de contracten met derden die namens of voor de gemeente persoonsgegevens verwerken moeten verwerkersovereenkomsten liggen. De privacy officer moet de verwerkersovereenkomsten checken en in het register opnemen. De meeste medewerkers weten de privacy officer hiervoor te vinden. Bij de meeste aanbestedingen gaat het goed, maar er kan geen garantie gegeven worden dat dit bij alle aanbestedingen, onder andere onder de aanbestedingsgrens, het geval is.

Voor hoe om te gaan met gegevensverwerking in het sociaal domein is een specifieke handreiking opgesteld en zijn onder andere convenanten

gesloten met derden om persoonsgegevens uit te wisselen. Er is nog geen (periodieke) check op de naleving van de afgesproken regels.

DPIA's/WPG

De verplichte data impact protection assessments (dpia's) brengen risico's m.b.t. informatiebeveiliging en privacy in kaart op werkprocessen met een hoog privacy-risico. De teamleiders voeren de dpia's uit en de FG controleert. De taak om dpia's uit te voeren is de afgelopen tijd stil komen te liggen, mede door drukte bij de teamleiders. Ze zijn wel weer opgepakt, er zijn evenwel nog veel processen te gaan waarvan de risico's met een dpia in kaart moeten worden gebracht. Op de Wet politie gegevens (WPG) is in 2022 een audit uitgevoerd en met de verbeterpunten die daaruit naar voren kwamen gaat de gemeente aan de slag in 2023.

Managementsysteem

Voor de monitoring van de stand van zaken op informatiebeveiliging, onder andere voor het vullen van de ENSIA-rapportage, is onder andere een Information security management system (ISMS) aanwezig. Het ISMS is gekoppeld aan de beleidsleercyclus, de PDCA-cyclus. De teamleiders vullen die nog niet, waardoor de PDCA-cyclus niet goed wordt gevolgd. Ook het aanwezige managementsysteem op privacy wordt niet ten volle benut. Actie daarop is meegenomen in het Actieplan.

Taakvolwassenheid

Geconstateerd wordt dat op informatiebeveiliging en privacy veel ad hoc maatregelen worden genomen. Het bewustzijn op risico is groeiende, de beheersingsmaatregelen zijn grotendeels aanwezig, maar worden informeel en niet consistent en gestructureerd uitgevoerd. Ingeschat wordt dat de taakvolwassenheid gemiddeld tussen 1 en 2 op een schaal van 5 scoort en behoeft verbetering.

Monitoring

Voor de monitoring is een aantal instrumenten aanwezig. Bijvoorbeeld het melden door medewerkers van incidenten in Topdesk gaat over het algemeen goed. Geconstateerd wordt dat de analyse van de meldingen en verbeteracties effectiever kan. De accountant maakt in zijn rapporten/managementletters ook opmerkingen ten aanzien van de informatieveiligheid van de administratie, met name met het oog op de rechtmatigheid. De jaarrapportage van de FG over privacy en ENSIA over informatiebeveiliging en gegevensbescherming worden opgesteld door de CISO. ENSIA ziet toe op de audits op een aantal applicaties die bij de gemeente draaien. Ten aanzien van DigiD en Suwinet worden door de landelijke toezichthouders zware eisen gesteld met betrekking tot autorisaties en beveiliging. Over 2021 bleek de gemeente nog niet te voldoen aan alle eisen, onder andere op logging (zie hieronder bij de kantlijnkop 'Techniek') en controle.

Techniek	Op de techniek vindt ook monitoring plaats, onder andere door middel van logging.[5] In het kader van Suwinet is geconstateerd dat logginggegevens niet uitvoerig gecheckt worden. Dat geldt ook voor andere applicaties. Verder zijn er de reguliere beschermingsprogramma's aanwezig, zoals firewalls en virusscanners. Een applicatie voor detectie van verdacht verkeer is er niet. Resultaten van de testen in opdracht van de rekenkamer-commissie op de systemen volgen bij de beantwoording van vraag 3 hieronder.

Onderzoeksvraag 3.	In hoeverre zijn gegevens bij de gemeente beschermd tegen de toegang door onbevoegden?

Systemen	De gemeente moet in het kader van BIO jaarlijks de systemen op kwetsbaarheden (laten) testen. Dat is voor 2022 niet gedaan door middel van zogenoemde pentesten.[6] In 2022 is met medewerking van de provincie Gelderland wel een externe netwerk pentest uitgevoerd en een mystery guest op de hoofdlocatie van de gemeente. De verbeterpunten die daaruit naar voren kwamen zijn in een verbeterplan opgenomen. Aanvullend heeft de rekenkamercommissie een viertal testen uitgevoerd, nl. een interne netwerk pentest, een AD audit [7], een phishing mail is uitgezet onder raadsleden en een mystery guest heeft geprobeerd ongeoorloofd op de locatie van de Henry Dunantweg binnen te komen.
Resultaten testen	De scope (bereik) van de testen is altijd beperkt, gezien de kosten. En een serieus kwaadwillende hacker heeft tijd om te proberen ergens binnen te komen. De tests zijn dus altijd momentopnames. Met die beperking is het geconstateerde risico bij de interne netwerk pentest als laag in te schatten. De Active Directory audit (AD) is een check op wachtwoordenbeleid en -gebruik. Met deze test zijn kwetsbaarheden gevonden die aanleiding hebben gegeven tot bijstelling van het wachtwoordenbeleid. De mystery guest test laat zien dat onbevoegden op de Henri Dunantweg ver kunnen doordringen tot in ruimtes die voor hen afgesloten zouden moeten zijn. Tot slot de phishing mail test onder raadsleden. 'Slechts' 18% van de

[5] Logging is een vorm van monitoring waarbij (inlog)gegevens geautomatiseerd worden geregistreerd, bedoeld om bij te houden welke gebeurtenissen/ handelingen binnen een systeem of applicatie hebben plaatsgevonden.

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

[7] AD staat voor Active Directory. De Active Directory staat beheerders toe om het beleid (rechten en instellingen) in het netwerk van een organisatie te beheren. Een AD audit test onder andere het wachtwoordenbeleid en inactieve accounts.

raadsleden, een score onder de benchmark van ca. 35%, heeft op de phishing mail geklikt.

De testen hebben risico's opgeleverd, die niet als heel kritiek zijn bevonden, maar wel aanleiding geven tot verbetermaatregelen op onder andere het wachtwoordenbeleid en de alertheid op onbevoegden op de fysieke locatie.

Onderzoeksvraag 4.	Hoe wordt de gemeenteraad betrokken bij het informatie-beveiligingsbeleid?

Informatie

De raad wordt jaarlijks geïnformeerd over informatiebeveiliging en privacy, zoals de BIO voorschrijft. In de jaarstukken in het kader van de P&C-cyclus komen de onderwerpen aan de orde, met enkele getroffen of te nemen maatregelen ter bestrijding van de risico's. De inhoud is evenwel als summier aan te merken zeker gelet op het toenemende belang van en risico's op informatiebeveiliging en gegevensverwerking voor gemeenten. De raad krijgt in de zijlijn van de rechtmatigheidsrapportages van de accountant, die een beperkte IT-audit uitvoert, een beeld van de stand van zaken op informatiebeveiliging en gegevensverwerking. De accountant wijst op het feit dat IT een steeds belangrijker onderdeel is van bedrijfsvoering. Maar er heeft bijvoorbeeld nog geen inhoudelijke discussie plaats gevonden tussen college en raad naar aanleiding van de aan de raad aangeboden informatie.

Verantwoordelijkheid raad

De raad heeft een kaderstellende en controlerende rol. Ook ten aanzien van informatiebeveiliging, wat doorgaans als onderdeel van bedrijfsvoering wordt gezien wat onder verantwoordelijkheid van het college valt. Er heeft nog geen gesprek plaatsgevonden over de ambities in het kader van informatiebeveiliging en privacy. Gelet op de motie die de raad op 7-11-2022 heeft aangenomen over 'cyberrisico' kan geconstateerd worden dat het onderwerp leeft bij de raad en er behoefte is aan meer informatie.

Conclusies

Hoofdconclusie

Het belang van informatiebeveiliging en gegevensverwerking wordt bestuurlijk onderschreven. Het streven is te voldoen aan de basisset aan maatregelen op deze terreinen. Activiteiten en beheersmaatregelen worden opgepakt door bestuur en functionarissen op informatiebeveiliging en privacy. Door verschillende oorzaken, waaronder bezuinigingen hebben informatiebeveiliging en privacy de afgelopen jaren niet de aandacht gekregen die ze verdienden, gezien de toenemende risico's. De urgentie om hierop te acteren wordt bestuurlijk gevoeld, en er is nog veel te doen om als gemeente Zutphen in control te komen op informatiebeveiliging en privacy.

Deelconclusies

Deze hoofdconclusie leidt tot de onderstaande deelconclusies:

1. Strategisch beleid op informatiebeveiliging en privacy is aanwezig, maar mist op punten aan actualiteit en volledigheid, onder andere in de onderliggende protocollen en richtlijnen. Veel moet nog ontwikkeld worden of worden aangepast aan de actualiteit.
2. De ambitie is te voldoen aan de BIO, wat een basisset aan maatregelen op informatiebeveiliging is. De gemeente weet wat er gedaan moet worden om dat te bereiken, en daarin ligt al een stevige opdracht. Een grotere ambitie dan voldoen aan de basisnormen is voor de korte termijn niet haalbaar en de gemeente loopt hierop risico's. Er ontbreekt ook een ambitieuzer streven voor de (middel)lange termijn.
3. Het risicomanagement, waarop informatiebeveiligingsbeleid en gegevensverwerking gebaseerd moeten zijn, is nog niet volledig uitontwikkeld.
4. De functionarissen op informatiebeveiliging en gegevensverwerking zijn aanwezig, recent in formatie versterkt en op de juiste plek gepositioneerd. Bezien wordt of strategische functies met omringende gemeenten gedeeld kunnen worden.
5. Bewustwording op de risico's en taakvolwassenheid bij medewerkers op informatiebeveiliging en privacy voldoet nog niet om 'in control' te zijn op informatiebeveiliging en privacy. Het urgentiegevoel bij het management om hierop te acteren behoeft versterking. E-learning wordt aangeboden aan medewerkers, maar daar wordt onvoldoende op gestuurd.
6. Geconstateerd is dat veel maatregelen ad hoc worden genomen, deels ook omdat informatiebeveiliging en privacy niet integraal opgenomen zijn in de beschrijving van alle werkprocessen. Systemen ter controle, toetsing op de naleving van de regels en de monitoring van het dataverkeer behoeven nog verbetering. Het managementinformatiesysteem is aanwezig, maar wordt niet goed gevuld. Daardoor functioneert de beleidsleercyclus, PDCA, niet effectief.
7. De in eigen opdracht en in opdracht van de rekenkamercommissie uitgevoerde testen op de systemen laten verbeterpunten zien, waar de gemeentelijke organisatie mee aan de slag is gegaan.
8. De informatie over informatiebeveiliging en privacy aan de raad en het gesprek tussen college en de raad is aan te merken als summier en op hoofdlijnen. Verdieping op de kaderstellende en controlerende rol van de raad wordt gemist.

Aansporingen en aanbevelingen

Aansporingen

Gemeente Zutphen zet de nodige stappen op informatiebeveiliging en privacy, waarbij de rekenkamercommissie het college wil aansporen door te gaan met de volgende punten.

- Blijf als gemeente voldoende aandacht en middelen besteden aan informatiebeveiliging en privacy (de norm die de IBD tegenwoordig hanteert is dat 10% van de middelen die aan ICT worden uitgegeven aan informatiebeveiliging worden besteed);

- Ga verder met en intensiveer waar nodig de activiteiten in het ‘Actieplan Informatiebeveiliging en Privacybescherming’;
- Blijf via periodieke (pen)testen de vinger aan de pols houden, niet alleen op de systemen en netwerken, maar ook op risicobewustzijn van medewerkers en de fysieke beveiliging, werk de verbeterpunten uit de testen voor opvolging uit in een verbeterplan;
- Blijf investeren in risicobewustzijn bij medewerkers en doordring management van urgentie van informatiebeveiliging en gegevens-bescherming;
- Ga verder met de uitvoeren van de voorgenomen dpia’s en het up-to-date houden van het verwerkingsregister.

Aanbevelingen

De hiervoor gepresenteerde conclusies leiden tot de volgende acht aanbevelingen aan het college en de gemeenteraad;

Aan het college

1. Actualiseer het informatiebeveiligings- en privacybeleid op basis van risicomanagement en formuleer ambities hierop in samenspraak met de raad;
2. Breng aantal en actualiteit van de protocollen en richtlijnen zoals voorgeschreven in de BIO up-to-date;
3. Maak effectiever gebruik van de reeds aanwezige middelen voor controle en monitoring op informatiebeveiliging en privacy;
4. Verricht een 0-meting naar de taakvolwassenheid en bewustwording van medewerkers op informatiebeveiliging en formuleer daarop een ambitie en stappenplan om daarop in control te komen;
5. Maak informatiebeveiliging en privacy integraal onderdeel van de werkprocessen;

Aan college en raad

6. Ga samen het gesprek aan om de horizontale verantwoording (tussen raad en college) in te vullen, zodat de raad voor zijn adviserende en controlerende rol zicht krijgt op opzet, bestaan en werking van de maatregelen op informatiebeveiliging en privacy;

Aan de raad

7. Neem als raad een actievere kaderstellende en controlerende rol op de beleidsterreinen informatiebeveiliging en privacy en gebruik hiervoor onder andere de rapportages op privacy- en informatiebeveiligingsaspecten van de FG, ENSIA en accountant.

1 Bestuurlijke reactie

Rekenkamercommisie gemeente Zutphen
T.av. mevrouw K. van den Berg
's Gravenhof 2
7201 DB ZUTPHEN

Inlichtingen bij: Willem Bal | *Telefoon:* 14 0575 | *Bijlage(n)*: -
Team: Control | *Zaaknummer*: 551625 | *Uw bericht van*: 24-04-2023
Onderwerp: Onderzoek Informatiebeveiliging en privacy | *Datum*: 30 mei 2023 | *Uw nummer*: -

Geachte rekenkamercommissie, mevrouw Van den Berg,

Op 24 april 2023 hebben wij uw brief ontvangen waarmee u de bestuurlijke nota, conclusies en aanbevelingen van het onderzoek naar informatiebeveiliging en privacy aanbiedt. U verzoekt ons om een bestuurlijke reactie die integraal wordt opgenomen in de aan de raad aan te bieden eindversie van het rapport. De bestuurlijke reactie hebben wij in deze brief opgenomen.

Dank u voor het nauwkeurige onderzoek. Wij zijn blij met de aansporingen en aanbevelingen die in het rapport 'Informatiebeveiliging en privacy gemeente Zutphen' zijn opgenomen.

Ambities op Informatiebeveiliging en Privacy
Het voldoen aan de regelgeving op het gebied van Informatiebeveiliging en Privacy wordt gezien als randvoorwaarde voor de professionele gemeente. Dit vraagt van ons flinke inzet om te komen tot beleid, het inrichten van veilige processen en het treffen van (technische) maatregelen. Deze zorgen ervoor dat onze inwoners en bedrijven zakendoen met een betrouwbare gemeentelijke overheid die zorgvuldig met haar gegevens omgaat. Het rapport van de rekenkamercommissie helpt ons om de te nemen stappen op het gebied van informatiebeveiliging en privacy extra goed tegen het licht te houden.

Wij beschouwen de onderwerpen informatiebeveiliging en privacy als een zeer belangrijk thema binnen de gemeente. Daarbij voelen we de urgentie om ons te versterken. Dit blijkt onder andere uit het gegeven dat wij in april 2023 het 'Actieplan Informatiebeveiliging en privacy' hebben vastgesteld dat tot doel heeft om in control te komen en de risico's voor de organisatie te verminderen. Om de borging en toename van de volwassenheid op dit thema te kunnen waarmaken loopt er tevens een aanvraag voor extra formatie ter versterking van de organisatie.
In hoofdlijnen richt het actieplan zich op:

- Een beschrijving opstellen van de governance (besturing) met betrekking tot informatiebeveiliging en privacy.
  Hierin worden de rollen, taken en bevoegdheden binnen de organisatie op het gebied van informatiebeveiliging en privacy helder beschreven en duidelijk belegd.
- Het verhogen van het eigenaarschap en informatiebeveiligingsbewustzijn bij medewerkers, leidinggevenden en bestuur.
- Het opstellen van benodigd beleid en inrichten van veilige processen.
- Het (technisch) veilig inrichten van de ICT-omgeving.

Aansporingen en aanbevelingen in het rapport 'Informatiebeveiliging en privacy gemeente Zutphen'
In de voorbereiding op het opstellen van het gemeentelijk 'Actieplan Informatiebeveiliging en privacy' is er in de organisatie een brede inventarisatie gedaan van de te ondernemen stappen op dit thema. Actiepunten zijn benoemd en geïntegreerd in één plan. Het gevolg is dat wij de in uw rapport genoemde aansporingen en aanbevelingen herkennen en erkennen. Alle aansporingen en aanbevelingen nemen wij ter harte en integraal over, behalve aanbeveling 4. Daarop en op een aantal andere in het rapport benoemde onderwerpen geven wij graag een nadere toelichting.

- Het rapport van de rekenkamercommissie beschrijft in aanbeveling 4 (pagina 13) dat er een 0-meting dient te worden verricht naar de taakvolwassenheid en bewustwording van medewerkers op

informatiebeveiliging om zodoende een ambitie en stappenplan te kunnen opstellen. Naar onze mening is dit niet nodig, omdat een dergelijke 0-meting al in 2021 is uitgevoerd. Daarbij kan deze 0-meting worden verrijkt met de informatie die in 2022 is opgehaald door een onderzoek dat binnen de gemeente is uitgevoerd vanuit de provincie (project Troje) en de tests die zijn uitgevoerd in het rekenkameronderzoek. Nu dus geen energie steken in een nieuwe 0-meting, maar juist de informatie die voorhanden is analyseren en de benodigde maatregelen treffen. Dit wordt uitgevoerd binnen het vermelde actieplan.

- Het rapport van de rekenkamercommissie stelt op (pagina 11) dat er nog geen inhoudelijke discussie heeft plaatsgevonden tussen ons en de raad naar aanleiding van de aan de raad aangeboden informatie over de stand van zaken op informatiebeveiliging en gegevensverwerking. Het gaat dan om de informatie verstrekt als onderdeel van de P&C-cyclus en rechtmatigheidsrapportages van de accountant. Dit is echter onjuist en onze vraag is waarop u deze stelling baseert?
- Het rapport van de rekenkamercommissie beschrijft in aanbeveling 1 (pagina 13) dat wij de ambities in het kader van informatiebeveiliging en privacy in samenspraak met de raad moeten opstellen. Het bespreken van de ambities en de op 7 november 2022 aangenomen motie ‘Cyberrisico’ vormen goede aanleidingen voor verder gesprek met de gemeenteraad. Er wordt hierover een open gesprek met de raad gefaciliteerd in een Forumspecial die is gepland voor september 2023.
- Aanbeveling 7 (pagina 13) van de rekenkamercommissie over de behoefte aan een actievere en verdiepende kaderstellende en controlerende rol door de raad is primair aan de raad gericht. Wij vinden dat ook heel belangrijk en constateren hierover dat:
    - Dit gesprek er logischerwijze niet is geweest door bezuinigingen en te weinig personele capaciteit.
    - De voortgang van implementatie van activiteiten op het gebied van informatiebeveiliging en privacy hierdoor ook vertraagd.
    - Activiteiten op het gebied van informatiebeveiliging en privacy werden niet integraal gepland en uitgevoerd, maar voornamelijk op ad hoc basis.

- Ons advies aan de raad is om een commissie informatieveiligheid en privacy in te stellen. Deze kan zich als vooruitgeschoven post verder verdiepen op dit belangrijke en urgente thema dat deels nogal technisch van aard is. Hierdoor kunnen wij in samenspraak werken aan de Digitale Weerbaarheid van de gemeente. En voor onze inwoners en bedrijven een betrouwbare gemeentelijke overheid zijn die zorgvuldig met haar gegevens omgaat.

Financiële gevolgen

Om de activiteiten, zoals die zijn opgenomen in het ‘Actieplan Informatiebeveiliging en privacy’, te kunnen uitvoeren is er geld nodig. Bij de behandeling van de bestemming van het jaarrekeningsaldo 2022 wordt voorgesteld om budget beschikbaar te stellen voor de uitvoering van het actieplan.
Verder houden wij rekening met structurele financiële en personele effecten voor de verdere implementatie van de regelgeving op het gebied van informatiebeveiliging en privacy. Dit is onder andere het gevolg van het actieplan dat moet worden uitgevoerd en de te verwachten intensivering van landelijk toezicht op de naleving van regelgeving. Dit vraagt om meer capaciteit, daarom loopt er een aanvraag voor extra formatie ter versterking van de organisatie.

Vragen

Als u nog vragen heeft over deze brief, neemt u dan contact op met Willem Bal, team Control. Dit kan via telefoonnummer 14 0575 (zonder kengetal) of info@zutphen.nl. Wilt u als u een bericht stuurt het zaaknummer vermelden?

Met vriendelijke groet,

burgemeester en wethouders van Zutphen,

de burgemeester, de secretaris,

2 Reactie rekenkamercommissie

De rekenkamercommissie waardeert het dat het college de belangrijkste aansporingen en aanbevelingen uit het onderzoek onderschrijft.

U heeft toegelicht waarom u aanbeveling 4 niet overneemt.
Wij hebben aanbevolen om een 0–meting uit te voeren naar de taakvolwassenheid en bewustwording van medewerkers. Uit de verstrekte informatie bleek namelijk niet dat deze is uitgevoerd. Dat is ook zo in de nota van bevindingen, die voor ambtelijke hoor en wederhoor (feitencheck) is voorgelegd, opgenomen. Daar is bij de feitencheck is helaas niet op gereageerd. Vandaar onze aanbeveling.
Goed om te constateren dat in 2021 een 0-meting is uitgevoerd en aangevuld met nieuwe informatie leidt tot maatregelen in het actieplan. We raden de raad alert te zijn op de opvolging van de maatregelen uit het actieplan.

U vraagt waarop de rekenkamercommissie zich baseert door te stellen dat er nog geen inhoudelijke discussie heeft plaatsgevonden tussen college en raad ten aanzien van informatiebeveiliging en gegevensverwerking.
De rekenkamercommissie constateert dat de informatie aan de raad summier is. De raad heeft in november 2022 een motie aangenomen om meer informatie te delen, onder andere in de driehoek. Dat is aanleiding geweest om te concluderen dat er geen inhoudelijke discussie over de ambities op informatiebeveiliging en privacy met de raad is gevoerd. Het is dan ook met instemming dat de rekenkamercommissie constateert dat het college in de bestuurlijke reactie de raad adviseert om een commissie informatieveiligheid en privacy in te stellen om een platform voor een dergelijke inhoudelijke discussie te creëren.

Wij zullen de uitwerking van de aanbevelingen nauwgezet volgen en we nemen ons voor in 2024 de doorwerking van de aanbevelingen te onderzoeken.

3 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 en Buren.

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

Dat zijn redenen voor de rekenkamercommissie Zutphen geweest om een onderzoek te doen naar opzet, bestaan en werking van het informatie-beveiliging- en privacybeleid in de gemeente Zutphen.

3.1 Leeswijzer

Samenvatting, conclusies en aanbevelingen zijn in het hieraan voorafgaande hoofdstuk opgenomen. In hoofdstuk 2 behandelen we de doelstelling, onderzoeksvragen en de aanpak van het onderzoek. Hoofdstuk 3 bevat de bevindingen, geordend aan de hand van de onderzoeksvragen. Deze bevindingen zijn getoetst bij de in dit onderzoek betrokken respondenten en in verband met de feitencheck (ambtelijke hoor en wederhoor).

In de bijlage 1 staan allereerst veel gebruikte termen en afkortingen die gebruikt worden bij informatieveiligheid en privacy. Daarna volgt in bijlage 2 de lijst met geraadpleegde stukken en de lijst met functies van de respondenten. Vervolgens komen in bijlage 3 de normen aan bod, gekoppeld aan de onderzoeksvragen. Bijlage 4 bevat een grafisch overzicht van de richtlijnen en procedures op informatiebeveiliging en privacy zoals door de Informatiebeveiligingsdienst (IBD) wordt weergegeven. In §3.2.5 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

[8] 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.

4 Doelstelling, onderzoeksvragen en aanpak

4.1 Doelstelling en onderzoeksvragen

Doelstelling en hoofdvraag

De Rekenkamercommissie Zutphen wil de gemeenteraad inzicht geven in de stand van zaken in de gemeente met betrekking tot beleid en uitvoering van informatiebeveiliging en privacy. Deze doelstelling is vertaald naar de volgende hoofdvraag:

"Heeft de gemeente Zutphen de informatiebeveiliging en gegevens-bescherming op orde?"

Onderzoeksvragen

De doelstelling en hoofdvraag worden uitgewerkt aan de hand van de onderzoeksvragen zoals opgenomen in onderstaande tabel 2.1.

Tabel 2.1. Onderzoeksvragen
1. Beschikt de gemeente Zutphen over een adequaat informatie-beveiligings- en privacybeleid?
2. Hoe wordt het beleid uitgevoerd en hoe wordt de uitvoering gemonitord?
3. In hoeverre zijn gegevens bij de gemeente beschermd tegen de toegang door onbevoegden?
4. Hoe wordt de gemeenteraad betrokken bij het informatie-beveiligings- en privacybeleid?

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

4.2 Korte inleiding op informatiebeveiliging en privacy

Informatiebeveiliging

Informatiebeveiliging gaat over het geheel aan preventieve, detectieve 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).[9] De BIO bevat maatregelen die gemeenten op basis van een risicoanalyse kunnen nemen om aan het basisniveau voor informatiebeveiliging te voldoen.

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

[9] 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.

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 komen met elkaar overeen. Overkoepelend wordt vaak de term informatieveiligheid gebruikt, zie onderstaand afbeelding 2.1.

Afbeelding 2.1. Informatieveiligheid met privacy en informatiebeveiliging.

Bron: Rekenkamer Utrecht, 2021.

In dit onderzoek worden de beide onderwerpen, informatiebeveiliging en privacy, geadresseerd.

4.3 Aanpak

De onderzoeksvragen worden beantwoord door middel van een analyse van documenten in deskresearch, interviewverslagen en pentesten (zie volgende alinea.) De documenten bevatten beleid en rapportages van de gemeente. De documenten die zijn bestudeerd zijn in bijlage 2 opgenomen, evenals de functies van de bestuurders en functionarissen van de gemeente Zutphen die zijn geïnterviewd. De deskresearch vond plaats in de periode oktober-december 2022. De interviews zijn in januari-februari 2023 afgenomen.

Pentesten

In december 2022 zijn in het kader van het rekenkameronderzoek verschillende pentesten uitgevoerd op de systemen, medewerkers en raadsleden van de gemeente Zutphen.[10] Door de gemeente is aangegeven dat deze, in samenwerking met de provincie, ook testen uitvoert op de systemen. Deze pentesten zijn door de onderzoekers gecheckt en als adequaat beoordeeld. De rekenkamercommissie heeft daarop besloten geen externe netwerkpentest uit te laten voeren.

Wel is besloten in het kader van het rekenkameronderzoek aanvullend een interne netwerk test, Active Directory (AD) audit [11], phishing [12] test en een mystery guest [13] uit te voeren. Voor een nadere uitleg van de testen en de resultaten zie §3.3.1.

De nota van bevindingen is in maart 2023 voor de ambtelijke hoor en wederhoor (feitencheck) aangeboden.

[10] 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.

[11] De Active Directory (AD) staat beheerders toe om het beleid (rechten en instellingen) in het netwerk van een organisatie te beheren. De AD bevat een database waarin onder andere accounts en inloggegevens zijn opgenomen. Een AD audit test onder andere het wachtwoordenbeleid en inactieve accounts.

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

[13] Tijdens een mystery guest bezoek probeert een onderzoeker onder valse voorwendselen fysiek binnen te dringen in de gemeentelijke organisatie. Doel is inzicht te krijgen in kwetsbaarheden als ongeautoriseerde toegang mogelijk is tot kantoren en werkruimtes, tot werkstations, informatie of dossiers op bureaus, printers of afvalcontainers.

5 Bevindingen

In dit hoofdstuk worden de bevindingen per onderzoeksvraag weergegeven.

5.1 Informatiebeveiligings- en privacybeleid

In deze paragraaf presenteert de rekenkamercommissie de bevindingen met betrekking tot onderzoeksvraag 1:

Beschikt de gemeente Zutphen over een adequaat informatiebeveiligings- en privacybeleid?

In de sub paragrafen gaan we achtereenvolgens in op het beleid, de protocollen en richtlijnen in het kader van het informatiebeveiligingsbeleid, de positionering van de functionarissen en de diverse overleggen op informatiebeveiliging.

5.1.1 Beleid informatiebeveiliging en privacy

Informatiebeveiligingsbeleid

Het strategisch informatiebeveiligingsbeleid is op 3-11-2020 vastgesteld door het college en in principe geldend van 2020-2024. Door de snelle ontwikkelingen, binnen en buiten de gemeentelijke organisatie, kan het informatiebeveiligingsbeleid volgens respondenten geactualiseerd worden. De Chief Information Security Officer (CISO) en de strategisch adviseur zijn bezig met het updaten van het beleid.

De strategische doelen zoals geformuleerd in het informatiebeveiligings-beleid zijn:

- Het managen van de informatiebeveiliging.
- Adequate bescherming van bedrijfsmiddelen.
- Het minimaliseren van risico's van menselijk gedrag.
- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers.
- 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 waarborgen van de naleving van dit beleid.

Ook de 10 bestuurlijke principes van informatiebeveiliging, behorende bij de BIO zijn in het beleid opgenomen.[14]

[14] De 10 bestuurlijke principes informatiebeveiliging van de VNG luiden: 1. Bestuurders bevorderen een veilige cultuur; 2. Informatiebeveiliging is van iedereen; 3. Informatiebeveiliging is risicomanagement; 4. Risicomanagement is onderdeel van de besluitvorming; 5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking; 6. Informatiebeveiliging

Ambitie

De ambitie van de gemeente is te voldoen aan eisen die de Baseline Informatiebeveiliging Overheid (BIO) stelt. Daarvoor moet een GAP-analyse[15] uitgevoerd worden en op basis daarvan worden, in combinatie met een risicoanalyse, de activiteiten op informatiebeveiliging in een jaarplan informatiebeveiliging opgenomen.

GAP- en risicoanalyse

Uit de interviews blijkt dat de GAP-analyse is uitgevoerd en er is een jaarplan opgesteld. Op moment van interview moest dat nog vastgesteld worden door het MT en daarna doorgestuurd worden naar het college. In het jaarplan zijn activiteiten opgenomen en is een bijbehorende claim op mensen en middelen neergelegd.

Geschetst wordt dat er een grote uitdaging voor de gemeente ligt. Uit de interviews blijkt dat de gemeente van ver komt, daar de afgelopen jaren op bezetting en techniek bezuinigd moest worden. Hetgeen gedaan moet worden om aan de ambitie te voldoen is volgens respondenten in beeld, in die zin wordt 'in control' zijn op informatiebeveiliging gedefinieerd. Maar niet alle activiteiten kunnen meteen opgepakt worden, met name met het oog op de snel ontwikkelende wereld in beveiligingsdreigingen. Vandaar dat prioriteiten gesteld moeten worden en een risicoanalyse gedaan moet worden op te nemen maatregelen. Daarbij wordt gelet op de maatregelen in de BIO en de risico's die de IBD schetst, onder andere op basis van incidenten elders. Risicomanagement in het algemeen en de methodiek om risico's op bedrijfsvoering en dienstverlening van de gemeente zelf te inventariseren en te wegen moet nog ontwikkeld worden.

Verantwoordelijkheden

In het informatiebeveiligingsbeleid zijn de verantwoordelijkheden voor de bestuurders, de functionarissen op informatiebeveiliging, lijnmanagement en medewerkers beschreven. College is eindverantwoordelijk en stelt het strategische beleid vast, de directie stelt het jaarplan vast en is verantwoordelijk voor de tactische uitvoering van de beleidsregels. De CISO is de onafhankelijke ondersteuner en rapporteert rechtstreeks aan de directie. De teamleiders zijn verantwoordelijk voor de uitvoering van beleidsregels op operationeel niveau. Tot slot zijn de medewerkers verantwoordelijk voor het verantwoord omgaan met de informatie waarover de gemeente beschikt en worden zij getraind in de beveiligingsprocedures.

Privacybeleid

In 2018 is een 0-meting uitgevoerd ten aanzien van de eisen van de Algemene Verordening Gegevensbescherming (AVG). Naar aanleiding daarvan is het privacybeleid opgesteld dat in 2018 door het college is vastgesteld. Dat is verouderd ten opzichte van de organisatorische

---

is een proces; 7. Informatiebeveiliging kost geld; 8. Onzekerheid dient te worden ingecalculeerd; 9. Verbetering komt voort uit leren en ervaring; 10. Het bestuur controleert en evalueert. Bron: De 10 bestuurlijke principes voor informatiebeveiliging. Behorende bij de Baseline Informatiebeveiliging Overheid (BIO), VNG, 2019.

15 De GAP-analyse betekent een controle en analyse of en in welke mate de maatregelen uit de BIO geïmplementeerd zijn.

ontwikkelingen en momenteel wordt door de privacy officer en de adviseur privacy gewerkt aan een nieuwe versie. Ook een privacyplan is opgesteld door het externe bureau, waarvan de uitvoering bij de ambtelijke organisatie ligt. Naar aanleiding van de activiteiten wordt jaarlijks een Jaarrapportage gegevensbescherming opgesteld.

Specifiek beleid

Op privacy in het sociaal domein is specifiek een handreiking opgesteld. Deze regelt onder andere hoe medewerkers op een AVG-conforme wijze rapportages waarin persoonsgegevens zijn verwerkt moeten opstellen. Voor andere beleidsterreinen en processen waarin persoonsgegevens worden verwerkt zijn geen specifieke handreikingen opgesteld.

Actieplan Informatie-beveiliging en Privacy-bescherming

Op informatiebeveiliging en privacy is begin 2022 het 'Actieplan Informatie-beveiliging en Privacybescherming' opgesteld. De achterliggende wens van van de gemeente was om het niveau van informatiebeveiliging en privacy-bescherming te verhogen, omdat een achterstand in voorgenomen activiteiten uit het privacyplan werd geconstateerd. Het actieplan is opgesteld naar aanleiding van een extern rapport. In juli en september 2022 is het geüpdatet met bevindingen van de interim CISO op informatiebeveiliging.
Getracht wordt met een projectmatige aanpak een aantal activiteiten uit te voeren, benodigd om te voldoen aan de BIO en AVG. Binnen een viertal prioriteiten zijn activiteiten opgenomen die met name met de organisatie- en menskant van het informatiebeveiliging- en privacybeleid te maken hebben. Daartoe behoren het opstellen van protocollen en implementeren van managementsystemen, zoals het Information Security Management System (ISMS). Er is, zo is ook geconstateerd uit de interviews, structuur aangebracht in de budgetten van het team I&A, waardoor mede op informatieveiligheid beter gestuurd kan worden. En tot de geprioriteerde activiteiten uit het actieplan behoort het vergroten van bewustzijn en kennis via trainingen van medewerkers.

Draagvlak en ambitie

Uit de interviews blijkt dat het bestuurlijk draagvlak groeiende is. Voorheen werd het gezien als een noodzakelijk kwaad, dat veel geld kost. Gezien de financiële uitdaging van de gemeente was dat een extra last. Geconstateerd kan worden dat in het coalitieakkoord de term informatiebeveiliging niet voorkomt en de term privacy een keer in het kader van cameratoezicht (zie hierna bij datagedreven werken.) Maar ook wordt in interviews gemeld dat onder andere door incidenten elders, zoals Hof van Twente, Buren en Lochem, de bestuurlijke aandacht is aangewakkerd. Momenteel zijn er twee portefeuillehouders, een op informatiebeveiliging en privacy en een op bedrijfsvoering en ICT. In interviews wordt gemeld dat bij beide voldoende aandacht op de onderwerpen aanwezig is.

Een beeld voor draagvlak voor informatiebeveiligings- en privacybeleid is in hoeverre in onder andere stukken voor de planning en control cyclus informatiebeveiliging en privacy ter sprake komt. In het coalitieakkoord

2022-2026 van het college dat na de gemeenteraadsverkiezingen in 2022 aantrad wordt nauwelijks melding gemaakt van informatiebeveiliging of privacy. Slechts een opmerking wordt gemaakt over cameratoezicht, zie hieronder bij 'datagedreven werken'. In de meerjarenbegroting jaarschijf 2023 worden wel opmerkingen gemaakt, zoals doorontwikkeling van het beleid op technisch en organisatorisch vlak. Plus het investeren in de verbetering van het Identity and Access Management (IAM), zie daarvoor ook §3.1.2 en 3.2.2). Ook wordt de continue aandacht gevraagd voor bewustwording rondom informatieveiligheid.

Datagedreven werken

Een apart hoofdstuk vormt datagedreven werken, het bij beslissings- en uitvoeringsprocessen gebruik maken van en koppelen van (big) data. Uit de interviews blijkt dat de wens er is om meer datagedreven te werken, maar er is nog geen beleid geformuleerd. Aan datagedreven werken kleven risico's en ethische vragen, zoals onder andere blijkt uit de toeslagenaffaire. In het coalitieakkoord 2022-2026 wordt opgemerkt dat cameratoezicht in veel gevallen het gevoel van veiligheid kan vergroten en helpen met het oplossen van overlast en criminaliteit. Er worden ook bezwaren op het gebied van privacy en de uitvoerbaarheid aangegeven. Gemeld wordt dat in deze raadsperiode een afwegingskader cameratoezicht zal worden opgesteld met kaders waarbinnen mogelijk cameratoezicht toegepast kan worden. Een discussie over informatiebeveiliging en privacy met betrekking tot bodycams van BOA's loopt. Er zijn ethische afwegingen te maken, zoals bijvoorbeeld bij armoedebeleid: welke data vraag je uit, met wie deel je de data en hoe voorkom je discriminatie?

Datagedreven werken is ook in de begroting 2023 opgenomen. Een van de projecten die regionaal wordt uitgevoerd is Datalab GO, waar de gemeente Bronckhorst de penvoerder van is. Algoritmes en dashboards met samengestelde managementinformatie worden ontwikkeld. Het heeft de aandacht van de gemeente, maar het staat nog in de kinderschoenen. Uit de interviews blijkt dat de gemeente hierop nog aan het leren en ontwikkelen is.

5.1.2 Protocollen en richtlijnen

Protocollen/richtlijnen

In het informatiebeveiligings- en privacybeleid schrijft de BIO een aantal protocollen en richtlijnen voor om op informatiebeveiliging en privacy in control te komen, zie bijlage 4. Bij het opvragen van de documenten en in de interviews is een deel aangereikt, zoals de procedures 'Back-up en restore' [16], 'Hardening' van de systemen, apparatuur en voorzieningen, 'Incidentmanagement', Wachtwoordbeleid' [17] en 'Toegangspassen'. Ook is

[16] Uit de ambtelijke reactie blijkt dat in maart 2023 de back-up en restore voorziening in 2022/2023 opnieuw is ingericht. Een actuele beschrijving van de inrichting en beleid moet echter nog worden opgesteld.

[17] Uit de ambtelijke reactie blijkt dat het wachtwoordbeleid is aangepast, mede naar aanleiding van de pentesten in opdracht van de rekenkamercommissie, zie §3.3.1.

aangegeven dat er het nodige aan vereiste documenten mist of deels aanwezig is, of geüpdatet of herijkt zou moeten worden. De interim CISO heeft in kaart gebracht wat er aanwezig is. Daaruit blijkt dat er nog grote stappen gemaakt moeten worden en er voorheen wel de plannen waren die niet volledig zijn uitgevoerd. Aangegeven is dat er te weinig mensen waren, en ook te weinig aandacht, om die plannen goed op te pakken.

Actieplan privacybescherming en infoveiligheid

In het Actieplan is binnen de vier prioriteiten opgenomen dat deze documenten aangevuld en geüpdatet zullen gaan worden. In een van de prioriteiten is het ontwikkelen van een integraal continuïteitsplan opgenomen. Dat was er ten tijde van de interviews nog niet volledig, aangegeven werd dat het er deels op verschillende deelterreinen is en deels in de hoofden van de betrokken medewerkers zit. Ook een autorisatiebeleid (Identity and Access Management), dat de wijze regelt waarop medewerkers toegang krijgen tot gegevens staat op de planning. Op basis daarvan kan dan het wachtwoordenbeleid op een juiste manier aangevuld worden. Een ruwe schatting uit de interviews is dat circa een kwart tot een derde van de benodigde documenten op informatiebeveiliging en privacy actueel en aanwezig is.

Een enkele respondent wijt dat aan de ad hoc manier van werken bij de gemeente. Uit een van de interviews blijkt dat bij vragen van medewerkers over informatiebeveiliging en privacy het antwoord soms is dat er met betrekking tot dat vraagstuk nog geen werkwijze over is afgesproken.

AVG

Op gebied van privacy zijn de meeste in de AVG vereiste protocollen bij de gemeente aanwezig. Er is een privacystatement dat gepubliceerd is waarop inwoners kunnen zien welke gegevens in het algemeen door of namens de gemeente worden verwerkt en hoe zij hun recht op inzage kunnen krijgen. Ook is er een verwerkingsregister, waarin opgenomen is welke persoonsgegevens de gemeente verwerkt en met wie de gemeenten deze deelt of welke partij namens de gemeente deze gegevens verwerkt. Daarnaast werkt de gemeente met verwerkingsovereenkomsten waarvoor het model van de VNG wordt gebruikt. Er is een procedure voor het melden van datalekken en een procedure voor het uitvoeren van een data protection impact assessment (dpia). Een toestemmingsprocedure om persoonsgegevens in het kader van P&O te mogen delen wordt gemist.

Werkprocessen

Een van de respondenten geeft aan dat er geen privacychecks aanwezig zijn in de besluitvormingsprocessen of werkprocessen waarin persoonsgegevens worden verwerkt. Dat wil zeggen dat gegevensbescherming vaak niet op voorhand bij besluitvorming of inrichting van werkprocessen wordt betrokken. Dat geeft een risico op inefficiëntie daar het in dat geval lastiger is het aspect privacy tijdig mee te nemen en te voldoen aan de AVG.

5.1.3 Omvang aanstelling en positionering functionarissen op informatiebeveiliging

Rollen op informatie-beveiliging en privacy

Op intranet staan de verschillende rollen van de functionarissen op 'privacy en AVG' gepubliceerd. Daarin is beschreven dat de teamleiders als proceseigenaar eindverantwoordelijk zijn en verantwoordelijk zijn voor de borging van de informatiebeveiliging en privacy in de werkprocessen in de teams. De medewerkers zijn verantwoordelijk voor het op peil houden van de eigen kennis op informatiebeveiliging en privacy. In het document 'Diverse rollen op gebied van privacy en AVG' wordt ook de CISO meegenomen, die met name op informatiebeveiliging werkzaam is. Hieronder gaan we op de verschillende specifieke functies op informatiebeveiliging en privacy in.

Informatiebeveiliging

Hiervoor is aangegeven dat er bezuinigd is op techniek en mensen en er zijn veel wisselingen in personeel op informatiebeveiliging te constateren. Zo zijn recent de adjunct directeur bedrijfsvoering (CIO), teamleider I&A en een strategisch adviseur gestart.

CISO

Er is voorzien in een CISO-functie, die momenteel interim door een externe kracht wordt ingevuld. De CISO coördineert het beleid op het vlak van informatiebeveiliging en zorgt voor een samenhangend pakket van technische en organisatorische maatregelen ter waarborging van de beschikbaarheid, integriteit en vertrouwelijkheid (biv) van de informatie binnen de gemeente. De CISO is de coördinator van de ENSIA-verplichtingen [18] en houdt zich ook bezig met risicoanalyses en interne audits en het afhandelen van beveiligingsincidenten. Hij geeft advies en rapporteert direct aan het management over informatiebeveiliging.

De CISO is strategisch en onafhankelijk van de lijn gepositioneerd. De vorige CISO was ook op tactisch en operationeel vlak actief. Een informatie-(beveiligings)adviseur op tactisch niveau die de liaison met het operationele niveau kan onderhouden is niet aanwezig. Dat betekent dat de strategische functie van de CISO nog veel tactische en operationele taken uitvoert. Of informatiebeveiliging op operationeel goed in de werkprocessen wordt geïmplementeerd is afhankelijk van de kennis en taakvolwassenheid op informatiebeveiliging bij de teammanagers. Zie daarvoor §3.2 beleidsuitvoering.

Functionaris Gegevensbescherming

Er is vanaf 2018 een voltijds Functionaris Gegevensbescherming (FG) aanwezig in de gemeente Zutphen, die vanaf 1 januari 2023 voor 0,8 fte werkzaam is. Die capaciteit is hierop binnen de organisatie vrijgemaakt omdat er geen extra middelen beschikbaar waren. Zijn taken zijn onder

[18] ENSIA staat voor de Eenduidige Normatiek Single Information Audit. Op basis van de resultaten van externe en interne audits worden de verticale toezichthouders (landelijke toezichthouders als Logius) en de horizontale toezichthouder (de gemeenteraad) geïnformeerd over de stand van zaken met betrekking tot informatiebeveiliging en privacy.

andere de organisatie informeren en adviseren over de AVG-verplichtingen, adviseren bij een dpia, als contactpersoon fungeren naar de Autoriteit Persoonsgegevens (AP) toe en aanspreekpunt voor inwoners met vragen over de AVG en privacy. De FG controleert als interne toezichthouder de naleving van de AVG en het privacybeleid. En rapporteert over zijn bevindingen aan de gemeentesecretaris en de portefeuillehouder. Deze functie is bedoeld om op strategisch niveau te functioneren.

Privacy officer en adviseur privacy

Naast de strategische functie van de FG zijn er nog twee functionarissen op tactisch niveau werkzaam. In 2022 is een privacy officer voor 18 uur aangesteld, dat was tot voor kort 16 uur. Deze functionaris is verantwoordelijk voor het daadwerkelijk vormgeven van het privacybeleid. Ook is voor 21 uur een adviseur privacy voor gegevensbescherming aan het werk gegaan. De privacy officer werkt organisatiebreed en is het aanspreekpunt voor de directie. De adviseur privacy is in eerste instantie meer gericht op het sociaal domein, waarin uiteraard veel (persoons)gegevens worden verwerkt. De privacy officer en adviseur privacy vallen onder bestuursondersteuning en vormen sinds kort het Privacyteam. Zij pakken de meeste vraagstukken en zaken op gegevensbescherming gezamenlijk op. Zoals adviseren en ondersteunen de teamleiders, die de 'proceseigenaren' zijn en verantwoordelijk zijn voor de werkprocessen binnen de teams. En zij beantwoorden de vragen van medewerkers uit de vakteams.

Actieplan

Tot de activiteiten van de functionarissen op informatiebeveiliging en privacy behoren onder andere de punten uit het Actieplan privacybescherming en informatieveiligheid (zie § 3.1.1).

Formatie

Zoals eerder geconstateerd zijn er veel wisselingen geweest en is de formatie en het op peil houden van kennis, kunde en capaciteit een aandachtspunt en forse uitdaging voor de gemeente. Te meer daar er krapte op de arbeidsmarkt heerst, met name bij de technisch geschoolde functies. Die krapte wordt ook gevoeld bij de afdeling Informatiering en Automatisering (I&A) van de gemeente. Daar is externe ondersteuning voor de vaste staf aanwezig. Voor een middelgrote gemeente als Zutphen is salariëring van functionarissen met een specifieke, in dit geval technische, expertise een knelpunt.

De CISO is voor 0,6 fte in dienst, en dat wordt uitgebreid naar 0,7. Uit de gesprekken blijkt dat de druk hoog is bij de functionarissen op informatiebeveiliging en privacy. Gegevensbescherming vergt continu aandacht en er moeten in de beschikbare uren keuzen gemaakt worden op basis van een inschatting van het risico.

1-pits functies

Gemeenten hebben moeite om vacatures voor gespecialiseerde 1-pits functies, zoals de FG en CISO, te vullen. In een aantal gemeenten worden deze functies gezamenlijk met buurgemeenten ingevuld. In de interviews wordt melding gemaakt van overleg tussen de gemeenten Voorst,

Brummen en Zutphen om dit soort functies dichter bij elkaar te organiseren en van elkaar te leren en elkaar te ondersteunen. Er zijn nog geen afspraken gemaakt om de functies gezamenlijk in te vullen.

Ambassadeurs

Uit de interviews blijkt dat wordt nagedacht over privacy ambassadeurs in de teams.[19] Dat zijn medewerkers uit de teams zelf, die een speciale opleiding gegevensbescherming en uren voor deze taak krijgen. Op het terrein van informatiebeveiliging zijn er geen plannen voor dergelijke medewerkers.

5.1.4 Overleggen op informatiebeveiliging en privacy

Er zijn verschillende interne overleggen waar aangelegenheden op informatiebeveiliging en gegevensbescherming worden besproken.

Team Privacy

De privacy officer en adviseur privacy vormen samen het team Privacy. Zij adviseren onder andere de teams en teamleiders, beantwoorden de vragen van medewerkers, handelen meldingen van datalekken af, beoordelen verwerkersovereenkomsten (zie §3.2.4) en zorgen voor bewustzijn op risico's bij de medewerkers.

Functionarissenoverleg

Vanaf februari 2023 is er een driewekelijks overleg tussen de functionarissen op informatiebeveiliging en privacy waarin de lopende zaken worden besproken. Daar maken de CISO, privacy officer en adviseur privacy deel van uit. Indien nodig sluit de adjunct-directeur bedrijfsvoering aan. Een van de respondenten meldt dat dit overleg vanwege andere prioriteiten vaak wordt afgezegd.

CIO-overleg

Er is in 2021 een projectgroep 'Versterken privacybescherming en informatieveiligheid' gevormd naar aanleiding van de geconstateerde achterstand in activiteiten op informatiebeveiliging en privacy. Daaruit vloeide het 'Actieplan privacybescherming en infoveiligheid' voort (zie hiervoor §3.1.1). De projectgroep is op 'stand by' gezet en in plaats daarvan vindt tweewekelijks een overleg plaats tussen de adjunct-directeur bedrijfsvoering (Chief Information Officer [CIO]), de CISO, de teamleider I&A en de strategisch adviseur I&A. Daar wordt informatiebeveiliging besproken en thema's als digitale dienstverlening en datagedreven werken.

Een enkele respondent geeft aan dat het goed zou zijn informatie-beveiliging en het jaarplan in een brede projectgroep op te pakken, en in de staande lijnorganisatie te beleggen. Dat betekent ook een grotere claim op mensen en middelen waar een college- en raadsbesluit over genomen zouden moeten worden.

---

[19] Uit de interviews blijkt er tot voor kort in de gemeenschappelijke regeling 'Het Plein' zogenoemde aandachtsfunctionarissen voor privacybescherming aangewezen waren. Zij kregen geen speciale training en moesten deze taak naast hun reguliere werk uitvoeren. Als het reguliere werk een hogere belasting met zich meebracht, vlakte de aandacht voor gegevensbescherming af.

Portefeuillehouderoverleg

Voorts is er een maandelijks overleg tussen de CISO, teammanager I&A en de portefeuillehouder. De portefeuillehouder heeft geen structureel overleg met de FG. De CISO en FG hebben in zeer urgente gevallen wel een directe lijn naar de portefeuillehouder, vanwege hun strategische en onafhankelijke positionering. De portefeuillehouder heeft daarnaast regelmatig overleg met de adjunct directeur bedrijfsvoering, waarin informatiebeveiliging en gegevensbescherming hoog op de agenda staan.

Crisisteam

Als er zich een crisis voordoet wordt een crisisteam gevormd. Zoals met de Log4J-kwetsbaarheid [20] die medio december 2021 wereldwijd werd geconstateerd. Op dat moment is een crisisteam gevormd van de directeur bedrijfsvoering, teammanager I&A en systeembeheerders dat tweemaal daags contact had om de crisis het hoofd te bieden.

Juridisch AVG-overleg

Specifiek voor de juridische aspecten op privacy en de AVG is er een wekelijks juristenoverleg. Hier zijn geen functionarissen op informatiebeveiliging en gegevensbescherming bij betrokken.

Rapportages

De FG stelt jaarlijks een gestructureerd verslag op van de geplande en gerealiseerde activiteiten op gegevensbescherming en privacy. Dat is ook wettelijk verplicht. Dit verslag wordt gedeeld met de gemeentesecretaris en het college. Merkwaardig is te constateren dat het verslag niet door de FG wordt gedeeld met de privacy officer en adviseur privacy. De FG neemt de opdracht letterlijk dat de rapportage strikt genomen bedoeld is voor de gemeentesecretaris. Daarnaast rapporteert hij indien nodig kort over lopende zaken.

De CISO rapporteert zelf niet apart over informatiebeveiliging, maar is wel ENSIA-coördinator. In ENSIA (zie ook §3.2.5) wordt op basis van externe en interne audits voor de verticale verantwoording aan landelijke toezichthouders en de horizontale verantwoording aan de gemeenteraad over informatiebeveiliging en privacy gerapporteerd.

5.2 Beleidsuitvoering en monitoring

Onderzoeksvraag 2

In deze paragraaf beantwoorden we de tweede onderzoeksvraag: “Hoe wordt het beleid uitgevoerd en hoe wordt de uitvoering gemonitord?” Hieronder gaan we in op draagvlak en bewustwording op informatiebeveiliging en privacy bij de gemeente, het autorisatieproces, afspraken op gegevensverwerking door derden, de data protection impact assessments (dpia’s) en monitoring van onder andere de beleidsuitvoering.

[20] Log4J-kwetsbaarheid betrof een ernstige kwetsbaarheid in de door veel websites gebruikte module Apache Log4J. Kwaadwillenden konden dit lek in de software misbruiken om een server op afstand over te nemen en willekeurige codes zoals ransomware te installeren. Daardoor zouden datalekken kunnen ontstaan. De kwetsbaarheid is door het Nationaal Cyber Security Center als kritiek bestempeld.

5.2.1 Draagvlak en bewustwording

Gevraagd naar wat er goed gaat met betrekking tot de uitvoering van het informatiebeveiligings- en privacybeleid antwoorden respondenten over het algemeen dat de bewustwording en draagvlak in de organisatie groeiende is. Medewerkers komen zelf vaker met vragen over informatie-beveiliging en privacy bij de functionarissen en melden eerder dan voorheen incidenten en datalekken. Er wordt meteen bij gemeld dat er nog een hele weg te gaan is en dat het onderwerp continu aandacht vergt.

Draagvlak

Een van de bestuurlijke principes in het strategisch informatiebeveiligings-beleid is dat het gemeentebestuur het belang van informatiebeveiliging uitdraagt. Over het algemeen wordt in de interviews aangegeven dat de 'tone at the top' zodanig is dat het belang van informatiebeveiliging en privacy wordt ingezien en het beleid goed wordt uitgedragen. In de directie is een nieuwe adjunct-directeur bedrijfsvoering die gevoel heeft bij de onderwerpen en in het college is een portefeuillehouder die daarop een pleitbezorger is. Zij willen zich als ambassadeur op de thema's informatiebeveiliging en privacy positioneren.

Bewustwording

In de teams in de staande organisatie moeten de medewerkers zich bewust zijn van de risico's op informatiebeveiliging en privacy en in de werk-processen het beleid borgen. Zoals een van de geïnterviewden aangeeft: "Het onderwerp moet van de medewerkers zelf gemaakt worden: als jij niet wil dat iets naars met jouw informatie gebeurt, zorg dat dat niet gebeurt met de informatie die je verwerkt." Kortom, informatieveiligheid is van iedereen in de organisatie.

De teamleiders zijn als proceseigenaar daarvoor verantwoordelijk. In de interviews wordt aangegeven dat het vaak nog schort aan voldoende besef bij teamleiders van hun specifieke rol (die van 'proceseigenaar') bij informatiebeveiliging en privacy. Respondenten geven aan dat door de vele wisselingen bij de teamleiders, tijdgebrek en andere prioriteitstelling het lastig is om beleid en bewustwording te borgen. De teams die al langer persoonsgegevens en gevoelige informatie verwerken zijn over het algemeen wel bewuster van de risico's en volgen de noodzakelijke procedures. De thema's informatiebeveiliging en privacy zijn nog niet in alle teams een -vast item bij de werkoverleggen. En vaak wordt aandacht voor deze thema's als een extra taak erbij ervaren, die afleidt van het 'echte' werk.

Aangegeven wordt dat in veel afdelingen informatiebeveiliging en privacy niet als onderdeel van werkprocessen zijn meegenomen. De beginselen van het beleid zijn neergezet, maar als daar geen werkproces aan ten grondslag ligt verdwijnt de aandacht naar de achtergrond. Er zijn geen medewerkers die de collega's aanspreken op gedrag, bijvoorbeeld met betrekking tot het 'clean desk'-beleid.

Bezoeken overleg

Corona gooide volgens geïnterviewden roet in het eten. Functionarissen op informatiebeveiliging en privacy kwamen wel eens langs bij teamoverleggen om kennis te maken, de praktijk te leren kennen en uitleg te geven. Door corona is dat niet meer gebeurd. Maar de functionarissen geven aan dat wel weer op te gaan pakken.

Case sociaal domein

Voor de uitvoering van het informatiebeveiligings- en privacybeleid geven we een korte schets hoe dat gebeurt in een domein waarin veel persoonsgegevens worden verwerkt. De beschrijving is in onderstaand kader opgenomen.

Case - Sociaal domein

In het team sociaal domein is men al langer gewend (bijzondere) persoonsgegevens te verwerken. In de teamoverleggen komen de onderwerpen informatiebeveiliging en gegevensbescherming vaak terug. Men was al gewend aan de Wet Bescherming Persoonsgegevens en de AVG heeft ook weer niet zo heel veel veranderd in de werkwijzen. Functionarissen op informatiebeveiliging en privacy merken wel dat sinds de AVG van kracht werd, medewerkers meer met vragen komen of gegevens gedeeld mogen worden. Medewerkers werkzaam in het sociaal domein geven aan dat bij elke processtap met persoonsgegevens men er bewust van is met wie men toegang heeft tot de informatie, met wie die gedeeld wordt en dat het delen van persoonsgegevens gebeurt in lijn met de AVG. Voordeel is dat voor 28 uur een kwaliteitsmedewerker is aangesteld die hierop ondersteunt.

Zoveel als mogelijk transparant werken en informatie opvragen en delen, bijvoorbeeld in het kader van de jeugdwet. Gespreksverslagen en rapporten worden in samenspraak met de betrokkenen opgesteld en ter inzage toegezonden. De verwerking en het delen van (bijzondere) persoonsgegevens geschiedt dan op basis van toestemming. In overleggen met externen, zoals de Veiligheidskamer of Vangnet, wordt casuïstiek besproken. Daarin komen persoonsgegevens aan de orde. Hoe met deze informatie wordt omgegaan wordt geregeld in convenanten of er wordt vaak anoniem op de inhoud ingegaan.

Met partijen die diensten verlenen aan de gemeente, zoals onafhankelijke keuringen in het kader van de Wmo, worden contracten met verwerkersovereenkomsten gesloten (zie ook §3.2.3). In het kader van preventie zijn landelijk overeenkomsten gesloten met partijen, zoals energiebedrijven, om vroegtijdig gegevens door te geven van inwoners met betalingsachterstanden en schulden. Met lokale partners, zoals de plaatselijke woningcorporatie kan dat ook lokaal geregeld worden.

Persoonsgegevens worden beveiligd via de mail verstuurd, met behulp van een button 'Beveiligde mail' in het mailprogramma. De externe die de mail ontvangt kan deze alleen openen met een code die via een ander kanaal wordt verzonden, bijv. een sms via een 06-nummer (2-factor authenticatie [2FA]). Sommige ontvangers geven aan dat te ingewikkeld te vinden en eigenlijk liever de mail met persoonsgegevens onbeveiligd te willen ontvangen. Dat gebeurt evenwel niet. Soms wordt de vergeten de mail beveiligd te versturen of naar een verkeerd adres gestuurd (een van de meest voorkomende gevallen van datalekken).

De locatie HDW, waar medewerkers sociaal domein werkzaam zijn en klantgesprekken met de inwoners plaats vinden, is kwetsbaar wat betreft veiligheid (zie §3.1.1 Pentesten) en gevoelig met betrekking tot privacy. Uit de interviews blijkt dat klantgesprekken, waarin bijzondere persoonsgegevens over tafel kunnen gaan, in de openheid plaatsvinden en afluisterbaar zijn. Aangegeven wordt dat de andere kant van openheid is dat de veiligheid van de medewerkers makkelijker geborgd kan worden.

E-learning en phishingmails

Medewerkers worden geacht de eigen kennis op informatiebeveiliging en privacy op peil te houden. Informatie kunnen medewerkers vinden op intranet, Sjaak bij Wegwijzer onder de kop Informatiebeveiliging en privacy. En er worden cursussen aangeboden. Het aanbieden van e-learning aan medewerkers is een middel om de verantwoordelijkheid in de lijn-organisatie te vergroten. Modules worden sinds 2022 aangeboden en zijn in principe verplicht. De medewerkers moesten meteen 2 of 3 certificaten behalen. In de interviews is aangegeven dat de check op het daadwerkelijk volgen van de e-learning modules beter kan.

Een wedstrijdelement tussen de teams is een ludieke manier om extra aandacht te vragen. De vraag die respondenten graag willen beantwoorden is hoe de intrinsieke motivatie van medewerkers te stimuleren. Aangegeven wordt dat medewerkers functiegericht zijn en behoefte hebben aan informatie die ze nodig hebben voor hun werkzaamheden. Met de vele functies in een gemeente is het lastig cursussen op maat aan te bieden.

Het bewustzijn wordt ook getest met test phishing mails, onder andere in het project Troje in samenwerking met de provincie.

Nieuwe medewerkers

Voor nieuwe medewerkers is een informatieboekje aanwezig. Daarin is informatie opgenomen over hoe als ambtenaar van de gemeente Zutphen om te gaan met informatie en beveiligingsmaatregelen. De e-learning maakt nog geen structureel onderdeel uit van het inwerkprogramma.

5.2.2 Autorisaties

Autorisaties

Het autorisatieproces (ook wel Identity and Access Management, IAM genoemd) betreft het verlenen van toegang (autorisatie) van medewerkers tot gebouwen, systemen en gegevens. Er is een procedure hoe autorisaties bij in-, door- en uitstroom (IDU) van medewerkers worden toegekend en

geblokkeerd. Dat proces verloopt via de teamleider, HRM en de beheerders. Als medewerkers instromen, dan moeten ze aan de slag kunnen en toegang krijgen tot applicaties en gegevens. Over het algemeen gaat dat goed daar waar de medewerker aan de slag moet.

Het autorisatieproces verloopt vaak niet correct bij functiewisseling of uitstroom van de medewerker. De teamleider moet de medewerker afmelden voor de functie die deze vervult. Als dat niet correct gebeurt kan het voorkomen dat rechten van medewerkers te lang blijven doorlopen. Dat kan mogelijk een datalek tot gevolg hebben, vanwege de ongeoorloofde toegang tot informatie. Uit de interviews blijkt dat dat vooral kan voorkomen omdat rechten worden toegekend aan medewerkers in plaats van aan functies of rollen van medewerkers.

Uit audits en accountantscontroles kwam herhaaldelijk naar voren dat er verbeterpunten zijn op het autorisatieproces. De accountantscontrole over 2020 gaf een aantal bevindingen op drie belangrijke applicaties (financiële, uitkerings- en salarisadministratie). De controle over 2021 wees uit dat een aantal punten is opgepakt, maar dat de controle op de autorisaties nog aangescherpt moest worden. Ook uit de interviews blijkt dat er te weinig controle op wordt uitgevoerd. In de interviews is aangegeven dat het autorisatieproces op basis van rollen of functies in 2023 op de rol staat geïmplementeerd te worden vastgelegd.[21]

5.2.3 Gegevensverwerking door derden

Gegevens en derden

De gemeente verwerkt gegevens, maar ook namens de gemeente worden door derden gegevens verwerkt waar de gemeente (verwerkings)verantwoordelijk voor is. Dat zijn bijvoorbeeld gegevens van inwoners in het sociaal domein, maar ook onder andere persoonsgegevens. Een aantal van de applicaties die gegevens verwerken draait zelfstandig bij de gemeente, een aantal draait in de ‘cloud’. Sinds de AVG moet de gemeente bijhouden door welke externe parttijen de gegevens worden verwerkt (in een verwerkingsregister). Onder de contracten met deze partijen moeten dan verwerkersovereenkomsten liggen waarin is opgenomen welke gegevens worden verwerkt, hoe deze beveiligd worden en hoe de gemeente daarop toeziet.

Verwerkersovereenkomsten

De procedure is dat verwerkersovereenkomsten onder de contracten met derden door de privacy officer worden gecontroleerd. Uit de interviews blijkt dat medewerkers daarop de privacy officer meer en meer weten te vinden. Met name als de aanbesteding boven de vastgestelde aanbestedingsgrenzen liggen. Uit de interviews blijkt dat niet gegarandeerd kan

[21] In de interviews wordt gesproken over ‘Role based access control’ (Rbac), wat betekent dat 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.

worden dat deze procedure wordt gevolgd als de aanbesteding onder de aanbestedingsgrens ligt.

De bijlage van de verwerkersovereenkomst die over de eisen met betrekking tot informatiebeveiliging gaat moet door de CISO gecontroleerd worden. Dat proces is nog niet goed ingericht, met als gevolg dat die bijlage van veel verwerkersovereenkomsten niet gecontroleerd worden.

Verwerkingsregister

De gemeente heeft via het verwerkingsregister zicht op alle processen waarin persoonsgegevens worden verwerkt en wordt aangegeven hoe informatiebeveiliging en privacy geregeld is in die processen. Ook de verwerkingsprocessen die door externe partijen voor of namens de gemeente worden uitgevoerd. Nieuwe contracten met onderliggende verwerkersovereenkomsten, die langs de privacy officer gaan, worden in het register opgenomen. Grote en langdurende contracten, zoals veel op het terrein van ICT, worden niet opengebroken om onderliggende verwerkersovereenkomst te sluiten. Alleen als de termijn afloopt en het contract vernieuwd wordt, wordt de verwerkersovereenkomst meegenomen en in het register opgenomen. Het verwerkingsregister loopt dus achter op de feitelijke situatie. Het register wordt bijgehouden met de applicatie I-Navigator en sinds eind 2022 is een beheerder aan de slag om het register up-to-date te brengen.

Convenanten

In het sociaal domein worden uiteraard veel persoonsgegevens verwerkt, ook door externe partijen. Voor meervoudige problematieken is het nodig gegevens met meerdere partijen te kunnen delen of te kunnen ontvangen. Er is een handreiking opgesteld voor privacy in het sociaal domein, zoals hoe een rapportage met persoonsgegevens conform de regels opgesteld moet worden. Uit de interviews blijkt dat de naleving van de handreiking niet periodiek wordt gecheckt.

Om gegevens te kunnen delen met of ontvangen van derden worden apart convenanten afgesloten over de voorwaarden waaronder de gegevens gedeeld kunnen worden. Dat gebeurt onder andere met de Veiligheidskamer, waarbij geregeld is dat bij ernstige zorgen informatie wel gedeeld kan worden.[22]

5.2.4 Dpia's

Data protection impact assessment (dpia)

Data impact protection assessments (dpia's) moeten volgens de AVG gehouden worden op werkprocessen waarbij persoonsgegevens worden verwerkt en een grote kans bestaat op een hoog privacy-risico. Onder andere de risico's moeten ingeschat worden en beheersmaatregelen moeten worden getroffen. Een dpia is een intensief assessment. Gelukkig hoeven niet alle werkprocessen aan zo'n assessment onderworpen te

[22] Met het Wetsvoorstel Aanpak meervoudige problematiek sociaal domein ('Wams'), dat in 2023 in de Tweede kamer op de rol staat, zou dat nog eenvoudiger moeten worden.

worden. Om te bepalen welke een hoog privacy-risico hebben kunnen pre-dpia's worden afgenomen. Daarbij kan op een relatief eenvoudige wijze geconstateerd kan worden of een dpia nodig is.

Teamleiders

Afgelopen jaren was het streven dpia's voortvarend op te pakken. De functionarissen op informatiebeveiliging en privacy kunnen daarbij van advies voorzien. Uit de interviews blijkt dat teamleiders het vullen van een dpia te technisch en lastig vinden. De teamleiders is een cursus aangeboden om dpia's uit te voeren, maar volgens respondenten is deze door drukte bij de teamleiders niet doorgegaan. Dat betekent dat de taak om dpia's grotendeels komt te liggen bij de privacy officer en adviseur privacy.

De dpia's worden sinds kort weer opgepakt en er moeten nog ca. 25 stuks uitgevoerd worden. Onder andere een over de Monitor Jeugd, die voor advies voorligt bij de FG. De lichte jeugdzorg moet nog een aparte dpia krijgen. Assessments over de Peutermonitor, Vroegsignalering en Handhaving zijn (bijna) afgerond. Onderweg zijn de dpia's over bodycams bij Boa's en ondermijning. Op een enkele dpia wordt iemand ingehuurd om de teamleiders te ondersteunen.

Wet politie gegevens (WPG)

In aanvulling op de eisen die de AVG is sinds 2019 een aparte richtlijn voor gegevensbescherming door politie en justitie geïmplementeerd in onder andere de Wet politie gegevens (WPG). Deze richtlijn is van toepassing op de verwerking van gegevens die politie en justitie met gemeenten delen, onder andere met de burgemeester en de Boa's. In dat kader moest uiterlijk 2022 door gemeenten een audit worden uitgevoerd, om aan te tonen dat de informatiehuishouding van de gemeente op orde was. Uit de interviews blijkt dat uit de audit bij de gemeente Zutphen veel verbeter-punten naar voren zijn gekomen, die in 2023 opgepakt moeten worden.

5.2.5 Monitoring

Door bezuinigingen op mensen en middelen is de uitvoering van het beleid achter op de beleidsintenties geraakt. Vele wisselingen en uitval van functionarissen en van teamleiders hebben daar ook aan bijgedragen. Zoals eerder aangegeven zijn niet nog niet alle protocollen en procedures op informatiebeveiliging en privacy aanwezig, zijn nog niet alle werkprocessen aangevuld met procedures, is de taakvolwassenheid van de organisatie nog niet op een voldoende hoog niveau.

Information security management system (ISMS)

Voor het genereren van management- en monitoringinformatie is een Information security management system (ISMS) bij de gemeente aanwezig. Dit systeem is gekoppeld aan de PDCA-cyclus.[23] Het ISMS kan ook efficiënt gebruikt worden voor de ENSIA-rapportages (zie hierna). Het systeem is er wel, maar wordt weinig gevuld door de teamleiders, die als

[23] PDCA is de beleidsleercyclus op basis van Plan-Do-Check-Act.

proceseigenaren aan zet zijn om het ISMS te vullen. Verbetering daarop wordt in het Actieplan meegenomen. Zolang het ISMS niet goed gebruikt kan worden, wordt de PDCA-cyclus niet goed nageleefd. Op privacy is ook een management informatiesysteem voorhanden, maar ook dat wordt niet ten volle gebruikt.[24] Op informatiebeveiliging en privacy gebeurt veel ad hoc, volgens enkele respondenten. Dat laat zich ook merken in het systeem 'Engage', dat gestructureerd werkprocessen in kaart kan brengen. Dat is volgens een enkele respondent niet goed gevuld en daar wordt niet op gestuurd. Dit hangt ook samen met de taakvolwassenheid van de lijnorganisatie.

Taakvolwassenheid

Uit de interviews blijkt dat het bewustzijn bij bestuur, MT, teamleiders en medewerkers groeit, maar zeker nog niet op het benodigde niveau is. Een meetlat voor de taakvolwassenheid op informatiebeveiliging van de organisatie op operationeel en strategisch niveau is die van de Nederlandse Beroepsorganisatie van Accountants (zie bijlage 5). Taakvolwassenheid geeft aan in hoeverre de organisatie op alle niveaus in control is op informatiebeveiliging, en in hoeverre medewerkers en management de beveiligingsvoorschriften zelfstandig kunnen uitvoeren. De taakvolwassenheid van de gemeente op informatiebeveiliging is niet gemeten, maar enkele respondenten die bekend zijn met deze meetlat geven aan dat uit de interviews blijkt dat deze tussen de 1 en 2 zou scoren. Dat houdt in dat beheersingsmaatregelen grotendeels aanwezig zijn, echter niet altijd consistent en gestructureerd, maar informeel worden uitgevoerd.

Incidentmanagement

Er is een procedure voor Incidentmanagement en er is een protocol voor het melden van datalekken. Incidenten op ICT, informatiebeveiliging en privacy worden via de helpdesk gemeld in de applicatie Topdesk. Over het algemeen gaat de melding en registratie naar behoren, maar de analyse en evaluatie van de incidenten en datalekken en het leren ervan kan volgens respondenten effectiever. Er waren tot voor kort nog veel openstaande geregistreerde datalekken, onder andere door onderbezetting volgens respondenten. Dat is een van de punten waarop in interviews is aangegeven dat Incidentmanagement en de procedure meldplicht datalekken beleid opnieuw bekeken moeten worden.

Rapportages

De CISO en PO stellen jaarplannen met activiteiten op informatiebeveiliging en privacy op, maar alleen de FG stelt een jaarverslag op. De CISO is wel ENSIA-coördinator, waarin op de vorderingen op de BIO (en deels AVG) worden gerapporteerd, richting landelijke toezichthouders en de gemeenteraad.

Privacyplan 2018

De gemeente Zutphen voldoet nog niet volledig aan de eisen van de BIO en de AVG. Op basis van de 0-meting op de AVG door een extern bureau uit

[24] Er is een extern onderzoek geweest naar de informatiebeheersystemen, maar dat rapport was nog niet openbaar tijdens het onderzoek.

2018 is volgens respondenten te constateren dat een aantal activiteiten uit het toen opgestelde privacy plan door omstandigheden nog niet zijn uitgevoerd.

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), Basisregistratie Ondergrond (BRO), Waardering Onroerende Zaken (WOZ) en de Structuur uitvoeringsorganisatie Werk en Inkomen (SUWI). Over informatiebeveiliging bij het gebruik en/of kwaliteit van deze registraties moet de gemeente door middel van ENSIA verantwoording afleggen richting de rijksoverheid. Met name aan DigiD en Suwinet worden hoge eisen met betrekking tot veiligheid gesteld. Het college moet hierover rapporteren met een assurance-statement van een extern bureau.

Daarnaast wordt in het kader van ENSIA aan de gemeenteraad gerapporteerd over de vorderingen op informatiebeveiliging in het kader van de eisen van de BIO (zie ook §3.4).

Logging

Uit de ENSIA-rapportage over 2021 blijkt dat de gemeente niet aan alle eisen voldoet. Onder andere op de logging [25] en controle op gebruik van Suwinet moeten nog stappen gezet worden. Uit de interviews blijkt dat de standaard rapportages worden gecontroleerd, maar de logging-gegevens niet gecheckt worden op de redenen waarom gegevens uit Suwinet worden ingezien. De procedure daarop is niet up-to-date. Uit de interviews blijkt ook dat er op een aantal andere (zaak)systemen logging mogelijk is en ook wordt geregistreerd, maar dat deze niet periodiek en stelselmatig wordt

[25] Logging is een vorm van monitoring waarbij (inlog)gegevens geautomatiseerd worden geregistreerd, bedoeld om bij te houden welke gebeurtenissen/ handelingen binnen een systeem of applicatie hebben plaatsgevonden.

gecontroleerd. Deze rol moet, volgens respondenten nog belegd worden in het beleid.

SIEM/SOC

Een detectie op verdacht verkeer op de systemen wordt meestal uitgevoerd met zogenoemde Monitoring en Response applicaties.[26] Gemeenten sloten zich via de samenwerking met de VNG aan bij een gezamenlijke inkoop van deze systemen. De gezamenlijke aanbesteding kwam tot een eind vanwege het stopzetten van de samenwerking tussen de VNG en KPN. Net als Zutphen beschikken veel gemeenten momenteel over een suboptimale detectie van dreigingen op de systemen. Uiteraard zijn de systemen van externe inbreuken beschermd door firewalls en virusscanners. Om toegang tot de systemen te krijgen moeten medewerkers ook voldoen aan de 2-factor verificatie (2FA).[27]

5.3 Bescherming van de gegevens

Onderzoeksvraag 3

In deze paragraaf beantwoorden we de derde onderzoeksvraag: In hoeverre zijn gegevens bij de gemeente beschermd tegen de toegang door onbevoegden?

ICT-infrastructuur

De gemeente Zutphen voert de ICT zelfstandig uit, samen met partijen die onderdelen van de infrastructuur in de 'cloud' organiseren.[28] De bescherming van de gegevens is afhankelijk van de wijze waarop de infrastructuur beveiligd is en hoe de werking van de beveiliging periodiek wordt getest. Ook moet getest worden of de dienstverlening van de gemeente bij een calamiteit binnen acceptabele tijd hervat kan worden.

Aansluiting IBD

De gemeente is aangesloten bij de IBD. Via de Algemene Contactpersoon Informatiebeveiliging (ACIB) en de Vertrouwde Contactpersoon Informatiebeveiliging (VCIB) krijgt de gemeente van de IBD updates over acute en minder acute dreigingen op de door de gemeente gebruikte soft- en hardware.[29]

Om na een calamiteit de dienstverlening weer op te starten is een externe uitwijklocatie met dezelfde ICT-infrastructuur voorhanden. Een test of de uitwijk binnen acceptabele tijden uitgevoerd kan worden moet nog uitgevoerd worden, blijkt uit de interviews. Back-ups worden uitgevoerd, maar zoals eerder aangegeven is het back-up procedure recent opnieuw

---

[26] Onder andere SIEM/SOC applicaties: Security Information & Event Management (SIEM) en Security Operations Center (SOC) is software die computerdreigingen en verdacht verkeer op systemen detecteert en monitort.

[27] Twee factor authenticatie is een authenticatie of verificatie methode waarbij twee stappen succesvol doorlopen moeten zijn om toegang te krijgen tot de systemen, zoals naast een wachtwoord het gebruik van een token of biometrisch gegeven.

[28] Uit de interviews blijkt dat er in het verleden samenwerking met de gemeente Apeldoorn op ICT verkend is, maar dat is niet doorgegaan.

[29] De Algemene Contactpersoon Informatiebeveiliging (ACIB) krijgt dreigingsmeldingen van algemene aard door van de IBD. De Vertrouwde Contactpersoon Informatiebeveiliging (VCIB) krijgt meldingen die vertrouwelijk van aard zijn, waarvan het dreigingsniveau van dien aard is dat deze niet openbaar verspreid mag worden.

ingericht maar moet het beleid en beschrijving van de inrichting en beleid nog worden opgesteld.

Testen

In de BIO is opgenomen dat gemeenten de ICT-infrastructuur minimaal 1x per jaar met behulp van pentesten op kwetsbaarheden onderzoeken. De accountant constateerde over 2021 dat de gemeente Zutphen dat niet heeft gedaan. Er is besloten budget uit te trekken om jaarlijks pentesten op de systemen uit te (laten) voeren. In 2022 is dat, in het kader van het Actieplan en met medewerking van het project Troje van de provincie Gelderland wel uitgevoerd. Er is een pentest door een extern bureau uitgevoerd op het externe netwerk. De gemeente is bezig met de verbeterpunten naar aanleiding van de hoge risico's die uit deze test zijn gebleken. Een deel van de verbetermaatregelen moet door de externe partijen, waarmee de gemeente op ICT samenwerkt, worden opgepakt. Ook heeft een mystery guest getracht ongeoorloofd binnen te dringen in het stadskantoor. Daarnaast zijn er onder medewerkers test phishing mails uitgezet. De medewerkers krijgen de resultaten uit de testen teruggekoppeld.

5.3.1 Pentesten

Aanvullend op de pentesten van de gemeente Zutphen heeft de Rekenkamercommissie Zutphen besloten een interne netwerk pentest, een Active Directory audit, een phishing mail test en een mystery guest bezoek uit te voeren. Getest wordt op een beperkt aantal doelen, de reikwijdte of scope van het onderzoek, met een bepaalde risicoclassificatie. Deze risicoclassificatie is in de onderstaande tabel weergegeven.

Tabel 3.5. Risicoclassificatie pentesten.

Risicoclassificatie	Toelichting
Kritisch (9-10)	Extreem hoge kans dat beveiligingsmaatregelen niet voldoende zijn of omzeild kunnen worden en dat hierdoor de kwetsbaarheid misbruikt kan worden met als gevolg catastrofale financiële verliezen.
Hoog (7. 0-8.9)	Hoge kans dat 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 omvat 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.

Afgesproken is dat kritieke risico's meteen gemeld zouden worden aan de CISO en gemeentesecretaris. Dat is niet aan de orde geweest. Hieronder gaan we nader in op de pentesten zelf en de daarbij gesignaleerde risico's.

Interne netwerk pentest

In de periode 12 tot en met 16 december 2022 is door een ethische hacker een test uitgevoerd om de beveiliging van het interne netwerk te testen. Daarmee wordt de effectiviteit van de genomen beveiligingsmaatregelen geverifieerd. Gedurende de pentest zijn drie kwetsbaarheden met een medium risico en 2 kwetsbaarheden met een 'best practice risico' aangetroffen. Op basis van de uitgevoerde pentest, is binnen de scope van de testen, het risico dat de gemeente Zutphen loopt als laag in te schatten.[30] Een pentest is altijd een momentopname en er wordt door ethische hackers altijd binnen een beperkte scope getest. De inschatting is dan ook altijd met het oog op die beperking geldig.

AD audit

De Active Directory (AD) audit is op 6 december 2022 uitgevoerd. Een AD staat beheerders toe om het beleid met betrekking tot rechten van medewerkers in het netwerk van een organisatie te beheren. De audit betrof de in totaal 1.409 accounts van de gemeente Zutphen, dat zijn gebruikers- en beheerdersaccounts. Niet allemaal worden ze door medewerkers en beheerders gebruikt, maar ze zijn wel met toegangsrechten in de Active Directory opgenomen.

De AD audit checkt onder andere op zwakke en gekraakte wachtwoorden. Zwakke wachtwoorden worden gecheckt op de moeilijkheidsgraad, gekraakte wachtwoorden worden vergeleken met een lijst op internet met wachtwoorden die in relatie gebracht kunnen worden met de gemeente.

Er zijn vier domeinen gescand op kwetsbaarheden en zwakheden van de daarin aanwezige accounts van gebruikers en administrators. Deze laatste hebben over het algemeen grotere toegangsrechten dan de gebruikersaccounts. Hieronder rapporteren we de totale aantallen voor alle vier domeinen. Van de in totaal 1.409 gebruikersaccounts zijn 388 met een wachtwoord van een jaar of ouder. De oudste wachtwoorden zijn sinds 2014 niet meer gewijzigd. Er zijn 3 zwakke wachtwoorden gevonden die niet voldoen aan de in het beleid gestelde moeilijkheidsgraad. In totaal zijn er 98 wachtwoorden die vaker gebruikt worden en 285 accounts waarvan niet is ingesteld dat het wachtwoord periodiek vervangen moet worden. 18 accounts hebben een kwetsbare beveiliging (missen de AES-beveiligings-sleutel). 206 accounts hebben wel een wachtwoord, maar is de optie 'password not required' ingeschakeld. Tot slot is op 1 account geen wachtwoord opgeslagen.

[30] De scope van de test kan volgend jaar anders zijn en kan mogelijk veel meer en andere bevindingen opleveren. Zeker gezien er in de afgelopen jaren geen pentesten zijn uitgevoerd.

Van een aantal gebruikersaccounts is het wachtwoord publiekelijk bekend en is het wachtwoord sinds dat deze op internet zijn gepubliceerd niet meer vervangen.[31] Daarnaast zijn op de administrator accounts ook risico's aangetroffen, en deze accounts brengen additionele risico's met zich mee.

Een aantal gevonden kwetsbaarheden lijkt voort te komen uit het niet consequent toepassen van het wachtwoordbeleid. Daarnaast lijkt er geen beleid specifiek met betrekking tot beheerdersaccounts opgesteld te zijn, met een regelmatige check op deze accounts of een melding en check wanneer een account een geprivilegieerde toegang krijgt toebedeeld.

Phishingmail

Er worden regelmatig test phishing mails rondgestuurd aan medewerkers, om de alertheid en meldbereidheid op dit soort mails te vergroten. Daarom heeft de rekenkamercommissie besloten niet nog een keer het bewustzijn van de medewerkers te beproeven, maar raadsleden te testen.

Op 12 en 13 december zijn naar in totaal 57 accounts van @raad.zutphen.nl phishing mails gestuurd. Het bericht was dat een bloemenbezorger voor een dichte deur heeft gestaan en verzocht werd om op een link te klikken voor een nieuwe afspraak. In totaal hebben 10 van de 57 geadresseerden op de link geklikt (18%). Degene die op de link klikten kwamen op een landingspagina waarop werd gemeld dat ze op een test phishing mail hadden geklikt. Zij werden doorverwezen naar een site waarin uitleg werd gegeven hoe ze een phishing mail kunnen herkennen.

Mystery guest

Op 14 december is op de fysieke locatie Henri Dunantweg 1 van de gemeente Zutphen een mystery guest assessment uitgevoerd. Voor deze locatie is gekozen omdat in het kader van het cyberweerbaarheidsproject Troje van de provincie Gelderland het gemeentehuis zelf al door een mystery guest is bezocht.

Door middel van social engineering [32] hebben de assessors toegang proberen te krijgen tot het gebouw, exclusieve ruimtes, documenten en/of computer systemen. Daarmee wordt de effectiviteit van de genomen beveiligingsmaatregelen en het risicobewustzijn van de medewerkers geverifieerd. De assessoren hebben toegang gekregen tot verdiepingen die gesloten zijn voor onbevoegden, toegang tot een technische ruimte en konden ongestoord werkzaamheden op een (eigen) computersysteem verrichten. Bij de rondgang zijn de assessoren niet aangesproken, behalve in een gereserveerde ruimte.

---

[31] Publiekelijk bekende wachtwoorden zijn wachtwoorden die door middel van eerdere hacks zijn verworven/gestolen en die daarna op internet, en met name op het zogenoemde Dark Web, zijn gepubliceerd. Hackers verkopen de wachtwoorden vaak, in combinatie met de daarbij verworven accountnamen. Aangeraden wordt het wachtwoord regelmatig te vernieuwen en niet voor verschillende accounts hetzelfde wachtwoord te gebruiken.

[32] Social engineering is het misbruiken van menselijke eigenschappen zoals nieuwsgierigheid, vertrouwen, hebzucht, angst en onwetendheid.

Resultaten pentesten

Vooraf aan de pentesten is afgesproken dat een kritiek risico meteen gemeld zou worden aan de CISO en gemeentesecretaris, zodat meteen eventuele maatregelen getroffen konden worden. Dat is niet aan de orde geweest. De technische rapporten zijn na afloop en in overleg met de rekenkamercommissie door de ethische hackers met de CISO en de gemeentesecretaris gedeeld. Daarmee kunnen maatregelen genomen worden om de niet kritieke risico's aan te pakken. Een medium of hoog risico kan zich tot een kritiek risico ontwikkelen.

5.4 Hoe wordt de gemeenteraad betrokken bij het informatiebeveiligingsbeleid?

Onderzoeksvraag 4

In deze paragraaf beantwoorden we onderzoeksvraag 4: Hoe wordt de gemeenteraad betrokken bij informatiebeveiliging en privacy?

Informatievoorziening

In de BIO is de eis dat de raad minimaal 1x per jaar in het kader van de P&C-cyclus wordt geïnformeerd over de stand van zaken met betrekking tot informatiebeveiliging. In de jaarstukken van de gemeente over 2021 komt informatiebeveiliging en gegevensbescherming een paar keer aan de orde. Bij risicobeheersing met een kans van 50% op een financieel gevolg van €200.000 en mate van beïnvloeding van 1,22% wordt het volgende risico opgenomen: "Er wordt onvoldoende invulling gegeven aan de wettelijke regels met betrekking tot de beveiliging van persoonsgegevens en informatiebeveiliging." De beheersmaatregel is het aanbieden van trainingen en invullen van functies. De trainingen en applicaties van I-Navigator en een nieuw ISMS worden genoemd. Zoals hiervoor is aangegeven moet het gebruik en de vulling van beide applicaties omhoog om effectief te zijn (zie §5.2.5).

Programma- en meerjarenbegroting

In de programmabegroting 2023 is het risico op langdurige uitval van computersystemen door hacken en gijzelsoftware opgenomen. Met een mogelijk financieel gevolg van €1 miljoen en een mate ven beïnvloeding van 1%.[33] In de Meerjarenbegroting wordt informatieveiligheid een paar keer geadresseerd. Namelijk dat het onderwerp continue aandacht en doorontwikkeling vraagt, op onder andere bewustwording, waarbij de verbetering van het Identity Access Management (IAM) genoemd wordt om te voldoen aan de verbetermaatregelen naar aanleiding van de ENSIA-audits. Aangegeven wordt dat de ICT-omgeving jaarlijks terugkerend intern en extern zal worden getest op kwetsbaarheden.

Motie gemeenteraad

Het onderwerp informatieveiligheid leeft bij de raad, onder andere vanwege de grote incidenten die bij andere gemeenten de afgelopen periode hebben gespeeld. Op 7 november 2022 heeft de gemeenteraad de motie aangenomen met als onderwerp 'cyberrisico'. Door middel van de

[33] Ter vergelijking, de financiële gevolgen van de hack met gijzelsoftware bij de gemeente Hof van Twente zijn berekend op in totaal €3,9 miljoen schade.

motie roept de raad het college op de verbetering van de informatie-beveiliging als vast agendapunt mee te nemen in het driehoeksoverleg burgemeester, griffier en gemeentesecretaris. Ook wordt het college verzocht de raad 2x per jaar te informeren over de stand van zaken rond de verbetering van de informatiebeveiliging.

Accountant

De accountantscontroles zijn voor de raad ook een bron van informatie over informatiebeveiliging en privacy, zoals eerder in dit rapport al is langsgekomen. De controles zijn niet primair gericht op het doen van een uitspraak over de continuïteit of betrouwbaarheid van de gegevens-verwerking door de gemeente. Wel constateert de accountant terecht dat IT een steeds belangrijker onderdeel vormt van de bedrijfsvoering en daarmee ook van de controle op de jaarrekening. De accountant voert op basis daarvan een (beperkte) IT audit uit. Deze is grotendeels gericht is op de rechtmatigheid van de financiële administratie van de gemeente, maar gaat ook breder. Daarmee kan de raad zich een beeld vormen van de bevindingen en beheersingsmaatregelen op authenticatie en autorisaties op enkele applicaties, fysieke beveiliging van de IT-omgeving, al dan niet uitvoeren van controles en pen-testen.[34]

Kaderstelling en controle

Uit de interviews blijkt dat het college en de raad nog geen gesprek zijn aangegaan met betrekking tot de ambitie van de gemeente op informatiebeveiligings- en privacybeleid. Dat is van belang met betrekking tot de kaderstellende rol van de raad. Uitvoering van beleid op Informatiebeveiliging en privacy vergt investeringen. De raad wordt met betrekking tot de controlerende rol geïnformeerd door middel van de ENSIA-rapportage en verder summier geïnformeerd in het kader van de P&C-cyclus. Onder andere vanwege de motie gaat de raad 2x per jaar geïnformeerd worden, dat gebeurt in het Forum. De raad wordt bij dreigende calamiteiten en grote incidenten incidenteel op de hoogte gehouden van het verloop, zoals met de dreiging van Log4J (zie §5.1.4).

Informatiebeveiliging raad

De raadsleden kunnen, vanuit hun rol, ook over (bijzondere) persoonsgegevens beschikken. Vandaar dat besloten is de e-learning voor medewerkers open te stellen voor raadsleden. Daarmee is tot na de verkiezingen en inwerkperiode gewacht.

[34] Zo constateert de accountant in de managementletter 2021 dat het ontbreekt aan procedure voor wijzigingsbeheer t.b.v. de gebruikersorganisatie/applicaties, procedure rondom uitgifte en controle op unieke en individuele gebruikersnamen, periodieke controle op actieve gebruikers, periodieke controle op inrichting van wachtwoordbeleid, procedure voor het gestructureerd toekennen, wijzigen en ontnemen van rechten, periodieke controle op inrichting van rechten in het systeem conform beleid (middels functie-autorisatie matrix).

Bijlage 1. Veel voorkomende termen en afkortingen

2FA	Twee factor authenticatie is een authenticatie of verificatie methode waarbij twee 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
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 informatie-beveiliging 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 kan worden vastgelegd wie toegang had tot persoonsgegevens.
NBA	De koninklijke Nederlandse Beroepsorganisatie van Accountants
NOREA	De Nederlandse Organisatie van Register EDP-Auditors
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 die 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.
Social engineering	Social engineering is een techniek waarbij een aanval op de computerbeveiliging via het verkrijgen van vertrouwelijke of geheime informatie (van personen).
SSO	Single Sign On, op 1 werkplek via 1 aanmelding toegang krijgen tot alle applicaties waar de gebruiker recht op heeft
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 de derde partij, die de gegevens voor de gemeente bewerkt voldoet aan de geldende richtlijnen inzake informatiebeveiliging
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. Lijst geraadpleegde stukken en lijst respondenten

Geraadpleegde stukken

- Accountantsverslag Gemeente Zutphen, Boekjaar 2021, door Baker Tilly, 9-6-2022
- Actieplan privacybescherming en infoveiligheid versie 20220727
- Actieplan privacybescherming en infoveiligheid versie 20220909
- Assurance-rapport IT-auditor, 21-4-2022
- Begeleidend memo Rapportage Securitytest Gemeente Zutphen_v1_ 16-8-2022
- Beleid logische toegangsbeveiliging gemeente Zutphen, 19-10-2020
- Beleidsuitgangspunten toegangsbeleid, 19-10-2020
- Beschrijving nulmeting Project Troje 6 mei 2022
- Bijlage 1_Conclusies en adviezen, Auxzenze
- Checklist Verwerkersovereenkomst
- Coalitieakkoord 2022-2026, gemeente Zutphen
- Communicatie memo – kennistest & motivatiesurvey, 19-09-2022
- Gemeente Zutphen Board letter 2020, 5-1-2021
- Gemeente Zutphen, management letter 2021, 11-1-2021
- Inkoop en aanbestedingsbeleid Zutphen 2018 vastgesteld door college op 22 mei 2018 def
- Inkoopvoorwaarden Leveringen en Diensten gemeente Zutphen 2018
- Jaarrapportage gegevensbescherming 2021, april 2022
- Jaarverslag en -rekening Gemeente Zutphen 2021
- Management letter 2020, 22-12-2020
- Management letter 2021, 11-1-2021
- Meerjarenbegroting gemeente Zutphen, jaarschijf 2023
- Model verwerkersovereenkomst gemeente Zutphen (versie 2.4-1)
- Motie Cyberrisico, 20221107
- Overzicht beleidsstukken informatiebeveiliging en privacy Zutphen
- Overzicht bevindingen en actieplan. Informatiebeveiliging en Privacybescherming (in bewerking), 27-2-2022, Projectgroep versterken privacybescherming en informatieveiligheid
- Procedure Back-up en restore
- Procedure Hardening gemeente Zutphen
- Procedure Incidentmanagement gemeente Zutphen
- Procedure Toegangspassen gemeente Zutphen
- Rapportage Securitytest Gemeente Zutphen - v1.0
- Rollen op privacygebied, intranet
- Strategisch informatiebeveiligingsbeleid gemeente Zutphen 2020-2024, 3-11-2020
- Toelichting kennistest en motivatiesurvey Troje project Wordversie
- Wachtwoordbeleid gemeente Zutphen, 19-10-2020

Functies respondenten

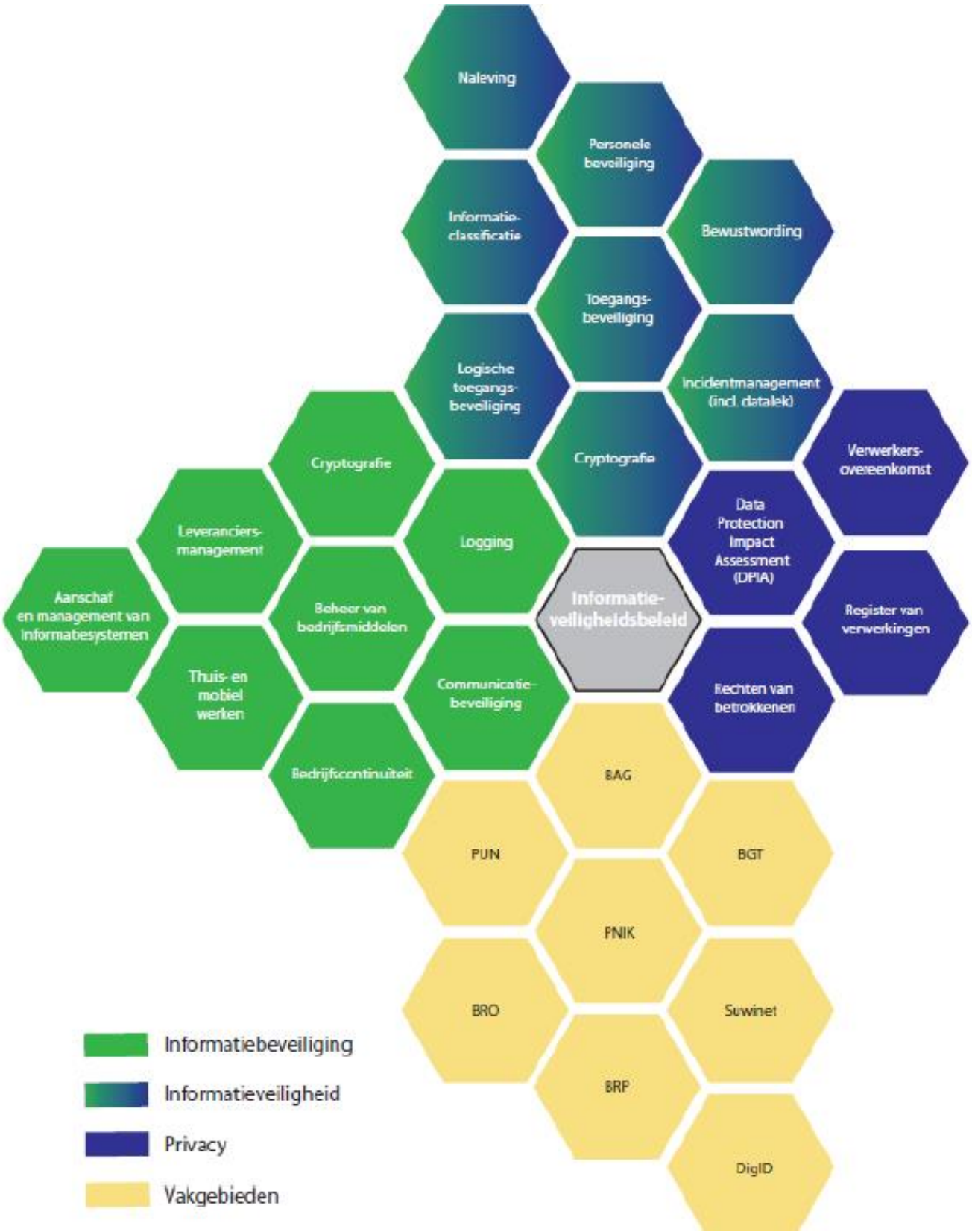
- Gemeentesecretaris
- Portefeuillehouder
- CISO
- FG
- Privacy officer
- Adviseur Privacy
- Afdelingshoofd I&A
- Drie medewerkers afdeling Sociaal Domein

Bijlage 3. Onderzoeksvragen en normen

De onderstaande normen zijn voornamelijk ontleend aan de BIO en de AVG.

Onderzoeksvragen	Normen
1. In hoeverre beschikt de gemeente Zutphen over een adequaat informatiebeveiligings- en privacy-beleid?	- Het college stelt het integrale beleid ten aanzien van informatiebeveiliging en privacy vast. - Er vindt sturing plaats op basis van de BIO. - Het informatiebeveiligingsbeleid is opgesteld aan de hand van een GAP-analyse. Jaarlijks wordt op basis van een risicoanalyse het informatiebeveiligingsplan ingevuld. De gemeente neemt maatregelen om risico's te verlagen. - Op onderdelen van informatiebeveiliging is beleid geformu-leerd en zijn richtlijnen opgesteld, zoals gebruik van wachtwoorden, 2 factor authenticatie, mobiele datadragers, autorisaties en monitoring, protocol datalekken, wijzigings-beleid enz. - De CISO en FG zijn gepositioneerd en geëquipeerd om hun taak adequaat uit te voeren.
2. Hoe wordt het beleid uitgevoerd en wordt de uitvoering gemonitord?	- Het bestuur en medewerkers dragen het beleid ten aanzien van informatiebeveiliging en privacy actief uit. - Medewerkers weten wat ze wel en niet mogen/moeten doen met gegevens, herkennen incidenten en rapporteren deze ook daadwerkelijk. - De gemeente heeft procedures om te leren van beveiligings-meldingen met als doel beheersmaatregelen te verbeteren. - Over het functioneren van informatiebeveiliging en privacy wordt gerapporteerd aan het management, bij voorkeur op basis van een ISMS (Information Security Management System). - Het ISMS, indien aanwezig, is gekoppeld aan de PDCA-cyclus. - Op de systemen is logging geïnstalleerd en er is capaciteit aanwezig om deze te monitoren. - Er is een procedure vastgesteld voor de wijze waarop informatiebeveiligingsgebeurtenissen en zwakke plekken in de beveiliging worden beheerd en gerapporteerd.
3. In hoeverre zijn gegevens bij de gemeente beschermd tegen de toegang door onbevoegden?	- Gegevens die door en/of namens de gemeente worden verwerkt zijn beschermd tegen ongewenste invloeden van buitenaf en van binnenuit. - Er worden jaarlijks beveiligingsaudits uitgevoerd. - De gemeente heeft in beeld met welke partners gegevens worden gedeeld met behulp van het verwerkingsregister. - De gemeente maakt met partners en leveranciers afspraken over het veilig uitwisselen en verwerken van persoonsgegevens en de daarvoor te nemen maatregelen.
4. Hoe wordt de gemeenteraad betrokken bij het informatie-beveiligingsbeleid?	- Over het functioneren van het informatiebeveiligingsbeleid wordt gerapporteerd aan de raad, in ieder geval jaarlijks in het kader van ENSIA.

Bijlage 4. Richtlijnen/procedures Informatiebeveiliging en privacy



Bron: IBD.

Bijlage 5. Volwassenheidsniveau NOREA

Bron: Handreiking bij Volwassenheidsmodel Informatiebeveiliging, januari 2019, NBA.

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.