Rekenkamer Soest

PBLQ

Digitale Veiligheid in Soest, van moetje naar must

Bestuurlijk rapport
17 maart 2025

PBLQ
verbinders in de informatiesamenleving

Inhoudsopgave

1. Conclusies en aanbevelingen 1

1.1 Conclusies 1
1.2 Aanbevelingen 3
1.2.1 Investeer in een robuuste digitale veiligheidsorganisatie 3
1.2.2 Stel op basis van het strategisch beleid een ‘aanvalsplan’ Digitale Veiligheid op dat erop gericht is om aan de wettelijke verplichtingen te voldoen 3
1.2.3 Ontwikkel in samenwerking met de raad een begrijpelijke rapportage gebaseerd op gangbare normenkaders, risico’s en kosten 4

3. Inleiding 5

3.1 Aanleiding 5
3.2 Opdrachtformulering 6
3.3 Normenkader 6
3.4 Werkwijze 7
3.5 Leeswijzer rapport 8

4. Wettelijke Kaders gemeentelijk beleid Digitale Veiligheid 9

5. Beleid en uitvoering Digitale Veiligheid in Soest 11

5.1 Gemeente Soest en de RID 11
5.2 Het beleidskader van de gemeente Soest 12
5.2.1 Incidenten(afhandeling) 13
5.2.2 BIO en ENSIA compliance in Soest 14
5.2.3 Organisatie, taken en verantwoordelijkheden 15
5.2.4 Bewustwording en opleiding informatieveiligheid 15
5.2.5 Crisisoefening 17
5.3 Beantwoording van de onderzoeksvragen 17

6. Informatiebeveiliging in de praktijk 19

6.1 De focusgroep Sociaal Domein 19
6.2 Over de raadsbijeenkomst 20
6.3 Beantwoording van de laatste onderzoeksvragen 20

Bijlage A Geïnterviewde personen 22

Bijlage B Bestudeerde documentatie 23

Bijlage C Stoplichtrapportage normenkader 24

Bijlage D Reactie college van B&W 27

1. Conclusies en aanbevelingen

1.1 Conclusies

Van mei tot en met oktober 2024 heeft PBLQ in opdracht van de rekenkamer een onderzoek uitgevoerd naar informatieveiligheid in de gemeente Soest. Dit onderzoek vond plaats in een periode waarin de ambtelijke organisatie aan het werk was om deze digitale veiligheid te versterken. Het was daarmee een ex-durante onderzoek. Lastig bij dit soort onderzoeken is dat (nog) niet alle informatie beschikbaar is en (nog) niet alle documenten in finale versie beschikbaar zijn voor de onderzoekers. Daarnaast speelt dat bij dit onderwerp sprake is van vertrouwelijke informatie; als informatie over zwakheden in de digitale verdediging van de gemeente openbaar wordt, kunnen hackers of andere kwaadwillenden daar immers van profiteren.

Dit heeft geen gevolgen voor de conclusies van het rapport, wel voor de nuance in de bevindingen. Zo hebben referenten in de interviews melding gemaakt van van een nul-meting digitale veiligheid. Hierin zouden tekortkomingen in de digitale veiligheid van de gemeente naar boven zijn gekomen. Omdat wij geen inzage hebben gekregen in het conceptrapport, kunnen wij geen specifieke uitspraken doen over deze tekortkomingen en de risico's die de gemeente daarbij loopt. Wel doen wij de uitspraak dat de gemeente Soest niet voldoet aan de ondergrens voor informatieveiligheid zoals die is vastgelegd in de Baseline Informatiebeveiliging Overheid (BIO).

Digitalisering en digitale veiligheid is steeds belangrijker voor gemeenten. Er is bijna geen gemeentelijk proces meer zonder digitale component. Omdat gemeenten steeds meer taken krijgen neemt het 'digitale aanvalsvlak' voor cybercriminelen toe. Gemeenten beschikken daarnaast over steeds meer persoonlijke informatie van inwoners, waardoor de kans op een zogenaamde datalek toeneemt. Dit geldt ook voor de gemeente Soest.

Om de werkzaamheden effectief en veilig te kunnen uitvoeren heeft de gemeente Soest, samen met Baarn, Bunnik, Utrechtse Heuvelrug, Wijk bij Duurstede en de Regionale Sociale Dienst een Gemeenschappelijke Regeling opgericht die fungeert als ICT dienstverlener. Deze organisatie, de RID-Utrecht, verzorgt de digitale werkplekken en de digitale infrastructuur voor de aangesloten organisaties. Hierbij is de RID ook deels verantwoordelijk voor de digitale veiligheid. De meeste taken ten aanzien van de digitale veiligheid vallen echter onder de verantwoordelijkheid van aangesloten gemeenten zelf.

Als kader voor de digitale veiligheid heeft de gemeente Soest het 'Strategisch Informatiebeveiliging- en privacybeleid'[1] vastgesteld voor de periode 2024 - 2028. Dit beleidsdocument is gebaseerd op de template van de Informatie Beveiligingsdienst (IBD) van de Vereniging van Nederlandse Gemeenten. In dit strategisch beleidsdocument zijn uitgangspunten, werkwijzen en processen beschreven die in de uitvoeringspraktijk van de gemeente Soest niet of onvoldoende zijn teruggevonden. Zo zou het strategisch beleid uitgewerkt moeten zijn in een jaarplan, zou het plan gebaseerd moeten zijn op continue verbetering (Plan Do Check Act) en zou de verantwoordelijkheid voor informatiebeveiliging voor een belangrjk deel liggen bij het lijnmanagement (three lines model). Zoals gezegd, het betreft hier een 'ex-durante' onderzoek en er wordt aan verbetering gewerkt, maar het is zeer de vraag of dit,

[1] Definitieve versie van 05-06-2024

gezien het huidige cyberdreigingsklimaat voldoende is. In 2025 wordt namelijk de Cyberbeveiligingswet (Cbw) van kracht. Deze wet is gebaseerd op de Europese NIS2 Richtlijn die in oktober 2024 al is vastgesteld. Deze richtlijn en wet stellen nieuwe verplichtingen aan de digitale veiligheid van alle gemeenten. Als er in het huidige tempo wordt doorgewerkt, gebeurt er 'too little too late' en voldoet de gemeente niet aan het wettelijk kader.

Dit betekent niet dat er in de praktijk van de gemeente Soest geen fundament ligt. Alle 'verplichte' functies op dit gebied zijn ingevuld; er is een Chief Information Security Officer (CISO), een Privacy Officer (Privacy Officer) en een Functionaris Gegevensbescherming (FG). Daarnaast vervult de ICT regisseur als ENSIA coördinator ook een rol in de informatiebeveiligingsorganisatie van de gemeente.

Ook blijkt uit het onderzoek dat de gemeente momenteel een inhaalslag aan het maken is op het gebied van informatiebeveiliging en privacy. Zo worden er door de FG en de PO structureel data protection impact assessments (DPIA's) uitgevoerd om de privacy van persoonsgegevens te borgen. Ook werken zij aan het privacy-bewustzijn in de organisatie, onder andere met de uitgave van een stripboek over privacy en een ronde langs de afdelingen. Ook heeft Soest in maart 2024 een goedkeurende ENSIA verklaring over 2023 ontvangen.

Op strategisch niveau is het eerder genoemde strategisch beleidsplan vastgesteld op het gebied van digitale veiligheid en privacy. Hiernaast wordt de samenwerking tussen Soest en de RID op een nieuwe leest geschoeid. Er wordt gewerkt aan een nieuwe Dienstverleningsovereenkomst en een Producten- en Dienstencatalogus, waarmee de dienstverlening van de RID en de daarmee gemoeide kosten transparant gemaakt worden.

Deze inhaalslag heeft er nog niet toe geleid dat de gemeente 'in control' is en planmatig werkt aan het mitigeren van digitale veiligheidsrisico's. De mate waarin de gemeente 'in control' kan worden weergegeven in volwassenheidsniveau' 's. Het gaat hierbij om een vijfpuntsschaal, waarbij 1 het laagste en 5 het hoogste niveau is van volwassenheid. Op dit moment bevindt de informatieveiligheid van de gemeente Soest zich op niveau een. Dat houdt in dat de werkzaamheden veelal Ad-Hoc en op verwerkersniveau plaatsvinden. De PDCA-cyclus, die volgens het strategisch beleidsdocument de basis zou vormen van het beleid, wordt nergens toegepast. De gemeente heeft aangegeven dat het vereiste volwassenheidsniveau vier is als later dit jaar de Cyberbeveiligingswet van kracht is. Hiervoor moet nog veel werk worden verzet.

Een randvoorwaarde voor de realisatie van deze doelstelling is een robuuste digitale veiligheidsorganisatie. Hierbij zijn thans vraagtekens te plaatsen vanwege de gebrekkige invulling van het 'three lines' model, dat beschreven is in het strategisch beleidsdocument. Met name de rol van het lijnmanagement (de eerste lijn) wordt onvoldoende ingevuld. Hiernaast is in de tweede en derde lijn te weinig capaciteit beschikbaar. Zo is de CISO werkzaam voor alle zes bij de RID aangesloten organisaties. Uit de interviews en focusgroepen blijkt dat medewerkers een groot verloop van digitale veiligheids-collega's ervaren. Zij kennen de betreffende medewerkers niet meer bij naam, vinden dat zij op afstand staan en onvoldoende beschikbaar en zichtbaar zijn in de organisatie.

Ook de controlerende en kaderstellende rol van de gemeenteraad is thans onvoldoende ingevuld, Uit het gesprek met de raad, dat in het kader van dit onderzoek plaatsvond, is gebleken dat de raad onvoldoende in stelling wordt gebracht om de sturende rol waar te maken. waar te maken. Duidelijk werd dat het niet aan de raad is om te 'sturen op techniek'. De raad zou wel willen weten of de gemeente voldoet aan de gestelde normen voor een digitaal veilige gemeente. De eerder genoemde

BIO-audit zou hiervoor als basis kunnen dienen. De aanwezige raadsleden gaven aan dit onderwerp belangrijk te vinden en hierover, naast de informatie uit de P&C cyclus, één keer per jaar aanvullende informatie te willen ontvangen.

Resumerend wordt op basis van dit onderzoek gesteld dat:

- ✓ ***De gemeente Soest in RID verband samenwerkt aan digitale veiligheid, maar dat de gemeente zelf verantwoordelijk blijft voor het eigen beleid en de implementatie daarvan;***
- ✓ ***De gemeente in 2024 een adequaat Strategisch Beleidsplan heeft vastgesteld, maar dat er thans onvoldoende conform dit plan wordt gewerkt;***
- ✓ ***De noodzaak wordt onderkend om te voldoen aan de wettelijke kaders die zijn aangegeven in de Europese NIS2 Richtlijn en in de loop van 2025 verplicht worden gesteld in de Cyberbeveiligngswet;***
- ✓ ***De gemeente hiervoor moet groeien van volwassenheidsniveau een naar volwassenheidsniveau vier;***
- ✓ ***Hiervoor extra inspanningen gevraagd worden van de ambtelijke organisatie en***
- ✓ ***De raad op dit moment onvoldoende in staat wordt gesteld om de sturende rol op dit dossier waar te maken.***
- ✓ ***De gemeente thans niet voldoet aan de Baseline Informatieveiligheid Overheden, de BIO norm waardoor de gemeente veiligheidsrisico's loopt.***
- ✓ ***Deze risico's kunnen leiden tot hacks met grote maatschappelijke en financiële gevolgen;***

1.2 Aanbevelingen

Bovenstaande conclusies leiden tot de volgende aanbevelingen die de raad als opdrachten aan het college van B&W kan geven.

1.2.1 Investeer in een robuuste digitale veiligheidsorganisatie

De aandacht voor digitale veiligheid is onvoldoende geborgd in de organisatie. Er moet duidelijkheid komen over de rol en de taken van het lijnmanagement ten aanzien van digitale veiligheid. Daarnaast moet er geïnvesteerd worden in de tweede en derde lijn van het 'three lines' model. Er is meer capaciteit nodig van de CISO, FG en de PO om de benodigde inhaalslag te maken. Hiervoor dienen voldoende middelen beschikbaar te zijn.

1.2.2 Stel op basis van het strategisch beleid een 'aanvalsplan' Digitale Veiligheid op dat erop gericht is om aan de wettelijke verplichtingen te voldoen

Het strategisch beleidsplan digitale veiligheid is een exacte kopie van een format van de Informatie Beveiligingsdienst (IBD) van de VNG en biedt alle aanknopingspunten voor verbetering. Een uitgangspunt van het beleidsplan is dat per jaar uitvoeringsplannen worden uitgewerkt en uitgevoerd. Voor 2025 zou dit uitvoeringsplan de status van aanvalsplan moeten krijgen. In dit aanvalsplan moeten de wettelijke verplichtingen ten aanzien van digitale veiligheid centraal staan. Het aanvalsplan

moet bestuurlijk geborgd zijn; periodieke voortgangsrapportages worden geagendeerd in het College en ook de gemeenteraad wordt periodiek geïnformeerd.

1.2.3 Ontwikkel in samenwerking met de raad een begrijpelijke rapportage gebaseerd op gangbare normenkaders, risico's en kosten

Raadleden ziet het belang van digitale veiligheid, maar hebben onvoldoende (bruikbare) informatie om hierop te sturen. De raad zou geholpen zijn met een jaarlijkse rapportage, waarin zonder jargon wordt aangegeven in welke mate de gemeente voldoet aan de wettelijke normen, wat de risico's van afwijking van deze normen zijn en tegen welke kosten deze risico's kunnen worden gemitigeerd. Op basis van zo'n rapportagemodel kan de raad onderbouwde besluiten nemen en de controlerende- en kaderstellende rol beter vervullen. Het verdient de voorkeur om dit rapport in samenwerking met (een deel van) de raad te ontwikkelen; dit komt de bruikbaarheid ten goede.

3. Inleiding

3.1 Aanleiding

De Rekenkamer van Soest heeft een onderzoek uitgevoerd naar de informatieveiligheid bij de gemeente. Digitale veiligheid heeft voor de gemeente een maatschappelijk en economisch belang en voldoet daarmee aan de criteria van de rekenkamer om onderzoek naar te doen. Dit belang is het best te illustreren aan de hand van de hack bij de gemeente Hof van Twente december 2020. In deze gemeente hadden cybercriminelen ingebroken in de informatiesystemen, de informatie versleuteld en persoonsgegevens buit gemaakt. De criminelen vroegen € 750.000,- losgeld; als zij dat niet zouden krijgen, dan werden de persoonsgegevens te koop aangeboden op het dark web en bleef de informatie op de servers onbruikbaar. Hof van Twente weigerde losgeld te betalen en moest de volledige informatievoorziening opnieuw opbouwen; een kostenpost van meer dan € 4 miljoen. Ook werd er een deuk geslagen in het vertrouwen van de inwoners in hun gemeente omdat hun persoonsgegevens bij de gemeente niet veilig waren opgeslagen.

Gemeenten zijn steeds afhankelijker geworden van digitalisering; elk gemeentelijk proces kent wel een digitale component. Daarom neemt ook het belang van digitale veiligheid toe. Dit belang wordt onderkend door de VNG die met en voor haar leden de Agenda Digitale Veiligheid heeft opgesteld. In deze agenda wordt gepleit voor meer bestuurlijke aandacht voor dit thema. Deze aandacht behelst niet alleen die van de burgemeester of het college van B&W, maar ook van de gemeenteraad. De VNG adviseert de colleges dan ook om periodiek het gesprek met de raad aan te gaan over digitale veiligheid[2].

Ook de Rijksoverheid en Europa dringen met Richtlijnen en wetgeving aan op digitaal veilige gemeenten. De Europese ‘Network and Information Security-directive’ ofwel de NIS2 richtlijn is bedoeld om de cyberbeveiliging en de weerbaarheid van ‘essentiële diensten’, waaronder lokale overheden, in de EU lidstaten te verbeteren. Op dit moment wordt de richtlijn naar Nederlandse wetgeving vertaald. De bepalingen worden opgenomen in de Cyberbeveiligingswet. Dit houdt in dat digitale veiligheid een plicht wordt voor gemeenten; de vrijblijvendheid gaat er vanaf. De Cyberbeveiligingswet treedt naar verwachting in oktober 2025 in werking.

Het gemeentelijk beleidsdomein van digitale veiligheid is dus, ook in Soest, volop in beweging. Daarom is dit een ‘ex-durante’ onderzoek; in de periode van het onderzoek is de gemeente Soest aan het werk om de digitale veiligheid te verbeteren. Dat betekende dat sommige documenten nog niet of in conceptversie beschikbaar waren. Dat leidde tijdens het onderzoek tot vragen of deze documenten gedeeld konden worden met de rekenkamer. In enkele gevallen is positief gereageerd op deze vragen en zijn aanvullende documenten gedeeld.

Gezien de toegenomen cyberdreigingen en de (op handen zijnde) wettelijke verplichting voor gemeenten op het gebied van digitale veiligheid is het van belang dat de gemeenteraad zijn kaderstellende en controlerende rol op dit domein invult. Het doel van dit onderzoek is om daaraan een bijdrage te leveren.

[2] VNG, ‘Digitale veiligheid en de gemeentelijke bestuurder – Bestuurlijke prioriteiten bij het IBD dreigingsbeeld 2023-2024’

3.2 Opdrachtformulering

De rekenkamer heeft onderzoeks- en adviesbureau PBLQ de opdracht gegeven om het onderzoek uit te voeren. Het doel van het onderzoek is ‘om voor de raad in beeld te brengen welke maatregelen genomen zijn om cyberaanvallen af te slaan, of de organisatie goed ingericht is om cyberaanvallen voor te blijven en om te beoordelen of de gemeente in een crisissituatie door een cyberaanval in staat is juist te handelen om de schade zo klein mogelijk te houden.’

De centrale vraag van dit onderzoek luidt als volgt:
Is het informatieveiligheidsbeleid van de gemeente Soest doeltreffend om cyberaanvallen zo veel mogelijk tegen te gaan en is de gemeentelijke organisatie voldoende toegerust om bij een toch geheel of gedeeltelijk geslaagde cyberaanval effectief te handelen?

Deze centrale vraag is opgesplitst in de volgende deelvragen:

- *Wat doet de gemeente aan het tegengaan van een cyberaanval en doet de gemeente dat beter, gelijk aan of slechter dan andere gemeenten?*
- *Hoe wordt het informatieveiligheidsbeleid uitgevoerd en zijn daar hiaten in te constateren, beoordeeld aan de hand van actuele maatstaven?*
- *Wat is protocollair vastgelegd over de informatieveiligheid, voldoet dat aan de huidige maatstaven en is het toereikend?*
- *Wat is de rol van de gemeenteraad bij Informatieveiligheidsbeleid en zijn de verantwoordelijkheden tussen raad – college – ambtelijke organisatie – RID duidelijk vastgelegd, geïmplementeerd en effectief ingericht gezien actuele maatstaven?*
- *Heeft Soest een crisisprotocol dat voorziet in handelingsperspectief, crisisorganisatie en (gemandateerde) beslissingsbevoegdheden aan bijvoorbeeld college of directeur RID in het geval van een (gedeeltelijk) geslaagde cyberaanval? In hoeverre zijn deze protocollen, mandaten en draaiboeken geïmplementeerd en toereikend gezien de actuele maatstaven?*
- *In hoeverre is de gemeentelijke organisatie voldoende wendbaar en adaptief om zich snel genoeg aan te kunnen passen aan nieuwe dreigingen? Welk lerend vermogen is er op dat gebied en in hoeverre is het beleid hierin ondersteunend?*
- *Wat is de cultuur in de gemeente ten aanzien van informatiebeveiliging en de digitale weerbaarheid van de gemeenten?*

3.3 Normenkader

Op basis van bovenstaande vragen hebben wij een normenkader uitgewerkt. Onderstaand normenkader, dat normen bevat over het gemeentelijk beleid, de uitvoeringspraktijk en de cultuur is toegepast in dit onderzoek:

Het normenkader ziet er als volgt uit:
Normen ten aanzien van het gemeentelijk beleid:

- De gemeente heeft informatiebeveiligingsbeleid dat voldoet aan de norm ‘Baseline Informatieveiligheid Overheid (BIO)’;
- De algemene uitgangspunten en kaders zijn besproken in en vastgelegd door de gemeenteraad.
- In het beleid wordt o.a. ingegaan op:
  - Strategische uitgangspunten
  - Risicomanagement

- Governance (waaronder rollen en verantwoordelijkheden)
- De PDCA-cyclus van de gemeente

- In (voortgangs)rapportages wordt ingegaan op informatiebeveiliging.
- In programma's en projecten wordt expliciet aandacht besteed aan informatiebeveiliging.
- Er is een procedure hoe wordt omgegaan met informatiebeveiligingsincidenten (waaronder cyberaanvallen) en een crisisprotocol.
- De gemeente heeft beleid voor informatiebeveiliging ten aanzien van samenwerkingspartners, gemeenschappelijke regelingen en leveranciers.

Normen ten aanzien van de Uitvoeringspraktijk

- In de praktijk wordt gehandeld conform de wijze waarop informatie wordt beveiligd, waaronder in de relevante werkprocessen, de toewijzing van verantwoordelijkheden, de inrichting van informatiesystemen, de autorisaties, de afspraken voor de verwerking van gegevens en de afspraken over het informeren van burgers en het vragen van toestemming.
- De gemeente heeft een leer- en verbetercyclus (PDCA-cyclus).
- De gemeente heeft inzicht in de belangrijkste verbeterplannen en –maatregelen.
- Er wordt in het geval van incidenten, calamiteiten en crisis volgens de vastgelegde procedures gehandeld.
- De vastgelegde controles en rapportages worden in de praktijk uitgevoerd.
- De gemeente test en toetst procedures regelmatig om de effectiviteit en werking te toetsen.
- De gemeente houdt toezicht op de afspraken ten aanzien van informatiebeveiliging met (samenwerkings)partners, regelingen en leveranciers.
- De raad wordt geïnformeerd op een manier die hem in staat stelt te sturen en te controleren.

Normen ten aanzien van de organisatiecultuur

- De medewerkers van de gemeente zijn bekend met het gemeentelijk beleid met betrekking tot informatiebeveiliging en worden van aanpassingen op de hoogte gehouden.
- In hun dagelijks functioneren geven de medewerkers er blijk van het gemeentelijk informatiebeveiligingsbeleid na te leven.
- In de relatie met ketenpartners bewaken de medewerkers actief dat deze ketenpartners zich conformeren aan de regels, standaarden en procedures van de gemeente op het gebied van informatiebeveiliging.

In het bestuurlijk rapport geven wij in Bijlage C met een stoplichtenrapportage aan of de gemeente Soest voldoet aan dit normenkader.

3.4 Werkwijze

Dit onderzoek bestaat uit verschillende fasen. Wij zijn begonnen met de startbijeenkomst voor betrokken medewerkers en bestuurders van de gemeente. Naast een toelichting op het onderzoek hebben wij in deze bijeenkomst ook ingezet op draagvlakverbreding. In deze bijeenkomst hebben we benadrukt dat leren en ontwikkelen ons belangrijkste uitgangspunt voor dit onderzoek is. Wij zijn op zoek naar wat er goed gaat en wat er beter kan! Vervolgens hebben wij een documentstudie uitgevoerd en verdiepende interviews gehouden. Om te onderzoeken hoe in Soest het beleid in praktijk wordt gebracht hebben we bijeenkomsten met twee focusgroepen en een raadsbijeenkomst

georganiseerd. Op basis van de verkregen informatie hebben wij onze analyse uitgevoerd en deze rapportage geschreven.

3.5 Leeswijzer rapport

Dit rapport is als volgt ingedeeld. In het volgende hoofdstuk wordende wettelijke en kwalitatieve kaders voor het gemeentelijk digitale veiligheidsbeleid beschreven. Wij gaan dieper in op (veranderingen in) de wet- en regelgeving als de NIS2 richtlijn, de Cybersecurity wet, de BIO2 en ENSIA2. Ook geven wij inzicht in de prioriteiten van de VNG, zoals beschreven in de Agenda Digitale Veiligheid, die relevant zijn voor alle gemeenten en dus ook voor Soest. Wij zijn van mening dat kennis van (de verandering van) dit wettelijk kader noodzakelijk is voor de gemeenteraad om sturing te kunnen geven aan dit domein.

Vervolgens behandelen wij in hoofdstuk drie het beleid en de uitvoering daarvan in de gemeente Soest. Dit hoofdstuk bevat een belangrijk deel van de bevindingen van ons onderzoek. De Regionale ICT Dienst Utrecht (RID) speelt hierbij een belangrijke rol. Deze RID is een Gemeenschappelijke Regeling (GR) waaraan naast Soest andere gemeenten aan deelnemen. In hoofdstuk drie beschrijven wij hoe de taken en verantwoordelijkheden ten aanzien van (de uitvoering van) het digitale veiligheidsbeleid verdeeld zijn tussen beide organisaties. Wij eindigen dit hoofdstuk met de beantwoording van het eerste deel van de onderzoeksvragen zoals hierboven in paragraaf 1.2 verwoord.

In hoofdstuk vier beschrijven wij onze bevindingen uit de focusgroepen en de raadsbijeenkomst die in september hebben plaatsgevonden. Dit hoofdstuk eindigt met de beantwoording van de resterende onderzoeksvragen.

In de bijlagen treft u ten slotte een overzicht van de medewerkers en bestuurders die wij in het kader van dit onderzoek hebben gesproken plus een overzicht van de documenten die wij hebben geraadpleegd.

4. Wettelijke Kaders gemeentelijk beleid Digitale Veiligheid

Een van de deelvragen van dit onderzoek heeft betrekking op de maatstaven van het digitale veiligheidsbeleid. Deze maatstaven zijn (of worden op korte termijn) vastgelegd in Europese Richtlijnen en nationale wetgeving waaraan alle gemeenten, dus ook de gemeente Soest moeten voldoen. Wij zijn van mening dat het voor raadsleden belangrijk is om hier kennis van te nemen om hun controlerende en kaderstellende rol te kunnen vervullen. Daarom beschrijven wij in dit hoofdstuk welke maatstaven relevant zijn voor gemeenten en schetsen wij de huidige ontwikkelingen die leiden tot aanpassingen ervan. Ook beschrijven we de samenhang tussen de juridische kaders en deze maatstaven.

Bij de uitvoering van het digitale veiligheidsbeleid maken gemeenten gebruik van verschillende normenkaders. De belangrijkste kaders zijn de Algemene Verordening Gegevensbescherming (AVG), de Baseline Informatiebeveiliging Overheid (BIO) en de Eenduidige Normatiek Single Information Audit (ENSIA). Hiernaast is een wettelijk kader in ontwikkeling, dat volgt uit de Europese Network- and Information Security 2 directive, de NIS2 richtlijn. Deze richtlijn is niet rechtstreeks van toepassing op gemeenten, maar wordt uitgewerkt in de Cyberbeveiligingswet, waar gemeenten wel aan dienen te voldoen. Naar verwachting wordt de wet in het derde kwartaal van 2025 ingevoerd. Vanaf het moment dat de wet ingaat moet de gemeentelijke digitale veiligheid voldoen aan de eisen die in deze wet staan.

Algemene Verordening Gegevensbescherming
In 2018 is de Algemene Verordening Gegevensbescherming (AVG) in werking getreden.[1] Deze verordening betreft een uitwerking van Europese regelgeving die bedoeld is om de privacy van alle inwoners (beter) te beschermen. De Autoriteit Persoonsgegevens houdt toezicht op de uitvoering van de AVG in Nederland. Wanneer gemeenten de bescherming van persoonsgegevens niet op orde hebben, riskeren zij een boete van de Autoriteit Persoonsgegevens. Het maatschappelijk en financieel belang van een adequaat privacybeleid is groot. Gemeenten hebben echter niet alleen een goed privacybeleid nodig, maar ook een goede uitvoering daarvan. Beiden zijn verplicht op grond van de AVG. Omdat de beveiliging van persoonsgegevens veel raakvlak heeft met de beveiliging van informatie in het algemeen, zijn de verplichtingen die voortvloeien uit de AVG ook meegenomen in dit onderzoek.

Baseline Informatiebeveiliging Overheid
De BIO is sinds 2018 het verplichte basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (en dus ook gemeenten). De BIO is gebaseerd op de informatiebeveiligingsstandaarden ISO 27001 en ISO 27002 en omvat een minimum aan maatregelen die getroffen moeten worden op het gebied van informatiebeveiliging. Gemeenten baseren hun informatiebeveiligingsbeleid en hun verantwoording aan de gemeenteraad en de toezichthouders vanuit het Rijk in belangrijke mate op deze BIO.

De BIO wordt op dit moment doorontwikkeld naar de BIO2 en zal wettelijk verplicht worden onder de Cyberbeveiligingswet, de wet die volgt uit de implementatie van de NIS2. In de BIO2 is mede naar aanleiding van de komst van de Cyberbeveiligingswet de verantwoordelijkheid van het hogere management in de gemeentelijke informatiebeveiliging vastgelegd. Ook het toewijzen van benodigde

middelen, het verhogen van veiligheidsbewustzijn en het uitvoeren van controles maken onderdeel uit van de BIO2.

Eenduidige Normatiek Single Information Audit
ENSIA is ontstaan uit een gezamenlijk initiatief van een aantal departementen en de VNG. Het doel van ENSIA is om tot een effectief en efficiënt ingericht verantwoordingsstelsel voor informatieveiligheid te komen. De ENSIA is een jaarlijkse audit die gebaseerd is op de BIO. Uitgangspunt voor ENSIA is het horizontale verantwoordingsproces waarin het college van B&W zich over de informatieveiligheid verantwoordt aan de gemeenteraad. Deze verantwoording vormt de basis voor de verantwoording aan de stelselhouder (bijvoorbeeld het ministerie van BZK of SZW). Er wordt dus jaarlijks één audit uitgevoerd waarvan (een deel van) de resultaten zowel naar de gemeenteraad als de stelselhouder gaan. Net als de BIO, wordt ook de ENSIA op dit moment doorontwikkeld naar een nieuwe versie. Deze moet vooral gebruikersvriendelijker worden, zowel voor de ambtelijke organisatie als het gemeentebestuur.

NIS2 en de Cyberbeveiligingswet
De NIS2 richtlijn van de Europese Unie heeft als doel om de informatiebeveiliging van essentiële diensten, waaronder die van gemeenten, in de EU-lidstaten te verbeteren. In de NIS2 is hiertoe onder meer een zorgplicht en een meldplicht opgenomen, en wordt ook het toezicht op informatiebeveiliging geregeld. De NIS2 richtlijn is niet rechtstreeks van toepassing op gemeenten, maar wordt uitgewerkt in de Cyberbeveiligingswet, waar gemeenten wel aan dienen te voldoen. Naar verwachting wordt de wet in het derde kwartaal van 2025 ingevoerd. Vanaf het moment dat de wet ingaat moet de gemeentelijke digitale veiligheid voldoen aan de eisen die in deze wet staan.

De maatregelen die de Cyberbeveiligingswet voorschrijft om de informatiebeveiliging te verbeteren, de zorgplicht, zijn grotendeels opgenomen in de BIO2. In de Cyberbeveiligingswet gaat het naast de beveiliging van kantoorautomatisering (KA) ook over de beveiliging van operationele technologie (OT). Deze OT betreft bijvoorbeeld gemeentelijke bruggen en sluizen die op afstand worden bediend, en camera's in de openbare ruimte. Nieuw met de komst van de Cyberbeveiligingswet is ook dat er naast ad hoc toezicht (achteraf, via rapportage aan de raad en de stelselhouders bij het Rijk) ook pro-actief toezicht zal worden gehouden op de digitale beveiliging van gemeenten. De Rijksinspectie Digitale Infrastructuur (RDI) is daarvoor aangewezen als toezichthouder voor de gemeenten en andere overheidsorganisaties.

De invoering van de Cyberbeveiligingswet leidt tot een taakverzwaring van gemeenten. Bij de ledenvergadering van de VNG in juni 2024 heeft de gemeente De Bilt, samen met de gemeenten Soest, Baarn Utrechtse Heuvelrug, Bunnik en Wijk bij Duurstede de motie 'NIS2: geen taken zonder knaken' ingediend. In deze motie wordt het bestuur van de VNG opgeroepen om bij het Rijk te bepleiten dat de NIS2 richtlijn in samenhang met komende richtlijnen op dit domein worden ingevoerd en dat er voldoende middelen voor gemeenten beschikbaar worden gesteld door het Rijk voor de implementatie. De ledenvergadering heeft deze motie aangenomen.

5. Beleid en uitvoering Digitale Veiligheid in Soest

Na het wettelijk kader dat geldt voor alle gemeenten, presenteren wij in dit hoofdstuk onze bevindingen over de wijze waarop het digitale veiligheidsbeleid in de gemeente Soest is ingericht en wordt uitgevoerd. De gemeente werkt hierbij sinds 2017 samen met de RID. In dit hoofdstuk gaan wij daarom eerst dieper in op deze samenwerking met de RID, waarbij wij aangeven welke taken de RID uitvoert voor Soest op het gebied van digitale veiligheid. De taken die niet bij de RID zijn belegd, worden door de gemeente Soest zelf uitgevoerd. Zo is de gemeente Soest zelf verantwoordelijkheid voor het beleid en de uitvoering daarvan. In paragraaf 3.2 beschrijven wij de wijze waarop dit in de gemeente gebeurt). Tot slot beantwoorden we in dit hoofdstuk het eerste deel van de onderzoeksvragen in paragraaf 3.3.

5.1 Gemeente Soest en de RID

De gemeente Soest is aangesloten bij de RID, een gemeenschappelijke regeling (GR) voor ICT beheer. Naast Soest maken Baarn, Bunnik, De Bilt, Utrechtse Heuvelrug, Wijk bij Duurstede en de Regionale Sociale Dienst in Zeist deel uit van deze GR. Deze organisaties zijn allen vertegenwoordigd in het Algemeen Bestuur van de GR.

Deze GR is in 2012 opgericht met als doelstelling:
'Het zorg dragen voor een betere (adequate) ICT dienstverlening voor die deelnemende organisaties. Door samen te werken kan dit worden gerealiseerd. Samenwerking biedt schaalvoordelen en ''het geheel is meer dan de som der delen''.

De RID verzorgt veilige digitale werkplekken voor de medewerkers van de aangesloten organisaties; het gaat hierbij zowel om apparatuur als om generieke applicaties. Soest en de RID werken samen op basis van een Dienstverleningsovereenkomst (DVO) uit 2017. Omdat de huidige DVO, mede vanwege het toegenomen thuiswerken sinds Corona, verouderd is en geen goede weerspiegeling meer biedt van de diensten die de RID levert[3], is een nieuwe overeenkomst in voorbereiding. Op basis van de DVO is tevens een gedetailleerde producten- en dienstencatalogus opgesteld. De nieuwe DVO was ten tijde van dit onderzoek in concept gereed. Besluitvorming over deze DVO was in voorbereiding.

In de nieuwe DVO wordt in hoofdstuk 2.9 de verantwoordelijkheid voor de informatiebeveiliging van de RID benoemd. Hier staat dat 'de RID gaat over het beveiligen van zowel de hardware (zoals servers, netwerkinfrastructuur en werkplekken) als de data die in beheer is bij de RID.' Informatiebeveiliging bij de RID is ingericht op basis van de BIO, waarbij de nadruk ligt op beschikbaarheid, integriteit en vertrouwelijkheid.

De rolverdeling tussen Soest en de RID ten aanzien van digitale veiligheid is nader beschreven in de notitie 'rolverdeling rondom informatiebeveiliging' van 7 juni 2023. In dit document is op hoofdlijnen de verdeling in verantwoordelijkheden en taken benoemd, waarbij de RID onder meer verantwoordelijk is voor de informatiebeveiliging van de generieke software en infrastructuur. De RID voert hiertoe onder

[3] De DVO van 2017 gaat uit dat werkplekken zich op het gemeentehuis bevinden. Sinds Corona is het gebruikelijk dat ambtenaren (meer) thuis werken. Dat heeft consequenties voor de devices (laptops en smart phones) en beveiliging daarvan. In de nieuwe DVO wordt hiermee rekening gehouden.

andere technische pentesten uit op de infrastructuur van gemeenten en rapporteert en adviseert de aangesloten gemeenten vervolgens over verbeteringen.

Ten aanzien van de Chief Information Security Officer (CISO) hebben de RID en aangesloten organisaties een gedeelde verantwoordelijkheid. De CISO wordt (tijdelijk) ingehuurd door de RID, maar werkt voor de bij de RID aangesloten gemeenten[4]. De CISO dient dus zes 'heren' en is voor elk van de gemeenten maar beperkte tijd beschikbaar.

De RID en deelnemende gemeenten hebben ook een gezamenlijke crisisstructuur voor cyberincidenten opgesteld. De structuur is opgezet voor het geval zich een verstoring voordoet van een applicatie of systeem waar de RID voor verantwoordelijk is. De teams, overlegstructuren en bevoegdheden daarvoor zijn uitgewerkt aan de hand van een viertal scenario's. De deelnemende partijen onderscheiden hierin drie vormen van opschaling: intern, RID en extern. De RID wordt genoemd als meest cruciale partner in het afhandelen van een cyberincident omdat daar de technische kennis ligt.

De gemeente Soest is zelf verantwoordelijk voor het beleid ten aanzien van digitale veiligheid en de uitvoering daarvan, voor zover niet belegd bij de RID. Hiertoe heeft de gemeente een visie en een beleidskader opgesteld en een veiligheidsorganisatie ingericht. Het beleid van de Gemeente Soest wordt in de volgende paragraaf nader omschreven.

5.2 Het beleidskader van de gemeente Soest

Het strategisch beleid voor informatiebeveiliging en privacy is bij de Gemeente Soest vastgelegd in het document 'Strategisch informatiebeveiliging- en privacybeleid'[5]. Hiervoor heeft de gemeente het format van de Informatie Beveiligingsdienst (IBD, een onderdeel van de VNG) overgenomen. Dit heeft als voordeel dat het een 'state of the art' document is, waarin alle aspecten van het strategisch informatiebeveiligingsbeleid beschreven zijn. Het nadeel is dat in het document geen betrekking heeft op de organisatie van de gemeente Soest[6]. Het beleidsdocument is hierdoor een algemene beschrijving van voorbeeldbeleid en is geen richtinggevend document voor de gemeente Soest.

Algemene voorbeelden van zaken die in het Strategisch beleid worden beschreven, maar in de praktijk (nog) niet zijn aangetroffen zijn:

- Informatieveiligheid van de organisatie zou volgens het beleidsdocument gebaseerd moeten zijn op de 'tien bestuurlijke principes voor informatiebeveiliging', die vooral gaan over de rol van het gemeentebestuur bij het borgen van informatiebeveiliging in de gemeentelijke organisatie. Enkele voorbeelden van deze principes zijn: 'Informatiebeveiliging is risicomanagement' (bestuurlijk principe 3) en 'Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking' (bestuurlijk principe 5). In de praktijk van de gemeente Soest is niet gebleken dat het bestuur deze principes als leidend gebruikt in hun rol.

[4] De RID beschikt over een eigen CISO voor de digitale veiligheid van de eigen organisatie.
[5] Versie 03-10-2024
[6] Het 1 op 1 overnemen van het format blijkt uit het feit dat vergeten is om de naam van de gemeente Soest in te vullen: 'Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds digitaler wordende overheid maakt het zorgvuldig omgaan met persoonsgegevens steeds complexer en noodzakelijker. De gemeente <naam> is zich hiervan bewust….. ', Strategisch Gemeentelijk Informatiebeveiliging beleid gemeente Soest, Pagina 7

- Volgens het strategisch beleid wordt ‘Het strategisch beleid gebruikt om de basis te leggen voor de tactische beleidsplannen en daarmee richting te geven voor verdere invulling van informatiebeveiliging en privacy op tactisch en operationeel niveau’[7]. Deze tactische en operationele plannen hebben wij niet aangetroffen.

- De PDCA cyclus zou volgens het strategisch beleid de basis vormen voor informatiebeveiliging: ‘Informatiebeveiliging en privacybescherming is een continu verbeterproces. ‘Plan, do check en act’ vormen samen het managementsysteem van informatiebeveiliging en privacybescherming’[8]. In praktijk hebben wij deze PDCA nergens aangetroffen. Deze bevinding wordt ondersteund in een presentatie van de CISO en de PO aan het MT waarin is aangegeven dat het de uitvoering van het digitale veiligheidsbeleid zich thans op het laagste volwassenheidsniveau (niveau 1) bevindt. Dat betekent dat ‘de werkzaamheden op verwerkingsniveau informeel worden uitgevoerd’. Dit moet naar niveau 4 bij het in werking treden van de NIS2 richtlijn. Bij dit niveau hoort dat ‘de prestaties worden gemeten, vergeleken met de branche en gebruikt voor een optimaal lerend vermogen’.

- De teamleiders zijn volgens het strategisch beleid verantwoordelijk voor het nakomen van het informatiebeveiligingsbeleid. Zij hebben de verantwoordelijkheid voor voldoende bewustwording in hun organisatieonderdeel. De medewerkers dragen eigen verantwoordelijkheid voor het zorgvuldig omgaan met informatieveiligheid. In de praktijk van de gemeente Soest is dit onvoldoende het geval. Het lijnmanagement neemt onvoldoende verantwoordelijkheid voor informatieveiligheid. Medewerkers geven aan dat de functionarissen die belast zijn met informatieveiligheid en privacy onvoldoende zichtbaar zijn in de organisatie.

Hieronder gaan we nader in op de uitvoering van cruciale aspecten van het veiligheidsbeleid, waarbij wij telkens de verbinding maken met het strategisch beleidsdocument.

5.2.1 Incidenten(afhandeling)

In het Strategisch Informatiebeveiligingsbeleid is een paragraaf opgenomen over incidenten(afhandeling). In de gemeente Soest is dit nader uitgewerkt in twee verschillende processen voor het vastleggen van incidenten. *De datalekkenprocedure* beschrijft het proces voor het melden en afhandelen van informatiebeveiligingsincidenten. In deze procedure worden ook definities en kaders beschreven, alsmede taken en verantwoordelijkheden voor het melden en afhandelen van incidenten. In het document *procedure melden van datalekken* worden de te nemen stappen uitgelicht, waarbij tevens proceseigenaren benoemd zijn.

De gemeente Soest heeft voor het melden van incidenten een eigen systeem. Bij de CISO en/of FG wordt een datalek gemeld en zij zorgen dan ook voor de afhandeling, waaronder het onderzoek en het verslag. De CISO is daarnaast verantwoordelijk voor de actualisatie van de procedure, de bekendmaking en het in kennis stellen van een datalek onder medewerkers, de medewerker is verantwoordelijk voor het melden van een datalek binnen de interne organisatie. De FG is verantwoordelijk voor de verdere afhandeling van een datalek naar het management en het bestuur. Meldingen komen ook bij de PO binnen daar de FG en de PO een gezamenlijke mailbox hebben.

[7] Strategisch Gemeentelijk Informatiebeveiliging beleid gemeente Soest, Pagina 6
[8] Idem, Pagina 8

De procedure voor het melden en vastleggen van incidenten is onderhevig aan een jaarlijkse controle, uitgevoerd door de CISO. Eventuele bevindingen worden opgenomen in een verbeter- en adviesplan. De CISO beoordeelt hierbij ook of de procedure nog in overeenstemming is met de uitvoering. Uit de interviews en documentatie blijkt dat het proces rondom de jaarlijkse controle momenteel onvoldoende geborgd en gedocumenteerd is. Er wordt niet planmatig verbeterd en er wordt niet gedocumenteerd gemonitord. De belangrijkste discrepantie met het beleidsdocument is dat de PDCA cyclus niet wordt toegepast op de incidentprocessen. Wij hebben geen verbeterplannen ontvangen en ook in de interviews is hierover geen informatie ontvangen.

5.2.2 BIO en ENSIA compliance in Soest

In het Strategisch Informatiebeveiliging- en privacybeleid wordt de BIO genoemd als het normenkader voor digitale veiligheid voor de gemeente. Een overheidsorganisatie die niet voldoet aan de normen van de BIO, voldoet dus niet aan het basisbeveiligingsniveau.

De gemeente Soest heeft een BIO zelfevaluatie uitgevoerd over de periode 2022 – 2023. Het BIO normenkader is ingedeeld in verschillende hoofdcategorieën (Technische maatregelen, Mensgerichte maatregelen, Organisatorische maatregelen en Fysieke maatregelen). De zelfevaluatie is een vragenlijst waarin is aangegeven of de gemeente wel, niet of deels voldoet aan de gestelde norm. In de audit over 2022 - 2023 zijn de vragen als volgt beantwoord:

BIO-audit 2022 – 2023	
Voldoet niet	112
Voldoet wel	82
Voldoet deels	35

De gemeente Soest is dus niet BIO compliant en voldoet daarmee niet aan het basisbeveiligingsniveau dat aan overheidsorganisaties wordt gesteld. Naar aanleiding van de zelfevaluatie is geen verbeterplan opgesteld.

Uit interviews gebleken dat de gemeente Soest ten tijde van de uitvoering van het onderzoek een ‘0-meting informatieveiligheid’ uitvoert. Voor deze 0-meting dient de BIO als basis. Deze 0-meting zou als input dienen voor een verbeterplan. Wij maken hieruit op dat de organisatie stappen zet om, conform de PDCA cyclus te werken aan de structurele verbetering van de digitale veiligheid. Ten tijde van het onderzoek was er echter nog geen rapportage over deze 0-meting beschikbaar.

Wel beschikt de gemeente over een goedkeurende auditverklaring voor de verplichte externe ENSIA audit[9] die specifiek gericht is op Suwinet, P-wet, BRP en reisdocumenten. Voor deze informatiesystemen voldoet de gemeente dus wel aan de gestelde veiligheidseisen.

.

[9] Gemeente Soest ENSIA 2023, rapportnummer AAS2023-1855

5.2.3 Organisatie, taken en verantwoordelijkheden

Uitgangspunt voor de organisatie van informatieveiligheid is volgens het strategisch beleid het 'Three lines' model[10]. In dit model wordt de eerste lijn gevormd door het lijnmanagement dat verantwoordelijk is voor informatiebeveiliging binnen de eigen processen. De tweede lijn bestaat uit de CISO, Security Officers en Privacy Officer. Hun rol is om te ondersteunen, te adviseren en coördineren. De derde lijn betreft het intern toezicht door een auditor en/of FG. De ENSIA coördinator behoort ook tot deze derde lijn.

De rol van het lijnmanagement wordt in de gemeente Soest ingevuld door de Concernmanager van het aandachtsgebied Bedrijfsvoering en de gemeentesecretaris. De overige lijnmanagers hebben geen formele rol als het gaat om digitale veiligheid. Aangegeven wordt dat de organisatie wordt gekenmerkt door een informele organisatiecultuur. Taken zijn niet formeel belegd en als er wat gebeurt, dan weten management en medewerkers elkaar wel te vinden, zo wordt in interviews aangegeven. Geconcludeerd kan worden dat de eerste lijn momenteel niet volledig conform het model is ingericht.

De functies van de tweede lijn in het model zijn wel ingevuld. Vanwege de schaal van de gemeente worden sommige functies gedeeld met andere gemeenten of gecombineerd. Zo functioneert de ICT-regisseur van Soest ook als ENSIA coördinator. Dit behoort formeel niet tot zijn takenpakket, maar is er informeel aan toegevoegd. De Privacy Officer is sinds een jaar vast in dienst bij de gemeente, de CISO is sinds kort als inhuurkracht werkzaam voor Soest. De CISO werkt voor alle (zes) bij de RID aangesloten organisaties. Deze CISO staat bovendien vanwege praktische redenen op de loonlijst van de RID. Dit gaat goed zolang alle bij de RID aangesloten organisaties dezelfde belangen hebben. Als dat niet het geval is dan kan het dienen van zes organisaties een probleem zijn voor de CISO.

Naast de ENSIA taken vervult de ICT regisseur een 'spin in het web' functie als het gaat om digitale veiligheid. Hij is in veel gevallen de contactpersoon tussen de functioneel beheerders in de lijnorganisatie en de RID.

De FG heeft geen onafhankelijke rol in de ambtelijke organisatie, maar valt, net als de PO onder de juridische afdeling van de gemeente. Dit kan afbreuk doen aan de kritische en onafhankelijke functie die de FG volgens de wet zou moeten hebben. De FG van Soest vervult in praktijk meer een beleidsrol dan de rol van onafhankelijke auditor zoals beschreven in het strategisch beleidsdocument. Dit heeft ook te maken met de inhaalslag die thans gemaakt wordt om de basis op orde te krijgen.

5.2.4 Bewustwording en opleiding informatieveiligheid

In het Strategisch Informatiebeveiliging beleid[11] is aangegeven dat:

- Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures.
- Alle medewerkers een minimale basiskennis hebben van de privacywetgeving en deze bewust weten toe te passen in hun dagelijks werk.

Het strategisch beleid is ten aanzien van opleiding en bewustwording in verschillende uitvoeringsplannen uitgewerkt. Het 'Actieplan digitaal werken' biedt ondersteuning voor medewerkers in het werken met digitale voorzieningen en geeft handvatten voor de verschillende tools. Dit

[10] Strategisch Gemeentelijk Informatiebeveiligingsbeleid gemeente Soest, p. 14
[11] Strategisch Gemeentelijk Informatiebeveiligingsbeleid gemeente Soest, p. 11

document is een uitwerking van de visie ‘Digitaal werken: zo doen we het in Soest’. In dit document komt de wens naar voren om de ambtelijke organisatie van Soest meer digitaal in verbinding te brengen. Dit valt onder een van de tien uitgangspunten, het volledig digitaal werken, zoals via het Zaaksysteem en afspraken rondom de opslag van documenten.

In het Actieplan digitaal werken wordt een aantal beoogde resultaten uiteengezet. Deze resultaten leggen de focus op de medewerkers, zodat zij beter digitaal kunnen werken, meer begrip hebben voor de ontwikkelingen en zich bewust zijn van informatieveiligheidsrisico’s. Om deze resultaten te behalen zijn er ook een aantal randvoorwaarden geformuleerd, die te maken hebben met draagvlak, voldoende tijd en ruimte en genoeg ondersteuning, capaciteit en budget. Daarnaast worden er kaders uiteengezet om de resultaten te behalen, zoals een aantal verplichte modules voor nieuwe medewerkers.

Naast dit actieplan is er nog een aantal documenten die bijdragen aan de bewustwording in de organisatie, zoals het Beheerplan i-Bewustzijn en het Privacy Officer stripboek. Deze documenten besteden aandacht aan de rollen, taken en verantwoordelijkheden in de informatiebeveiliging. De contactpersonen en aanspreekpunten worden zo duidelijk voor medewerkers in de organisatie. Uit interviews en gesprekken in de focusgroepen is gebleken dat medewerkers inderdaad op de hoogte zijn bij wie ze moeten zijn in het geval van een incident, DPIA of een vraag over informatieveiligheid.

In het onboarding programma voor nieuwe medewerkers komt digitale veiligheid aan bod in de vorm van een aantal verplichte modules. Verder worden er (nog) geen trainingen aangeboden aan het zittend personeel om de bewustwording voor dit domein te vergroten of structureel te versterken.

Om na te gaan of medewerkers in de praktijk bewust omgaan met mogelijke verstoringen, voert de gemeente incidenteel *human factor pentesten* en *phishing mails* uit. Pentest staat voor ‘penetratie-test’; hierbij wordt getest of een onbevoegd persoon fysiek of digitaal toegang kan krijgen tot gemeentelijke informatiesystemen. Bij een phishing mail krijgen medewerkers een e-mailbericht, waarin om geld of (vertrouwelijke) informatie gevraagd wordt. De mail lijkt van een betrouwbare afzender te komen (een bank, zorginstelling of de burgemeester), maar is niet authentiek.

De uitgangspunten van het strategisch beleid worden deels nagevolgd. Alle nieuwe medewerkers krijgen een training over informatiebeveiliging, maar dit is enkel bij het indiensttreding. Zittende medewerkers volgen niet periodiek een verplichte opfriscursus[12]. Daarnaast wordt er via verschillende wegen informatie over privacy verstrekt aan medewerkers, al is dit allemaal vrijblijvend. De privacykennis wordt incidenteel bij medewerkers getoetst via phishing mails of human pentesten.

Vanwege de vertrouwelijkheid van de informatie kregen de onderzoekers aanvankelijk onvoldoende mogelijkheden om rapportages over deze pentesten en phishing mails in te zien. Uiteindelijk is een presentatie over de pentesten en phishing mails gedeeld. Hieruit bleek dat er verbeterpunten zijn ten aanzien van het I-bewustzijn. Zo zou 30% van de medewerkers op de link in de phishing mail hebben geklikt en 9% van de medewerkers informatie hebben achtergelaten. Ook ten aanzien van de fysieke toegang tot het gemeentehuis zijn belangrijke risico’s geconstateerd. Uit interviews bleek voorts dat activiteiten vaak eenmalig worden uitgevoerd, zonder dat er een plan aan ten grondslag ligt. Ook ten aanzien van pentesten en phising-mails wordt er niet volgens de PDCA cyclus gewerkt.

[12] Sinds oktober 2024 worden wekelijks digitale ‘nano-learnings’ naar alle medewerkers gestuurd om het bewustzijn en het kennisniveau te verhogen. Dit is gestart nadat dit onderzoek is afgerond; onduidelijk is of de nano-learnings verplicht zijn en of het lijnmanagement hierop stuurt.

5.2.5 Crisisoefening

De RID en deelnemende gemeenten hebben een crisisstructuurplan opgezet, zodat duidelijk is hoe er gehandeld moet worden in het geval van een cyberincident of -crisis.

De gemeente Soest heeft in de afgelopen jaren een tweetal cybercrisisoefeningen gedaan. De eerste in 2023 was enkel voor de gemeente Soest; de tweede in mei 2024 is in RID verband uitgevoerd. De cybercrisisoefening wordt niet structureel, maar incidenteel uitgevoerd; nieuwe oefeningen zijn nog niet gepland.

Tijdens de oefening in 2023 hebben de leden van het crisisteam ervaren welke risico's en gevolgen een cyberaanval heeft en hoe zij hier adequaat op kunnen reageren. De 'Terugkoppeling lerende oefening' beschrijft de casus en het verloop van de oefening. De oefening is uitgevoerd onder begeleiding van een extern adviesbureau. Na afloop van de oefening heeft dit bureau een aantal aanbevelingen gedaan. Deze hebben betrekking op de samenstelling van het crisisteam en de interne- en externe communicatie van de verstoringen. Er is niet vastgelegd wat er met deze aanbevelingen is gedaan. Wel is aangegeven dat deze aanbevelingen (mede) input zijn geweest voor de opzet van de crisisstructuur dien in RID verband is opgesteld en de daarop volgende oefening.

Op 24 mei 2024 is er een cybercrisismanagement scenariosessie geweest in RID verband. Uit deze sessie zijn de volgende aanbevelingen gekomen:

- De beschreven regionale crisisstructuur bij een cybercrisis sluit grotendeels aan en past hierdoor bij de behoefte en noodzaak tot regionale samenwerking met de RID. De opschalingscriteria waren echter nog niet volledig helder en vergen meer structuur;
- Tijdens de planvorming is er een discrepantie in mandaten tussen de beschreven crisisstructuur en de reguliere afspraken rondom mandaatregeling RID Utrecht;
- De wijze waarop informatie over onder meer aard, omvang, duur en (mogelijke) impact gedeeld wordt voorafgaand en gedurende een cybercrisis dient nader te worden uitgewerkt;
- Om de crisisstructuur werkend te krijgen om zo adequaat op een cybercrisis te reageren, dienen enkele cruciale randvoorwaarden te worden ingevuld. Dit betreft de capaciteit bij een cybercrisis, het omgaan met (de gevolgen van) ransomware en crisiscommunicatie en woordvoering.

Daarnaast is het belang van het periodiek oefenen met de crisisorganisatie en het periodiek toetsen van gemaakte afspraken benoemd tijdens de sessie.

Uit de evaluatie van de cyberoefeningen komt naar voren dat het document 'Crisisstructuur cyberincident RID gemeenten' nog onvoldoende doorleefd wordt door alle stakeholders en verdere aanscherping nodig heeft. Het is goed dat de gemeente Soest een eerste aanzet heeft gedaan om te oefenen op een mogelijke cybercrisis.

5.3 Beantwoording van de onderzoeksvragen

Aan het einde van dit hoofdstuk kunnen wij de meeste onderzoeksvragen beantwoorden. Hieronder volgen de vragen met antwoorden in dezelfde volgorde als beschreven in paragraaf 1.2. Het restant van de onderzoeksvragen wordt beantwoord aan het einde van het volgende hoofdstuk.

Wat doet de gemeente aan het tegengaan van een cyberaanval en doet de gemeente dat beter, gelijk aan of slechter dan andere gemeenten?

De gemeente Soest heeft verschillende maatregelen genomen om een cyberaanval tegen te gaan. Deze maatregelen zijn conform de BIO te categoriseren in Technische maatregelen, Mensgerichte maatregelen, Organisatorische maatregelen en Fysieke maatregelen. Uit een zelfevaluatie die is uitgevoerd in 2023 blijkt dat de gemeente niet voldoet aan de basisnormen. Op het moment van onderzoek wordt er wederom een zelfevaluatie op basis van de BIO uitgevoerd. Deze zelfevaluatie wordt als 0-meting gebruikt voor het verbeteren van de digitale veiligheid van de gemeentelijke organisatie.
Er zijn geen cijfers beschikbaar over de prestaties van de gemeente Soest in relatie tot andere gemeenten. Wel blijkt uit onderzoeken dat de meerderheid van de gemeenten niet voldoet aan de BIO.

Hoe wordt het informatieveiligheidsbeleid uitgevoerd en zijn daar hiaten in te constateren, beoordeeld aan de hand van actuele maatstaven?

De gemeente Soest heeft strategisch beleid vastgesteld in het document ‘Strategisch informatiebeveiling- en privacybeleid’. Het beleid wordt niet conform dit document uitgevoerd. De belangrijkste hiaten betreffen het gebrek aan borging omdat er niet volgens de PDCA cyclus wordt gewerkt. Voorts is het strategisch beleid niet uitgewerkt in jaarplannen en ontbreekt de eerste lijn in het ‘three lines’ beveiligingsmodel. In de organisatie is men zich ervan bewust dat de cyberbeveiligingswet extra eisen stelt aan de gemeentelijke informatiebeveiliging. De gemeente moet zich in een periode van twee jaar van volwassenheidsniveau 1 naar volwassenheidsniveau 4 ontwikkelen. Hiervoor zijn nog geen concrete plannen opgesteld.

Wat is protocollair vastgelegd over de informatieveiligheid, voldoet dat aan de huidige maatstaven en is het toereikend?

Soest heeft protocollen voor het melden en afhandelen van datalekken alsmede een protocol voor een crisisorganisatie in geval van digitale verstoringen. De laatste is opgesteld in samenwerking met de RID. De datalekprotocollen voldoen aan de maatstaven en zijn toereikend. Bij de volgende vraag wordt nader ingegaan op het protocol ten aanzien van de crisisorganisatie.

Heeft Soest een crisisprotocol dat voorziet in handelingsperspectief, crisisorganisatie en (gemandateerde) beslissingsbevoegdheden aan bijvoorbeeld college of directeur RID in het geval van een (gedeeltelijk) geslaagde cyberaanval? In hoeverre zijn deze protocollen, mandaten en draaiboeken geïmplementeerd en toereikend gezien de actuele maatstaven?

De gemeente Soest en de RID hebben samen een crisisstructuurplan opgezet. Hierin zijn verschillende scenario’s voor digitale verstoringen uitgewerkt met bijbehorende crisisorganisatie. Er is de afgelopen jaren incidenteel geoefend met deze crisisorganisatie. Uit deze oefeningen zijn verbeterpunten naar voren gekomen, maar deze zijn niet aantoonbaar opgevolgd.

In hoeverre is de gemeentelijke organisatie voldoende wendbaar en adaptief om zich snel genoeg aan te kunnen passen aan nieuwe dreigingen? Welk lerend vermogen is er op dat gebied en in hoeverre is het beleid hierin ondersteunend?

Tot nu toe heeft zich in de gemeente Soest geen omvangrijke digitale verstoring voorgedaan. Dat betekent dat de wendbaarheid en het adaptief vermogen moet blijken uit crisisoefeningen. In het fysiek domein vinden deze oefeningen regelmatig plaats, maar op het gebied van digitale veiligheid wordt er incidenteel geoefend. Het beleid is niet ondersteunend; het strategisch informatiebeleid bevat geen richtlijnen voor een crisissituatie.

6. Informatiebeveiliging in de praktijk

In het onderzoek hebben wij, naast een documentstudie en interviews twee focusgroepen gesproken en een raadsbijeenkomst georganiseerd om te horen hoe men in de praktijk omgaat met digitale veiligheid. Voor de focusgroepen zijn de leidinggevenden van het Sociaal – en het Fysiek Domein gevraagd om 8 – 10 van hun medewerkers af te vaardigen voor een bijeenkomst van anderhalf uur in de raadszaal van het gemeentehuis. De focusgroep Sociaal Domein heeft daadwerkelijk plaatsgevonden; er waren 10 medewerkers aanwezig. Voor de tweede focusgroep meldde zich maar één medewerker. Met deze medewerker is een individueel gesprek gevoerd. Wij hebben dus een beperkt beeld van de mate waarin digitale veiligheid in de lijn is belegd en kunnen geen uitspraken doen over de hele organisatie.

Bij de raadsbijeenkomst was wel een goede afspiegeling van de raad aanwezig; 8 van de 10 fracties waren vertegenwoordigd. Met de aanwezige raadsleden hebben wij besproken op welke wijze zij thans betrokken zijn en hoe zij betrokken willen worden bij het thema digitale veiligheid. Het verslag van bovengenoemde activiteiten treft u hieronder aan.

6.1 De focusgroep Sociaal Domein

Uit de focusgroep Sociaal Domein bleek dat *alle* medewerkers oog hebben voor de omgang met privacygevoelige informatie de inwoners van Soest. Deze informatie wordt uitsluitend via beveiligde kanalen gedeeld met derden (als bijvoorbeeld zorginstellingen en scholen), ook al gaat dit ten koste van de gebruikersvriendelijkheid. Medewerkers maken gebruik van tweefactor authenticatie waar nodig en houden wachtwoorden geheim. Ook zijn zij alert op het vergrendelen van computers als zij even weg moeten, zodat onbevoegden geen toegang hebben tot vertrouwelijke informatie. Ondersteuning door het ‘e-team’ bij het gebruik van technische middelen was in het verleden beter georganiseerd en wordt nu gemist door de medewerkers.

Waar gehakt wordt vallen spaanders; een enkele medewerker gaf aan weleens een datalek te hebben veroorzaakt. Dit betreft veelal het verkeerd adresseren van een (digitale) brief. Betreffende medewerkers weten de FG en/of PO in dit soort gevallen te vinden en maken daar melding van de datalek. De FG of PO maken daar vervolgens weer (voorlopig) melding van bij de Autoriteit Persoonsgegevens (AP). Vanwege personele wisselingen is lang niet bij alle medewerkers duidelijk wie nu de FG is en waar ze hun melding moeten doen.

Medewerkers gaven aan dat digitale veiligheid geen onderwerp van gesprek is in team- of afdelingsoverleggen. Ook in functionerings- of beoordelingsgesprekken is digitale veiligheid geen onderwerp van gesprek. Uit gevoerde gesprekken blijkt dat het management een afwachtende houding heeft ten aanzien van het onderwerp. Medewerkers geven aan dat ze voor informatie afhankelijk zijn van berichten die op het intranet geplaatst worden. Maar in de drukte van alledag worden deze berichten weinig gelezen. Als er dan toch wat tijd is, dan is het bericht alweer uit het startscherm verdwenen en wordt het vaak vergeten.

Het voeren van het goede gesprek over digitale veiligheid wordt gemist door de medewerkers uit de focusgroep. Door voorbeelden of casuïstiek te bespreken zou het onderwerp veel meer gaan leven en wordt ook een handelingsperspectief gecreëerd. Nu ontbreekt dat en daardoor is ook maar beperkt zicht op de risico’s en hoe hiermee om te gaan. Eén van de medewerkers gaf aan het stripboek over

privacy min of meer toevallig gelezen te hebben. Juist het gesprek over de betekenis hiervan voor de dagelijkse praktijk zou meerwaarde hebben gehad.

Wel geven medewerkers aan dat zij incidenteel een mail krijgen of een bericht op het intranet over digitale veiligheid voorbij zien komen. Hier wordt over het algemeen weinig aandacht aan besteed. Dat komt niet alleen door drukte, maar ook omdat teksten, vanwege technisch of juridisch jargon, lastig leesbaar zijn.

6.2 Over de raadsbijeenkomst

Na een korte introductie over de status van het rekenkameronderzoek, zijn de aanwezige raadsleden in kleine groepjes uiteen gegaan om een casus te bespreken. Deze casus speelde zich af in een fictieve gemeente die vergelijkbaar was met Soest. Na deze casus hebben we plenair het gesprek gevoerd over de wijze waarop de raad de controlerende en kaderstellende rol ten aanzien van digitale veiligheid vervult. Ook is er gesproken over mogelijke verbeteringen van de invulling van deze rol.

Raadsleden hebben een wisselend kennisniveau als het gaat om digitalisering en digitale veiligheid. Een aantal raadsleden is goed geïnformeerd, zij werken in de IT sector en uitten aanvankelijk de wens om gedetailleerde informatie te ontvangen over applicaties en het risicobeheer daarvan. Het merendeel van de aanwezige raadsleden vond dit geen goed idee. Zij beschikten over weinig tot geen inhoudelijke IT kennis en waren van mening dat je als raadslid niet op de stoel van de ambtenaar of wethouder moest gaan zitten. Wel waren zij van mening dat de raad op dit moment onvoldoende in stelling werd gebracht op het thema digitale veiligheid. Als er een raadsbesluit gevraagd werd, had men niet het idee dat er een keuze voorlag. Als er een extra investering wordt gevraagd, kan je alleen maar ja zeggen omdat je de consequenties niet kan overzien, zo gaven meerdere raadsleden aan.

Een van de aanwezigen gaf aan dat hij als contactpersoon vanuit de raad betrokken was bij de RID. Nu de samenwerking met de RID op een nieuwe leest geschoeid werd, was er ook een wens om de raden van de aangesloten gemeenten beter te betrekken. Het raadslid stond positief tegenover deze ontwikkeling, maar gaf aan dat informatie hem te laat bereikte om zijn rol als contactpersoon goed in te vullen.

Over de frequentie waarmee de raad geïnformeerd zou moeten worden, is enige tijd doorgesproken. Uiteindelijk zou één tot twee keer per jaar voldoende moeten zijn, zo dacht het merendeel van de raadsleden. Wel moest dan de informatie in begrijpelijke taal gepresenteerd worden, zodat de raad in voorkomende gevallen beter gefundeerde besluiten zou kunnen nemen.

Er is ook gesproken over de inhoud van de raadsinformatie. Raadsleden gaven aan dat meer gemeenteraden in het land tegen dit vraagstuk aan moesten lopen. Zij vroegen zich af of er geen normenkader bestond dat dienst kon doen als stuurinformatie. In dit verband kwam de BIO en de ontwikkeling van de BIO2 als verplichte norm ter sprake. Raadsleden wisten niet of en in welke mate de gemeente Soest aan de BIO normen voldeed. Wel zagen zij in de BIO aanknopingspunten om besluitvorming in de raad te onderbouwen en raadsinformatie te verstrekken.

6.3 Beantwoording van de laatste onderzoeksvragen

Na deze beschrijving van de uitkomsten van de focusgroepen en de raadsbijeenkomst kunnen ook de laatste twee onderzoeksvragen beantwoord worden.

Wat is de rol van de gemeenteraad bij Informatieveiligheidsbeleid en zijn de verantwoordelijkheden tussen raad – college – ambtelijke organisatie – RID duidelijk vastgelegd, geïmplementeerd en effectief ingericht gezien actuele maatstaven?
De rol van de gemeenteraad van Soest bij het informatieveiligheidsbeleid is marginaal. De raad wordt via de P&C cyclus en raadsinformatiebrieven geïnformeerd, maar raadsleden vinden dat zij onvoldoende in stelling zijn gebracht om hun kaderstellende en controlerende rol te vervullen. Verantwoordelijkheden in de ambtelijke organisatie zijn onvoldoende vastgelegd; aangegeven wordt dat de gemeente beschikt over een kleine en informeel georganiseerd ambtelijke organisatie. Toch geven medewerkers aan dat direct betrokkenen bij het informatieveiligheidsbeleid onvoldoende zichtbaar zijn in de organisatie. De taakverdeling tussen het RID en de ambtelijke organisatie wordt duidelijk vastgelegd in een nieuwe Dienstverleningsovereenkomst (DVO) met onderliggende producten- en dienstencatalogus. Deze documenten moeten nog ondertekend worden namens de gemeente en de RID, maar zijn in concept gereed.
Wat is de cultuur in de gemeente ten aanzien van informatiebeveiliging en de digitale weerbaarheid van de gemeenten?
Er heerst een open cultuur waarin het maken van fouten niet wordt afgestraft. Ambtenaren weten voorbeeld wat ze moeten doen in het geval van een datalek. Informatiebeveiliging wordt in de beleids- en uitvoerende teams niet als kerntaak gezien. Digitalisering is er vooral ter ondersteuning van de primaire werkprocessen en beveiligingsmaatregelen worden vooral gezien als noodzakelijk kwaad, zeker als dit in de overvolle agenda om een tijdsinvestering vraagt.

Bijlage A Geïnterviewde personen

Functie	Organisatie
Wethouder ICT & informatiebeleid	Gemeente Soest
Strategisch adviseur informatiebeleid	Gemeente Soest
ICT-regisseur	Gemeente Soest
CISO	Gemeente Soest
TISO	RID
Teamleder advies en dienstverlening	Gemeente Soest
Privacy Officer	Gemeente Soest
Functionaris Gegevensbescherming	Gemeente Soest
Teammanager Diensten	RID
Gemeentesecretaris	Gemeente Soest
Manager bedrijfsvoering	Gemeente Soest

Daarnaast is gesproken met verschillende medewerkers uit het sociaal en fysiek domein.

Bijlage B Bestudeerde documentatie

Documentnaam	Versie	Datum
Super PO	1.0	01-12-2023
Rapportage zelfevaluatie informatiebeveiliging 2023		2023
Actieplan digitaal werken		14-09-2022
Algemeen privacybeleid	3.0	08-04-2024
Beleid rechten van betrokkenen	1.0	28-12-2023
Crisisstructuur cyberincidenten	0.4	13-05-2024
DPIA bodycams	1.0	07-05-2021
DPIA raamwerk	1.1	25-02-2022
DPIA vroegsignalering schulden	3.0	28-05-2021
DPIA i-Navigator	1.01	15-11-2021
ENSIA rapportage 2023	1.0	18-14-2024
Terugkoppeling Cybercrisisoefening	1.0	
Strategisch Informatiebeveiliging- en privacybeleid	0.1	17-04-2024
ICT-crisiscommunicatieplan	1.0	
Organogram gemeente Soest		01-2023
Procedure melden van datalekken		13-05-2024
Procedure meldplicht datalekken & informatiebeveiligingsincidenten		08-12-2021
Processtappen voor het opstellen van een verwerkersovereenkomst		
SOO	1.0	
Beheerplan i-Bewustzijn	1.0	
Sturen op weerbaarheid		
Uitvoeren van uitwijktest voor BRP & Suite		12-10-2023
Verslag uitwijktest Key2Burgerzaken en Suite voor Sociaal Domein		21-10-2023

Bijlage C Stoplichtrapportage normenkader

Nummer	Norm	Kleur stoplicht
Normen ten aanzien van het gemeentelijk beleid		
1	De gemeente heeft informatiebeveiligingsbeleid dat voldoet aan de norm ‘Baseline Informatieveiligheid Overheid (BIO)’	
2	De algemene uitgangspunten en kaders zijn besproken in en vastgelegd door de gemeenteraad	
3	In het beleid wordt o.a. ingegaan op: • Strategische uitgangspunten • Risicomanagement • Governance (waaronder rollen en verantwoordelijkheden) • De PDCA-cyclus van de gemeente	
4	In (voortgangs)rapportages wordt ingegaan op informatiebeveiliging	
5	In programma’s en projecten wordt expliciet aandacht besteed aan informatiebeveiliging	
6	Er is een procedure hoe wordt omgegaan met informatiebeveiligingsincidenten (waaronder cyberaanvallen) en een crisisprotocol	

7	De gemeente heeft beleid voor informatiebeveiliging ten aanzien van samenwerkingspartners, gemeenschappelijke regelingen en leveranciers	
Normen ten aanzien van de Uitvoeringspraktijk		
8	In de praktijk wordt gehandeld conform de wijze waarop informatie wordt beveiligd, waaronder in de relevante werkprocessen, de toewijzing van verantwoordelijkheden, de inrichting van informatiesystemen, de autorisaties, de afspraken voor de verwerking van gegevens en de afspraken over het informeren van burgers en het vragen van toestemming	
9	De gemeente heeft een leer- en verbetercyclus (PDCA-cyclus).	
10	De gemeente heeft inzicht in de belangrijkste verbeterplannen en –maatregelen	
11	Er wordt in het geval van incidenten, calamiteiten en crisis volgens de vastgelegde procedures gehandeld	
12	De vastgelegde controles en rapportages worden in de praktijk uitgevoerd	

13	De gemeente test en toetst procedures regelmatig om de effectiviteit en werking te toetsen	
14	De gemeente houdt toezicht op de afspraken ten aanzien van informatiebeveiliging met (samenwerkings)partners, regelingen en leveranciers	
15	De raad wordt geïnformeerd op een manier die hem in staat stelt te sturen en te controleren	
Normen ten aanzien van de organisatiecultuur		
16	De medewerkers van de gemeente zijn bekend met het gemeentelijk beleid met betrekking tot informatiebeveiliging en worden van aanpassingen op de hoogte gehouden	
17	In hun dagelijks functioneren geven de medewerkers er blijk van het gemeentelijk informatiebeveiligingsbeleid na te leven	
18	de relatie met ketenpartners bewaken de medewerkers actief dat deze ketenpartners zich conformeren aan de regels, standaarden en procedures van de gemeente op het gebied van informatiebeveiliging	

Bijlage D Reactie college van B&W

Gemeente Soest

Rekenkamercommissie Soest
Arco de Baat
Postbus 2000
3760 CA Soest

Soest, 11 februari 2025 Verzonden: 12 februari 2025

Behandeld door : Marloes Klooster
Zaaknummer : 1059499
Onderwerp : Rekenkameronderzoek Informatieveiligheid

Beste Arco de Baat,

Op 17 januari 2025 heeft u ons de resultaten van uw onderzoek naar het Informatiebeveiligingsbeleid van de gemeente Soest gestuurd. In uw brief vraagt u ons in het kader van bestuurlijk hoor en wederhoor om een inhoudelijke reactie op de conclusies en aanbevelingen in uw rapport. In deze brief leest u onze reactie op uw rapport.

Voordat wij inhoudelijk op uw rapport reageren willen wij onze oprechte waardering uitspreken voor de inspanningen van de Rekenkamer. Uw bevindingen en aanbevelingen hebben wij dan ook aandachtig gelezen.

Zoals u ook in het onderzoeksrapport aangeeft, heeft uw onderzoek plaatsgevonden in een periode waarin wij diverse stappen aan het nemen waren om in te spelen op de huidige ontwikkelingen. Na oktober 2024 is de inzet van de ambtelijke organisatie verder voortgezet. Wij nemen uw conclusies en aanbevelingen mee in het licht van continu verbeteren van onze kennis, kunde en organisatie van dit thema.

Reactie op conclusies en aanbevelingen

In het onderzoeksrapport worden een aantal conclusies getrokken. Deze conclusies herkennen wij grotendeels. Voor een deel vragen deze conclusies wat nuancering. Het strategisch beleidsplan hebben wij in het najaar 2024 vastgesteld. De uitwerking en uitvoering hiervan wordt op dit moment door de organisatie verder opgepakt. Binnenkort ontvangen wij ook de definitieve uitkomsten van de BIO-nulmeting. De uitkomsten van dit onderzoek en de BIO-nulmeting vormen voor de organisatie handvatten om vervolgacties te nemen, zodat de informatieveiligheid verder verbeterd kan worden. We groeien toe naar volwassenheidsniveau 4.

In het onderzoeksrapport wordt ook ingegaan op de bewustwording van informatieveiligheid bij onze medewerkers. De afgelopen periode is hier invulling aan gegeven. Dit doen we op verschillende manieren. Zo ontvangen alle medewerkers wekelijks een vraag over informatieveiligheid. Middels monitoring wordt de deelname en kennisniveau gemonitord en

Telefoon: 035-6093411
Bezoekadres: Raadhuisplein 1, Soest
Internet: www.soest.nl
Postadres: Postbus 2000, 3760 CA Soest

waar nodig bijgestuurd. Ook volgen alle nieuwe medewerkers trainingen en dit jaar krijgt ook al het zittende personeel een (herhaal)training. Op deze manier proberen we medewerkers bewust te laten zijn van de risico's die wij lopen op het gebied van informatieveiligheid en hen bekend te laten zijn met de stappen die ze moeten nemen op het moment dat er sprake is bijvoorbeeld een datalek of phishingmail.

Onderstaand geven wij een beknopte reactie op uw aanbevelingen.

1. *Investeer in een robuuste digitale veiligheidsorganisatie*

Zoals aangegeven, gaan de ontwikkelingen op het gebied van informatieveiligheid snel. De komende periode geven we nader invulling aan ons strategisch beleid, waarin ook de rol en taken van het lijnmanagement nader zijn uitgewerkt. In de aanbevelingen wordt aangegeven dat er geïnvesteerd moet worden in de tweede en derde lijn van het 'three lines'model, waaronder de functies van CISO, FG en PO, om de benodigde inhaalslag te maken. We zijn aan het onderzoeken op welke wijze deze bestaande functies het beste ingevuld kunnen worden. Hierbij werken we ook samen in de regio, met de RID deelnemers. Gezamenlijk wordt kennis uitgewisseld en worden instrumenten ontwikkeld.

2. *Stel op basis van het strategisch beleid een 'aanvalsplan' Digitale Veiligheid op dat erop gericht is om aan de wettelijke verplichtingen te voldoen*

In het onderzoeksrapport wordt de aanbeveling gedaan om voor 2025 een aanvalsplan Digitale Veiligheid op te stellen. Zoals hiervoor aangegeven gaan we aan de slag met de vertaling van het strategische beleid en de uitkomsten van de BIO-nulmeting om vervolgstappen te nemen. Doel van deze vervolgacties is om door te groeien naar volwassenheidsniveau 4. We stellen voor de raad via de P&C cyclus, in de paragraaf Bedrijfsvoering, te informeren over de voortgang en uitvoering.

3. *Ontwikkel in samenwerking met de raad een begrijpelijke rapportage gebaseerd op gangbare normenkaders, risico's en kosten*

In het rapport doet u de aanbeveling om een jaarlijkse rapportage op te stellen over de stand van zaken van de informatieveiligheid. Deze aanbeveling nemen wij graag over. We zullen in overleg met de agendacommissie van de raad een informatiebijeenkomst plannen.

Telefoon: 035-6093411
Bezoekadres: Raadhuisplein 1, Soest
Internet: www.soest.nl
Postadres: Postbus 2000, 3760 CA Soest

Pagina 3 van de brief met zaaknummer: 1059499

Heeft u nog vragen of opmerkingen over deze brief?

Dan kunt u terecht bij Marloes Klooster, manager bedrijfsvoering. Bellen kan op werkdagen tot 12.30 uur op 035-609 34 11. Mailen kan via het contactformulier op soest.nl/contact. Tip: noem uw zaaknummer. Dan kunnen wij u sneller helpen.

Met vriendelijke groet,

Burgemeester en wethouders

LV
11-02-2025
Leontine Vermond

Gemeentesecretaris

RM
11-02-2025
Rob Metz

Burgemeester

Internet: www.soest.nl
Postadres: Postbus 2000, 3760 CA Soest