Gemeente Raalte
Rekenkamercommissie

Digitale weerbaarheid in gemeente Raalte

Onderzoeksrapportage

Eindrapport (voor bestuurlijk wederhoor)
Mei 2023

Inhoudsopgave

Voorwoord

De Rekenkamercommissie heeft onderzoek verricht naar de digitale weerbaarheid in de gemeente Raalte. Aangezien Raalte samenwerkt op onderdelen van bedrijfsvoering met Deventer en Olst-Wijhe is ook die samenwerking tegen het licht gehouden.

De Rekenkamercommissie heeft voor het onderwerp digitale weerbaarheid in de gemeente Raalte gekozen gezien de actualiteit van dit vraagstuk. Gemeenten en andere organisaties in het publiek domein zijn (steeds) meer doelwit van cybercriminaliteit. Zo zijn recentelijk een aantal gemeenten, maar bijvoorbeeld ook de Universiteit van Maastricht, getroffen door gijzelsoftware. Dit kan organisaties veel geld kosten; de dienstverlening loopt gevaar, het is slecht voor het imago en het kan ten koste gaan van het vertrouwen van bijvoorbeeld inwoners in de organisatie. Er is organisaties daarom veel aan gelegen de informatieveiligheid in het algemeen, maar zeker voor persoonsgegevens, goed op orde te hebben. Dat is de reden dat we onderzoek hebben gedaan naar de bescherming en weerbaarheid van de digitale systemen van de gemeente Raalte en het beveiligings-bewustzijn van de medewerkers, om zo mogelijk cyberaanvallen buiten de deur te kunnen houden.

Bij de onderwerpkeuze hanteert de Rekenkamercommissie de volgende selectiecriteria:

- het onderwerp heeft een duidelijk maatschappelijk, politiek en/of financieel belang;
- er is sprake van een beredeneerde twijfel over het (al dan niet aanwezige) beleid;
- er is sprake van een risico: een gebrekkige uitvoering heeft relatief ernstige financiële of maatschappelijke gevolgen;
- de meerwaarde van een onderzoek door de Rekenkamercommissie moet duidelijk zijn;
- het onderwerp moet voor de Rekenkamercommissie haalbaar zijn en passen binnen haar financiële en organisatorische mogelijkheden.

Voor dit onderzoek is, voor het eerst, samengewerkt met onderzoeksbureau PBLQ. Vanuit PBLQ is het onderzoek uitgevoerd door de heer Peter Castenmiller en mevrouw Juliette Mies. Namens de Rekenkamercommissie heeft mevrouw Aljona Wertheim het onderzoek gecoördineerd.

Wij hopen met dit rapport de gemeenteraad, maar ook het college van B&W en de ambtelijke organisatie, waaronder DOWR, inzicht te geven in de digitale weerbaarheid van Raalte.

Tenslotte willen wij iedereen bedanken, die heeft meegewerkt aan dit rapport. Ambtenaren van Raalte, DOWR, de burgemeester en de raadsleden van de gemeente Raalte. Ook deze keer kregen we weer alle steun van de gemeente bij het aanleveren van documenten en het beantwoorden van vragen. Tot slot gaat onze dank ook uit naar de ondersteuning door de medewerkers van de griffie.

Mei 2023

Mevrouw O.P. Wertheim – Davygora	lid Rekenkamercommissie
De heer D. Hoek	lid Rekenkamercommissie
De heer A. Titsing	voorzitter Rekenkamercommissie

1. Inleiding

1.1 Aanleiding

Allerlei organisaties in het publieke domein, zoals gemeenten of onderwijsinstellingen, kunnen doelwit zijn van cybercriminaliteit. Een geslaagde cyberaanval kan zo'n organisatie veel geld kosten, de dienstverlening in gevaar brengen en ten koste gaan van het imago en het vertrouwen van burgers. Er is publieke organisaties daarom veel aan gelegen de informatiebeveiliging goed op orde te hebben.

Gemeenten hebben de bedrijfsvoering steeds verder gedigitaliseerd. Zij wisselen zowel intern als met andere organisaties en met burgers en ondernemingen digitaal veel gegevens uit. Omdat het daarbij vaak gaat om persoonsgegevens of andere gevoelige informatie, is het voor gemeenten van extra groot belang om de informatiebeveiliging goed op orde hebben.

Cybercriminelen worden steeds slimmer en hun techniek steeds geavanceerder. Er moet niet alleen rekening worden gehouden met het daadwerkelijk plaatsvinden en eventueel slagen van digitale aanvallen, in de praktijk gebeurt dat al. Omdat 100% veiligheid niet bestaat, heeft het de voorkeur om in een organisatie te kijken naar de digitale weerbaarheid. Een digitaal weerbare organisatie kan potentiële incidenten vroegtijdig signaleren, maar ook tijdig adequate maatregelen treffen om de gevolgen van een incident te beperken.

De Rekenkamercommissie van de gemeente Raalte heeft in 2022 onderzoek gedaan naar de digitale weerbaarheid. Dit betreft de mogelijkheden om cyberaanvallen tegen te kunnen gaan en om in geval van een daadwerkelijk incident adequaat te kunnen reageren.

1.2 Opdrachtformulering

Aan de basis van het onderzoek staat de volgende centrale onderzoeksvraag:

Centrale onderzoeksvraag
Hoe is het gesteld met de beveiliging van persoonsgegevens en andere informatie en de voorbereiding op incidenten in de gemeente Raalte?
Deze centrale onderzoeksvraag is uitgewerkt in de volgende deelvragen.
Deelvragen
1. Hoe weerbaar zijn de digitale systemen van de gemeente Raalte tegen cybercriminaliteit? 2. Hoe is de samenwerking van Raalte met Deventer en Olst-Wijhe van invloed op de informatiebeveiliging in de gemeente Raalte? 3. Hoe beveiligingsbewust zijn de medewerkers van de gemeente Raalte als het gaat om persoonsgegevens en andere informatie? 4. Hoe is de gemeente voorbereid in de respons op daadwerkelijke incidenten? 5. Waar liggen de grootste risico`s en hoe kan de gemeente Raalte hierin verbeteringen aanbrengen? **6.** Welke controle- en sturingsmogelijkheden heeft de gemeenteraad bij informatiebeveiliging en worden deze ook ingezet?

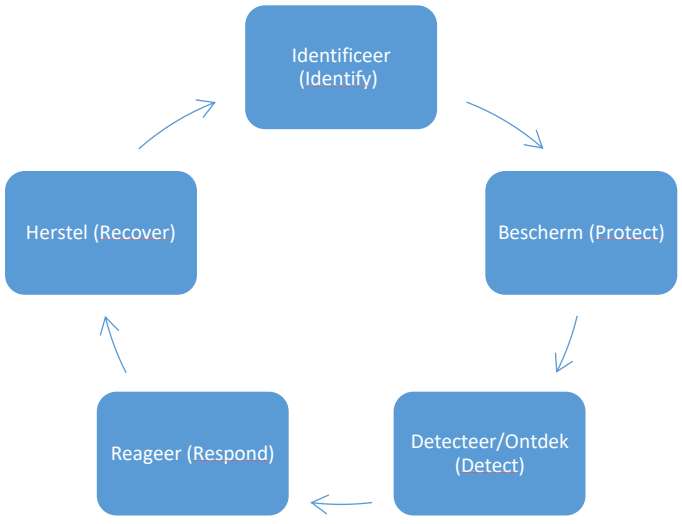
1.3 Normenkader

In onderzoeken van gemeentelijke rekenkamers is het gebruikelijk om vooraf een normenkader in te richten, dat als basis dient voor de beoordeling van de bevindingen. Het normenkader beschrijft de 'ideale situatie'. Door de bevindingen daaraan te relateren wordt duidelijk welke verschillen er zijn tussen de bevindingen in Raalte en de geschetste ideale situatie.

Het onderzoek concentreert zich op het inventariseren en beoordelen van de wijze waarop Raalte investeert in de beveiliging van de binnen de organisatie beschikbare informatie. Informatiebeveiliging betreft maatregelen en procedures om beschikbaarheid, integriteit en vertrouwelijkheid van informatie te garanderen en in het bijzonder om de continuïteit van de informatie en informatievoorziening te waarborgen en de gevolgen van incidenten tot een acceptabel niveau te beperken. De maatregelen die in het kader van informatiebeveiliging worden genomen zijn bedoeld om te beschermen tegen cybercriminaliteit, maar ook tegen andere bedreigingen zoals menselijke fouten of technisch falen. Tevens gaat bescherming tegen beveiligingsincidenten niet alleen over de betrouwbaarheid en beveiliging van de informatiesystemen van de gemeente en de (persoons-) gegevens die erin zijn opgeslagen. Digitale weerbaarheid gaat ook over de betrouwbaarheid en continuïteit van de belangrijkste processen van de gemeente, zoals de dienstverlening aan burgers, de interne bedrijfsvoering en het democratische proces.

In dit onderzoek wordt gekeken naar de bescherming van persoonsgegevens in de context van de algemene digitale weerbaarheid tegen cybercriminaliteit. Daarbij staan de verschillende activiteiten centraal die de gemeente moet uitvoeren om gegevens te beschermen, maar ook om adequaat te reageren bij grootschalige incidenten. Dit is een integrale insteek, juist omdat het niet alleen gaat om het detecteren en het voorkomen van mogelijke incidenten, maar ook over de respons van de gemeente Raalte als een incident zich voordoet en hoe je als organisatie daarvan leert.

In dit onderzoek is het NIST[1] Framework for Improving Critical Infrastructure Cybersecurity als basis voor het normenkader genomen. Het NIST-framework verschaft een kader waarmee de verschillende activiteiten ten behoeve van de weerbaarheid tegen cybercriminaliteit geanalyseerd kunnen worden.



[1] De afkorting NIST verwijst naar het National Institute of Standards and Technology; zie: https://www.nist.gov/about-nist

Door de kernactiviteiten uit het kader centraal te stellen, wordt inzicht verkregen in de voorbereiding van de gemeente op een incident, hoe het deze kan detecteren en hoe de gemeente erop kan reageren en ervan kan herstellen.

Het normenkader is als volgt uitgewerkt:

Normenkader
Identificeer (Identify)
• De gemeente heeft een duidelijk beleid en uitvoeringskader bij hoe zij omgaat met cybersecurity risico's van/aan systemen, mensen, gegevens, informatie en middelen. • De gemeente heeft de belangrijkste processen, systemen en risico's in beeld. • De gemeente stelt dit risicobeeld periodiek bij op basis van (onder andere) informatie over dreigingen en veranderingen in processen en systemen.
Bescherm (Protect)
• De gemeente heeft maatregelen ontwikkeld en geïmplementeerd om te zorgen voor de continuïteit en bescherming van kritische processen en dienstverlening. • Medewerkers werken volgens de maatregelen en zijn bewust van eigen handelen en verantwoordelijkheid.
Detecteer/ Ontdek (Detect)
• De gemeente heeft maatregelen ontwikkeld en geïmplementeerd om cybersecurity incidenten te detecteren. • Er is een procedure voor het melden van incidenten en medewerkers kennen en gebruiken deze procedure. • Er is een escalatieprocedure richting de directie, college en gemeenteraad.
Reageer (Respond)
• De gemeente heeft maatregelen/acties/processen geïmplementeerd om actie te (kunnen) ondernemen tegen/na potentiële cybersecurity incidenten. Het gaat bijvoorbeeld om een incidentrespons procedure en nood/continuïteitsplannen. • De gemeente toetst, oefent en evalueert deze maatregelen/acties/processen periodiek (zoals het oefenen van een cyberaanval). • De rollen en verantwoordelijkheden van functionarissen, directie en raad zijn vastgelegd en in de praktijk bekend.
Herstel (Recover)
• De gemeente werkt planmatig aan weerbaarheid en is voorbereid op activiteiten ten behoeve van herstellen van processen en dienstverlening. • Incidenten op het gebied van informatiebeveiliging of cybersecurity worden geëvalueerd en leiden tot structurele verbetermaatregelen.
Algemeen
• De raad wordt periodiek geïnformeerd over de digitale weerbaarheid van de gemeente en de ontwikkelingen op dat vlak. • De informatieverstrekking aan de raad biedt de raad voldoende mogelijkheden om de sturende en controlerende verantwoordelijkheden waar te maken. • De maatregelen, die de gemeente neemt, worden periodiek getoetst, geoefend en/of geëvalueerd.

De gemeenteraad heeft een belangrijke rol bij digitale weerbaarheid. Deze wordt expliciet meegenomen in dit onderzoek. Door het gemeentelijke beleid voor de bescherming van persoonsgegevens en andere informatie te toetsen op doeltreffendheid, doelmatigheid en rechtmatigheid, geeft de raad invulling aan haar controlerende rol. Vanuit de volksvertegenwoordigende rol is het voor de raad van belang de weerbaarheid tegen cybercriminaliteit te toetsen en daarbij het belang en perspectief van de inwoner mee te nemen en op basis hiervan eventueel nadere kaders te stellen.

1.4 Werkwijze

Het onderzoek is gestart met een documentanalyse waarin de belangrijkste beleidsdocumenten zijn bestudeerd. Om het ‘papieren beeld’ te verrijken hebben daarna interviews plaatsgevonden met sleutelfiguren, zoals de portefeuillehouder, gemeentesecretaris, CISO en andere betrokken medewerkers. Op basis van het verkregen beeld heeft de rekenkamercommissie twee casussen geselecteerd: publiekszaken en vergunningen. Aan de hand van casusbesprekingen is meer inzicht ontstaan over de uitvoering van het beleid in de praktijk. Na de casusbesprekingen heeft een convergentiesessie plaatsgevonden met een aantal sleutelfiguren, waarin bevindingen zijn getoetst en aangescherpt. De onderzoeksactiviteiten zijn in 2022 afgerond. De uit het onderzoek verkregen inzichten staan in voorliggende rapportage.

Bij het ambtelijk wederhoor bleek dat een aantal beleidsstukken inmiddels herzien waren. Waar deze herziening van beleid impact had op de bevindingen is dit zoveel mogelijk verwerkt in de rapportage.

1.5 Leeswijzer

In hoofdstuk twee van de rapportage worden de deelvragen en hoofdvraag beantwoord, conclusies uiteengezet en aanbevelingen gedaan. In hoofdstuk drie wordt het gemeentelijk informatiebeveiligingsbeleid uiteengezet, waarbij wordt ingegaan op de centrale beleidsdocumenten- en voornemens van de gemeente op het gebied van informatiebeveiliging. Het laatste hoofdstuk schetst hoe deze beleidsuitgangspunten in de praktijk door de gemeente worden uitgevoerd. Tevens wordt apart aandacht besteed aan de rol van de gemeenteraad.

In bijlage 3 is een lijst met afkortingen en begrippen beschikbaar.

2. Conclusies en aanbevelingen

2.1 Samenvatting van de bevindingen

De gemeente Raalte werkt intensief samen met de gemeenten Deventer en Olst-Wijhe (DOWR) op het gebied van bedrijfsvoering. De samenwerking tussen de gemeenten is van grote betekenis voor de inrichting en de dagelijkse praktijk van de informatiebeveiliging. De samenwerking, die overigens op meer thema's dan louter ICT plaatsvindt, is ingegeven door de ambitie om de slagkracht van de gemeenten te versterken en de kwetsbaarheid te verminderen. Over het algemeen bestaat er tevredenheid over deze samenwerking. Dat geldt zeker voor de samenwerking rond ICT. Uit de interviews blijkt dat dankzij de samenwerking de gemeenten de technische beveiliging relatief goed op orde hebben. Genoemd is dat de DOWR samenwerking met betrekking tot ICT in landelijke context wel als 'koploper' wordt getypeerd. Dankzij de samenwerking heeft DOWR financiële en personele schaalvoordelen waardoor bovengemiddelde technische waarborgen mogelijk zijn.[2]

In het verlengde daarvan bestaat binnen de organisatie van Raalte eveneens een positief beeld van de samenwerking op het gebied van informatiebeveiliging. Het beleid bestaat uit een visie, een strategisch informatiebeveiligingsbeleid, een meerjarige roadmap en diverse onderliggende beleidsstukken, waarin onder andere rollen en verantwoordelijkheden zijn vastgelegd. Richtlijnen en maatregelen zijn geconcretiseerd in diversie beleidsdocumenten en jaarplannen. Het jaarplan informatiebeveiliging en privacy wordt systematisch uitgewerkt.

Binnen de DOWR-samenwerking is er veel aandacht voor de 'technische borging' van het beleid. Zonder de samenwerking zou lang niet dezelfde kennis en slagkracht beschikbaar zijn.
Voor informatiebeveiliging wordt op verschillende manieren aandacht gevraagd in de organisatie. Een veel genoemde maatregel zijn de zogenoemde nano-leanings, een bewustwordingscampagne voor informatiebeveiliging en privacy. Uit de interviews blijkt dat de nano-learnings als effectief worden ervaren voor het beveiligingsbewustzijn. Er wordt gesteld dat informatiebeveiliging bij medewerkers in de haarvaten zit, maar dat het onder de aandacht brengen van het belang ervan wel een continu proces moet zijn. In dat verband zijn er soms twijfels geuit of het instrument van nano-learning 'sleets' dreigt te worden; medewerkers van de gemeente zouden het als een verplicht nummer kunnen gaan beschouwen. In het recente Privacy en Informatiebeveiligingsplan 2023 wordt dit risico onderkend. Het plan bevat het voornemen om de managers te vragen het belang van nano-learning in hun team of domein uit te dragen. Om het enthousiasme verder te versterken wordt voorgesteld om een wisselbeker voor het best deelnemende team of domein beschikbaar te stellen.

Uit de gesprekken blijkt dat de gemeente bij nieuwe processen en applicaties meestal risico-analyses uitvoert. Niet voor alle bestaande processen zijn deze analyses uitgevoerd. Kritische processen rondom persoonsgegevens zijn beter in beeld dan kritische processen rond informatiebeveiliging. Baselinetoetsen BIO (Baseline Informatiebeveiliging Overheid) met risicoafwegingen van de processen en een compleet risico-overzicht van processen en systemen, zijn in het onderzoek niet geconstateerd. Vanuit privacy oogpunt wordt de achterstand aan uitvoering van de (uit AVG oogpunt) wettelijk verplichte risico-analyses ervaren als een risico.[3]

Ondanks de technische maatregelen kunnen incidenten voorkomen. De gemeente heeft diverse processen in het geval van incidenten. Voor het reageren in het geval van grote incidenten heeft de gemeente een business continuityplan uitgewerkt, waarbij de samenwerkende gemeenten elkaar als uitvalsbasis kunnen inzetten. De uitwijkmogelijkheid wordt jaarlijks getest en ook het herstellen van

[2] Zoals in hoofdstuk 3 al genoemd blijkt dit onder meer uit de ICT-benchmark gemeenten 2022.
[3] In het Toezichtjaarverslag informatieveiligheid en privacy 2022 van de FG en CISO van de gemeenten Deventer, Olst-Wijhe en Raalte wordt het ontbreken van volledige risicoanalyses eveneens als aandachtspunt genoemd. In het Privacy en Informatiebeveiligingsplan 2023 wordt aan deze constatering gerefereerd en aangegeven daar in 2023 versterkte aandacht aan te besteden.

back-ups wordt een paar keer per jaar getest. Er wordt daarnaast gewerkt aan een Cybercrisisplan in DOWR-verband. In 2013 vinden er ook trainingen en oefeningen plaats in dit kader, inclusief (crisis)oefeningen op het thema informatiebeveiliging. In het geval van incidenten wordt er naderhand ook geëvalueerd.

2.2 Beoordeling normenkader

In onderstaand overzicht wordt het voor het onderzoek opgestelde normenkader toegepast op de bevindingen. Dit geeft het volgende resultaat:

Normenkader	Beoordeling
Identificeer (Identify)	
De gemeente heeft een duidelijk beleid en uitvoeringskader bij hoe zij omgaat met cybersecurity risico's van/aan systemen, mensen, gegevens, informatie en middelen.	Positief
De gemeente heeft de belangrijkste processen, systemen en risico's in beeld.	Neutraal
De gemeente stelt dit risicobeeld periodiek bij op basis van (onder andere) informatie over dreigingen en veranderingen in processen en systemen.	Positief
Bescherm (Protect)	
De gemeente heeft maatregelen ontwikkeld en geïmplementeerd om te zorgen voor de continuïteit en bescherming van kritische processen en dienstverlening.	Positief
Medewerkers werken volgens de maatregelen en zijn bewust van eigen handelen en verantwoordelijkheid.	Positief
Detecteer/ Ontdek (Detect)	
De gemeente heeft maatregelen ontwikkeld en geïmplementeerd om cybersecurity incidenten te detecteren.	Positief
Er is een procedure voor het melden van incidenten en medewerkers kennen en gebruiken deze procedure.	Positief
Er is een escalatieprocedure richting de directie, college en gemeenteraad.	Positief
Reageer (Respond)	
De gemeente heeft maatregelen/acties/processen geïmplementeerd om actie te (kunnen) ondernemen tegen/na potentiële cybersecurity incidenten. Het gaat bijvoorbeeld om een incidentrespons procedure en nood/continuïteitsplannen.	Positief
De gemeente toetst, oefent en evalueert deze maatregelen/acties/processen periodiek (zoals het oefenen van een cyberaanval).	Positief
De rollen en verantwoordelijkheden van functionarissen, directie en raad zijn vastgelegd en in de praktijk bekend.	Positief
Herstel (Recover)	
De gemeente werkt planmatig aan weerbaarheid en is voorbereid op activiteiten ten behoeve van herstellen van processen en dienstverlening.	Positief
Incidenten op het gebied van informatiebeveiliging of cybersecurity worden geëvalueerd en leiden tot structurele verbetermaatregelen.	Positief
Algemeen	
De raad wordt periodiek geïnformeerd over de digitale weerbaarheid van de gemeente en de ontwikkelingen op dat vlak.	Negatief
De informatieverstrekking aan de raad biedt de raad voldoende mogelijkheden om de sturende en controlerende verantwoordelijkheden waar te maken.	Negatief
De maatregelen, die de gemeente neemt, worden periodiek getoetst, geoefend en/of geëvalueerd.	Positief

Het beeld is overwegend positief. Deze positieve beoordeling is voornamelijk het gevolg van het gegeven dat binnen de DOWR-samenwerking zowel de technische randvoorwaarden als procedures en werkprocessen uitgebreid ingericht zijn. Wel zijn er tekortkomingen geconstateerd als het gaat om het structureel onderscheiden van mogelijke risico's en bedreigingen (het onderdeel Identify van het normenkader). Voorts kan op basis van het normenkader worden vastgesteld dat de

informatievoorziening aan de raad tekort schiet, waardoor het voor de raad lastig is om de sturende en controlerende verantwoordelijkheden waar te maken.

2.3 Conclusies

2.3.1 Beantwoording onderzoeksvragen

De tijdens het onderzoek opgedane inzichten en de beoordeling daarvan resulteren in de navolgende beantwoording van de onderzoeksvragen.

Onderzoeksvraag 1: Hoe weerbaar zijn de digitale systemen van de gemeente Raalte tegen cybercriminaliteit?
De gemeente Raalte werkt via de samenwerking DOWR aan het beheersen en verbeteren van de informatiebeveiliging. Daarbij maakt zij gebruik van diverse normenkaders, waaronder de BIO. De gemeente inventariseert jaarlijks waar zij nog niet voldoet en via jaarplannen wordt gewerkt aan verbeteringen om maatregelen te inventariseren. De gemeente (en DOWR) beschikt over een veelvoud aan technische maatregelen en beveiligingsactiviteiten om de informatie en systemen te beschermen. Op een deel van de processen zijn risico-analyses uitgevoerd. Al deze maatregelen maken de digitale systemen van Raalte (ruim) voldoende weerbaar.

Onderzoeksvraag 2: Hoe is de samenwerking van Raalte met Deventer en Olst-Wijhe van invloed op de informatiebeveiliging in de gemeente Raalte?
Door de samenwerking van Raalte met Deventer en Olst-Wijhe heeft DOWR financiële en personele schaalvoordelen waardoor uitgebreide technische waarborgen mogelijk zijn. Binnen de samenwerking wordt aangestuurd op standaardisatie, maar de gemeente is niet verplicht zich te conformeren indien dat niet passend wordt bevonden. DOWR geeft grotendeels uitvoering aan informatiebeveiliging via technische maatregelen, waardoor deze buiten de eerste lijn zijn geplaatst. Via de informatiemanager van Raalte wordt de verbinding tussen de eerste lijn (het management Raalte) en tweede lijn (DOWR) gehouden.

Onderzoeksvraag 3: Hoe beveiligingsbewust zijn de medewerkers van de gemeente Raalte als het gaat om persoonsgegevens en andere informatie?
Via nano-learnings worden medewerkers van de gemeente Raalte eens per drie weken gewezen op (een thema binnen) informatieveiligheid. Dit lijkt goed te werken want in het onderzoek zijn de learnings meermaals aan de orde gekomen. Uit de casusbesprekingen blijkt dat ook medewerkers zich goed bewust zijn van het belang van informatieveiligheid, technische maatregelen en hun eigen handelen. Wel dient er voor gewaakt te worden dat de nano-learnings voldoende effectiviteit behouden.

Onderzoeksvraag 4: Hoe is de gemeente voorbereid in de respons op daadwerkelijke incidenten?
Vanuit de DOWR-samenwerking heeft de gemeente diverse processen ingericht waar zij op terug kan vallen bij incidenten. Er is onder andere een security-incident-response-proces en een business-continuityplan. Daarnaast wordt gewerkt aan een cybercrisisplan. Er wordt jaarlijks geoefend met uitwijkmogelijkheden en er wordt regelmatig getest met het herstellen van back-ups.

Onderzoeksvraag 5: Waar liggen de grootste risico`s en hoe kan de gemeente Raalte hierin verbeteringen aanbrengen?
De gemeente (en DOWR) brengt op verschillende manieren risico's in kaart. Dit gebeurt onder andere op basis van de jaarlijkse BIO gap-analyse, informatie van de Informatiebeveiligingsdienst en het Vulnerabilty management en op basis van risico-analyses bij nieuwe processen. Echter, keuzes en afwegingen of informatie in nieuwe en bestaande processen adequaat is beveiligd in termen van beschikbaarheid, integriteit en vertrouwelijkheid zijn niet voor alle processen inzichtelijk. De gemeente heeft daarmee nog geen sluitend risicomanagement-proces, waarin processen en informatiesystemen beveiligd worden op basis van de risico's die de gemeente (wil) lopen.

Onderzoeksvraag 6: Welke controle- en sturingsmogelijkheden heeft de gemeenteraad bij informatiebeveiliging en worden deze ook ingezet?
Het jaarlijkse verslag met de collegeverklaring ENSIA over informatiebeveiliging is het belangrijkste controle- en sturingsinstrument van de gemeenteraad. Hier zijn door raadsleden nauwelijks vragen over gesteld. Alleen als er incidenten zijn, worden raadsleden alert en zijn ze wel geneigd om vragen te stellen. Zoals geconstateerd in dit onderzoek is er zelden sprake van incidenten. In het kader van het inwerkprogramma van de in 2022 nieuw gekozen raad heeft er medio november 2022 een uitgebreide bijeenkomst over informatieveiligheid plaatsgevonden. Gezien de context en inrichting van deze bijeenkomst heeft ook nu de raad zich primair laten informeren. Verschillende raadsleden hebben aanvullende en verduidelijkende vragen gesteld. Tot een gedachtewisseling over de uitgangspunten die bij informatieveiligheid worden gehanteerd en de consequenties daarvan voor onderwerpen als de dienstverlening door de gemeente en de effectiviteit van de organisatie is het niet gekomen.

2.2.2 Hoofdconclusie

Bij aanvang van het onderzoek is een centrale probleemstelling geformuleerd. Na beantwoording van de onderzoeksvragen kan nu ook deze probleemstelling in deze paragraaf worden geadresseerd. Deze probleemstelling is de volgende:

Hoe is het gesteld met de beveiliging van persoonsgegevens en andere informatie en de voorbereiding op incidenten in de gemeente Raalte?

Raalte heeft mede dankzij de samenwerking binnen DOWR de informatiebeveiliging goed op orde. Door de samenwerking zijn er overwegend voldoende expertise en (financiële) capaciteit om te werken aan de weerbaarheid van gemeente Raalte, tegen alleszins aanvaardbare investeringen. Dit uit zich in een gedegen strategisch beleid, dat neerslaat in onderliggend beleid, diverse procedures en jaarplannen en een breed scala aan beveiligingsmaatregelen. Er wordt aandacht besteed aan het menselijk handelen. Dat wordt gezien als van groot belang voor de weerbaarheid.

Er is sprake van een nadruk op technische maatregelen bij het realiseren van informatiebeveiliging. Een verklaring hiervoor is dat een groot deel van de uitvoering bij de DOWR organisatie ligt, waar met name de technische maatregelen en overkoepelende processen worden ingericht. Alle medewerkers onderschrijven het belang van een goede informatiebeveiliging en handelen daarnaar. Door sommige medewerkers worden de technische maatregelen en de vastgelegde procedures wel als knellend voor hun dagelijkse werkzaamheden ervaren.

Voor de gemeentelijke uitvoering lijkt structureel inzicht en overzicht te ontbreken op risico's binnen processen en de systemen waar zij gebruik van maken. Daardoor kan op DOWR-niveau geen compleet beeld hiervan ontstaan. Dat betekent dat processen en informatiesystemen niet integraal beveiligd worden op basis van de risico's die de gemeente (wil) lopen. Het management maakt op voorhand niet structureel keuzes en afwegingen of informatie in nieuwe en bestaande processen adequaat beveiligd is in termen van beschikbaarheid, integriteit en vertrouwelijkheid. Een sluitend risico-managementsysteem helpt een manager en portefeuillehouder bij het maken van keuzes. Deze keuzes

en afwegingen kunnen vervolgens dienen als verantwoording naar de gemeenteraad. De gemeenteraad wordt nu onvoldoende geïnformeerd en in staat gesteld te controleren.

2.3 Aanbevelingen

Uit de beantwoording van de onderzoeksvragen en de daaruit volgende conclusies leidt de Rekenkamercommissie de volgende aanbevelingen voor het College van B&W af:

1. Breng het risicomanagement op orde. Voer ontbrekende risico-analyses op systemen en processen uit en maak een expliciete risico-afweging, waarbij wordt aangegeven welke risico's de gemeente bereid is te accepteren. Maak hiervoor een plan, stel voldoende capaciteit beschikbaar en geef het uitvoeren van risico-analyses prioriteit.

2. Integreer het risicomanagement met het Information Security Management Systeem dat vanuit de BIO al wordt verplicht. Risicomanagement wordt daarmee expliciet onderdeel wordt van de PDCA-cyclus, zodat niet alleen bij nieuwe systemen en processen een afweging wordt gemaakt, maar ook bij veranderingen.

3. Maak geregeld een onderbouwde afweging van de verhouding tussen ingezette technische maatregelen ter bevordering van informatiebeveiliging en de consequenties daarvan voor het gebruikersgemak. Besteedt daarbij aandacht aan de praktische vertaling naar de processen en de werkvloer. Het gaat hier niet alleen om de inhoudelijke boodschap, maar ook om de gebruikte taal.

4. Informeer de gemeenteraad periodiek over de digitale weerbaarheid van de gemeente en de ontwikkelingen en bedreigingen. Deel bijvoorbeeld een (half)jaarlijkse rapportage, met een samenvatting van openstaande punten uit de gapanalyse BIO, de voortgang op de jaarplannen en statistieken omtrent eventuele incidenten en datalekken.

5. De raad informeren draagt bij aan het geven van voldoende mogelijkheden om de sturende en controlerende verantwoordelijkheden waar te maken. Informeer de raad wanneer risico's worden geaccepteerd of laat de raad meepraten over het risicobeeld en een afweging maken omtrent de impact van mogelijke dreigingen.

Informatiebeveiliging wordt vaak gezien als een uitvoeringskwestie. Een dergelijke benadering doet onvoldoende recht aan het belang van het thema. Een ontoereikende beveiliging kan om te beginnen consequenties hebben voor kerntaken van de gemeente zoals de dienstverlening. Inbreuken in de veiligheid kunnen ook de privacy van burgers aantasten. Uiteindelijk kan het vertrouwen in de overheid worden beschadigd. Daarmee heeft ook de gemeenteraad een belangrijke verantwoordelijkheid in het bevorderen en bewaken van de randvoorwaarden voor goede informatiebeveiliging. Vanuit deze optiek heeft de Rekenkamercommissie ook twee aanbevelingen aan de gemeenteraad. Deze zijn gebaseerd op de constatering dat de raad zich vooralsnog louter in algemene zin heeft laten informeren over het beleid. De raad geeft daarmee te weinig invulling aan de sturende en controlerende verantwoordelijkheden. Dit vertaalt zich in de volgende aanbevelingen.

6. Voer met enige regelmaat een discussie over het ambitieniveau van het gevoerde informatiebeveiligingsbeleid. Vertaal dit naar de risico-afwegingen die gemaakt worden en weeg dat af tegen andere waarden zoals gebruiksvriendelijkheid en de voordelen uit samenwerking met DOWR.

7. Laat u informeren over de wijze waarop het college van B&W opvolging geeft aan deze uitgangspunten en kom op basis daarvan tot een beoordeling van het gevoerde beleid.

3. Het gemeentelijk informatiebeveiligingsbeleid

In dit hoofdstuk staan de uitgangspunten van informatiebeveiligingsbeleid van Raalte centraal. Raalte werkt intensief samen met de gemeenten Deventer en Olst-Wijhe op het gebied van bedrijfsvoering. Daaronder valt ook de inrichting en toepassing van de ICT. Het beleid van Raalte op het gebied van informatiebeveiliging is binnen het samenwerkingsverband DOWR (Deventer, Olst-Wijhe, Raalte) opgesteld.

Het beleid bestaat uit een visie, een strategisch informatiebeveiligingsbeleid en diverse onderliggende beleidsstukken, waarin onder andere rollen en verantwoordelijkheden zijn vastgelegd.

3.1 i-Visie DOWR

De i-Visie (2018-2022) is het richtinggevende kader voor de DOWR gemeenten. Hierin hebben zij vastgelegd hoe zij de gemeentelijke informatievoorziening willen inzetten om de gemeentelijke ambities en maatschappelijke opgaven te realiseren. De gemeenten stellen in de i-Visie dat goede informatievoorziening en ICT een strategische factor is, en doorslaggevend is voor de uitvoering van de maatschappelijke opgaven, de effectiviteit en efficiency van de primaire processen en de dienstverlening van de gemeenten.

Informatieveiligheid en stabiliteit zijn volgens de i-Visie topprioriteit:

> "Wij geven de hoogste prioriteit aan informatieveiligheid en de privacy van persoonsgegevens. We treffen daarom als DOWR-gemeenten gezamenlijk aanvullende maatregelen en doen serieuze (extra) investeringen om onder andere te voldoen aan de BIG[4], de Baseline Informatiebeveiliging Nederlandse Gemeenten. Met deze ambitie borgen we geen 100% garantie op het voorkomen van veiligheidsincidenten, maar we voldoen wel aan de BIG. Wij geven de hoogste prioriteit aan de stabiliteit van de DOWR-informatievoorziening en ICT. Het borgen van de continuïteit heeft de eerste prioriteit, gevolgd door het doorvoeren van wettelijke maatregelen en het snel volgen van relevante ontwikkelingen." (i-Visie DOWR 2018-2022)

Toelichting op de Baseline Informatiebeveiliging Overheid (BIO)

De BIO is gericht op risicomanagement. Dat betekent dat processen en informatiesystemen beveiligd worden op basis van de risico's die de gemeente (wil) lopen. Het management zal daarbij op voorhand keuzes en afwegingen moeten maken of informatie in nieuwe en bestaande processen adequaat beveiligd is in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

Naar aanleiding van de visie is een aantal relevante ontwikkelthema's uitgewerkt, waaronder 'omgang met informatieveiligheid'. Digitaal gegevens delen, voldoen aan landelijke normenkaders zoals BIO[5] en ENSIA[6], en het groeiende digitale verkeer worden als belangrijke onderwerpen genoemd.

[4] De BIG, de Baseline Informatie Gemeenten, is een door de VNG opgestelde systematiek om een goede basis voor de informatiebeveiliging te realiseren. In afstemming met waterschappen, provincies en het rijk is de BIG doorontwikkeld naar de BIO, Baseline Informatiebeveiliging Overheid.

[5] BIO betreft de Baseline Informatiebeveiliging Overheid, deze vervangt de BIG, Baseline Informatiebeveiliging Nederlandse Gemeenten.

[6] ENSIA staat voor Eenduidige Normatiek Single Information Audit. Deze wordt door onder meer door gemeenten gebruikt om zich te verantwoorden over de staat van informatiebeveiliging op basis van de BIO (Baseline Informatiebeveiliging Overheid) en het gebruik van de Geo-basisregistraties.

Daarnaast wordt een uitgebreide ambitie geformuleerd ten aanzien van informatieveiligheid:

Ambitie omgang met informatieveiligheid – Thema's i-Visie 2018-2022
We minimaliseren onze informatierisico's, door zo spoedig mogelijk volledig te voldoen aan de Baseline Informatiebeveiliging Gemeenten. We maken en onderhouden de risicoanalyse BIG. We treffen alle aanvullende maatregelen en doen serieuze (extra) investeringen in informatieveiligheid. Dit vormt tevens het pakket van eisen aan leveranciers. Hierbij volgen we landelijke standaarden zoals BIG en AVG. We implementeren dit successievelijk met behulp van ons inkoopbeleid. We accepteren beperkingen in de beleving van klantvriendelijkheid en gebruikersvriendelijkheid als die het onvermijdelijke gevolg van te treffen maatregelen zijn. Bij ICT samenwerking veroorzaakt de zwakste schakel risico's voor de andere deelnemers. Informatieveiligheid leent zich - met uitzondering van de lokale organisatorische maatregelen - niet voor differentiatie tussen gemeenten. We zorgen voor maximale onafhankelijkheid en minimale belangentegenstelling om het beleid goed te implementeren en te handhaven. Informatieveiligheid wordt een vast onderdeel van de planning & control systemen van de gemeenten. Het maken van risico afwegingen ligt hoog in de organisatie. We verwachten nog maar in beperkte situaties dat we geconfronteerd worden met veiligheidsincidenten, maar kunnen die niet volledig voorkomen. We kunnen aantonen dat we al het mogelijke hebben gedaan om incidenten te voorkomen.

3.2 Strategisch beleid

Het 'Strategisch Informatiebeveiligingsbeleid DOWR-gemeenten 2020-2022' is door de Colleges van B&W van de drie gemeenten vastgesteld. Het beleid is gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO) en geldt voor alle processen van de gemeenten Deventer, Olst-Wijhe en Raalte.

Het beleid dient de informatievoorziening gedurende de hele levenscyclus van informatie- systemen te borgen, ongeacht de toegepaste technologie en het karakter van de informatie. Het beleid beperkt zich niet alleen tot de ICT, maar heeft ook betrekking op het politieke bestuur, alle medewerkers, burgers, gasten, bezoekers en externe relaties. Binnen het beleid is een aantal strategische doelstellingen geformuleerd:

- De DOWR-gemeenten staan garant voor correcte en veilige informatievoorzieningen.
- De DOWR-gemeenten zijn weerbaar tegen cyberaanvallen en beschermen haar vitale belangen in het cyberdomein.
- De DOWR-gemeenten handelen op het gebied van informatiebeveiliging in lijn met het algemene beleid en de relevante landelijke Europese wet- en regelgeving.
- De DOWR-gemeenten beschikken over voldoende kennis en kunde op het gebied van cybersecurity en investeren in ICT-innovatie om haar doelstellingen op het gebied van informatieveiligheid en privacy te behalen.
- De DOWR-gemeenten bouwen aan coalities met overheidspartners binnen het cyberdomein.
- De DOWR-gemeenten investeren in veilige en betrouwbare ICT-producten en -diensten ter bescherming van de informatie en de privacy van haar medewerkers, burgers en bedrijven.

Het strategische beleid is aangevuld met onderwerpspecifieke beleidsdocumenten voor informatiebeveiliging op tactisch en operationeel niveau. De uitwerking van het beleid vindt plaats aan de hand van een jaarlijks opgesteld Informatiebeveiligingsplan.

In haar beleid formuleert de DOWR-samenwerking een aantal uitgangspunten die voor dit onderzoek relevant zijn:

- Alle informatie en informatiesystemen zijn van belang voor de gemeente. Bepaalde informatie is zelfs van vitaal belang. Het college van B&W is eindverantwoordelijk voor de beveiliging van alle gemeentelijke informatie.
- De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het lijnmanagement. Alle informatiesystemen die gebruikt worden door de gemeente hebben een interne eigenaar die de vertrouwelijkheid en/of waarde bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming daarvan ligt dan ook bij de eigenaar van de informatie.
- Door periodieke controle, organisatiebrede planning en coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatiebeveiligingsbeleid vormt samen met het Informatiebeveiligingsplan (IBP) het fundament onder een betrouwbare informatievoorziening. In het IBP wordt de betrouwbaarheid van de informatievoorziening organisatiebreed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.
- Informatiebeveiliging is een continu verbeterproces. De fasen Plan, Do, Check en Act (PDCA) vormen samen het managementsysteem van informatiebeveiliging.
- De gemeente stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze zoals gesteld in dit beleid.
- Regels en verantwoordelijkheden voor het beveiligingsbeleid dienen te worden vastgelegd.
- Iedere medewerker is verplicht om gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

Daarnaast worden er drie randvoorwaarden geformuleerd ten aanzien van de informatieveiligheid binnen de gemeenten:

1. Externe leveranciers en ketenpartners buiten de overheid zijn zelf niet rechtstreeks gebonden aan de BIO, maar moeten wel voldoen aan de eisen van de opdrachtgever. Alle voorwaarden om te voldoen aan het informatiebeveiligingsbeleid van de gemeente moeten daarom in de contracten zijn vastgelegd.

2. Kennis en bewustzijn van informatiebeveiliging en het omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.

3. Jaarlijks wordt een Informatiebeveiligingsplan (IBP) opgesteld onder leiding van de CISO. Hierin worden de tactische en operationele aspecten van de informatiebeveiliging verder uitgewerkt, aangevuld met de planning van concrete acties om de praktijk in overeenstemming te brengen met de maatregelen uit het beleid. Het IBP is gebaseerd op de volgende bronnen:

    a. De uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA).

    b. Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten, opgesteld door de Informatiebeveiligingsdienst (IBD).

    c. De door de teammanagers, teamleiders en domeinmanagers ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn.

3.2.1 Roadmap Digitale weerbaarheid 2021-2023

De Roadmap Digitale weerbaarheid 2021-2023 is richtinggevend in de uitvoering van het strategische informatiebeveiligingsbeleid voor DOWR gemeenten. Per jaar is er een strategisch thema aan de hand waarvan gewerkt wordt aan een digitaal weerbare gemeente.

In 2020 was dat de basis voor informatiebeveiliging conform BIO, in 2021 lag de focus op een bewust bekwame organisatie en in 2022 wordt de stap gezet naar een digitaal veilige organisatie.

Strategische thema's informatieveiligheid DOWR-gemeenten 2020-2023

2020 – Basis informatiebeveiliging geborgd De DOWR gemeenten waarborgen de kwaliteit van informatie conform de Baseline Informatiebeveiliging Overheid (BIO)	**2021 – Bewust bekwame organisatie** De DOWR gemeenten waarborgen het bevorderen van de bewustwording van medewerkers (strategisch, tactisch en operationeel), zodat zij vanuit hun functie bewust/bekwaam handelen en veilig omgaan met betrouwbare informatie.
2022 – Digitaal veilige organisatie De DOWR gemeenten zijn informatieveilige bewuste organisaties en werken uitsluitend samen met VERTROUWDE partners om de vertrouwbaarheid van de keten te garanderen.	**2023 – Digitaal weerbare samenleving** De DOWR gemeenten waarborgen en faciliteren een veilige digitaal weerbare samenleving met betrouwbare informatie

3.3 Tactisch beleid

Het strategisch informatiebeveiligingsbeleid wordt op tactisch en operationeel niveau ingevuld aan de hand van onderliggende beleidsdocumenten en plannen, waarin richtlijnen en maatregelen zijn geconcretiseerd. Het gaat om onderstaande beleidsdocumenten:

- Beleid Anti-Malware DOWR-gemeenten
- Beleid Backup en Recovery DOWR-gemeenten
- Beleid Change Management DOWR-gemeenten
- Beleid Cloud Computing DOWR-gemeenten
- Beleid Contract Management DOWR-gemeenten
- Beleid Encryptie DOWR-gemeenten
- Beleid Fysieke Beveiliging DOWR-gemeenten
- Beleid Incident Management en Response DOWR-gemeenten
- Beleid Logging en Monitoring DOWR-gemeenten
- Beleid Logische Toegangsbeveiliging DOWR-gemeenten
- Beleid Mobiele Apparaten DOWR-gemeenten
- Beleid Personeel DOWR-gemeenten
- Beleid Telewerken DOWR-gemeenten
- Beleid Wachtwoorden DOWR-gemeenten

De uitwerking van dit beleid in concrete maatregelen vindt plaats in een jaarlijks Informatiebeveiligingsplan (IBP). Jaarlijks wordt ook een gap-analyse gedaan in het kader van het voldoen aan de BIO-normen.

3.5 Informatiebeveiligingsplan

Het jaarlijks informatiebeveiligingsplan is gecombineerd met het jaarlijkse privacyplan. In het Jaarplan Informatieveiligheid & Privacy 2022 worden actiepunten genoemd om de bescherming van persoonsgegevens en de beveiliging van informatie verder te verbeteren. De bevindingen van de

Functionaris Gegevensbescherming en Chief Information Security Officer uit de jaarrapportages 2021 en de Roadmap Digitale weerbaarheid 2021-2023 liggen mede ten grondslag aan de actiepunten van het jaarplan 2022.

De uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA), het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten[7] en door de teammanagers, teamleiders en domeinmanagers ingebrachte onderwerpen worden eveneens meegenomen in het informatiebeveiligingsplan.

3.4 Verantwoordelijkheden

Bij de uitvoering van het beleid hebben het bestuur, de directie en het middenmanagement (zijnde de teammanagers, teamleiders en domeinmanagers van de gemeente Raalte) alle een eigen rol en verantwoordelijkheid. Deze verdeling is gebaseerd op het Three Lines of Defense model (3LoD). Dit is een model waarbij de beheersing van risico's over een eerste, tweede en derde lijn wordt verdeeld. De drie linies hebben een gezamenlijke cruciale rol bij het inschatten van het belang van de verschillende delen van de informatievoorziening, de risico's in beeld te brengen en te bepalen welke van deze risico's onacceptabel hoog zijn.

3.4.1 De eerste lijn

Het lijnmanagement, de eerste lijn, is primair verantwoordelijk voor de informatiebeveiliging in de eigen processen. De aansturing in de eerste lijn wordt door de directie van Raalte verzorgd. De directie (of directieteam) stelt ook het gewenste niveau van continuïteit en vertrouwelijkheid vast. Zij zorgt dat alle processen en systemen onder verantwoordelijkheid vallen van een teammanager, teamleider of domeinmanager, dat zij zich verantwoorden over de beveiliging én dat de portefeuillehouders binnen het college worden geïnformeerd.

Taken die het lijnmanagement als eerste lijn uitvoert zijn:

- Het leveren van input voor wijzigingen op maatregelen en procedures.
- Het binnen de eigen afdeling uitdragen van het beveiligingsbeleid en de daaraan gerelateerde procedures.
- Het vroegtijdig signaleren van de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld.
- Bespreking van beveiligingsincidenten en de consequenties die dit moet hebben voor beleid en maatregelen.

Uitvoerende werkzaamheden kunnen worden gedelegeerd naar de tweede lijn, maar verantwoordelijkheid niet.

3.4.2 De tweede lijn

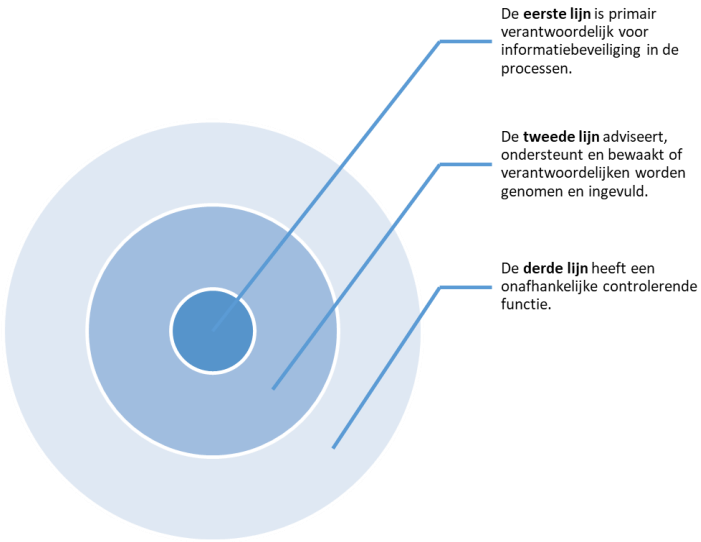
De Chief Information Security Officer en Security officers vormen de tweede lijn, die ondersteunt, adviseert, coördineert en bewaakt of de eerste lijn, het management, zijn verantwoordelijkheden ook daadwerkelijk neemt. De tweede lijn ligt voor Raalte voornamelijk binnen de DOWR-samenwerking belegd, de informatiemanager van Raalte is belangrijke schakel naar DOWR.

[7] opgesteld door de Informatiebeveiligingsdienst (IBD)

3.4.3 De derde lijn

De derde lijn wordt gevormd door (interne of externe) auditors, zoals de Functionaris Gegevensbescherming. De derde lijn heeft een onafhankelijke rol bij de controle op de eerste en tweede lijn.

Samenvattend kunnen de drie verdedigingslijnen als volgt grafisch worden weergegeven:



4. Informatiebeveiliging in de praktijk

Het gemeentelijk informatiebeveiligingsbeleid in Raalte leidt tot diverse processen en maatregelen. Tijdens het onderzoek is aan de hand van interviews en casusbesprekingen verkend hoe het beleid zich vertaalt naar de praktijk en hoe beveiligingsmaatregelen zorgen voor weerbaarheid in processen waarbij gebruik wordt gemaakt van data en informatie. De opgedane inzichten zijn uiteindelijk nog getoetst en verdiept in een zogenoemde convergentiesessie. Hieraan hebben sleutelpersonen in de ambtelijke organisatie voor digitale veiligheid deelgenomen.

In de interviews, casusbesprekingen en convergentiesessie is niet alleen naar maatregelen gekeken die vooraf (preventief) ter bescherming zijn genomen, maar ook naar maatregelen die de gemeente heeft genomen om in het geval van een incident of een (grote) aanval te handelen, en op welke manier de gemeente voorbereid is op een crisis. In dit hoofdstuk worden de bevindingen over de informatiebeveiliging in de praktijk weergegeven aan de hand van de organisatorische borging van de veiligheid in processen, de organisatiecultuur met betrekking tot informatiebeveiliging en de technische maatregelen. Als laatste wordt stilgestaan bij de positie van de raad ten aanzien van informatiebeveiliging.

4.1 De samenwerking binnen DOWR

De samenwerking tussen de gemeenten Deventer, Olst-Wijhe en Raalte binnen DOWR is van grote betekenis voor de inrichting en de dagelijkse praktijk van de informatiebeveiliging. Deze samenwerking bestaat sinds 2012. De samenwerking, die overigens op meer thema's dan louter ICT plaatsvindt, is ingegeven door de ambitie om de slagkracht van de gemeenten te versterken en de kwetsbaarheid te verminderen. Over het algemeen, zo komt uit de interviews naar voren, bestaat er tevredenheid over deze samenwerking, zowel in het algemeen als specifiek over de samenwerking met betrekking tot de ICT. In een recente benchmark is bovendien gebleken dat de gemiddelde kosten voor ICT in deze samenwerking in vergelijking met referentiegemeenten beneden het gemiddelde liggen, terwijl de prestaties juist bovengemiddeld zijn.[8]

In het verlengde van de geconstateerde tevredenheid bestaat binnen de organisatie van Raalte eveneens een positief beeld van de samenwerking op het gebied van informatiebeveiliging. De geïnterviewde medewerkers van de organisatie benadrukken dat als Raalte rond dit onderwerp zelfstandig zou opereren, lang niet dezelfde kennis en slagkracht beschikbaar zouden zijn. Ook wordt ervaren dat de kwetsbaarheid van Raalte vanwege de samenwerking is afgenomen. Er is een relatief grote staf van kundige ambtenaren beschikbaar, die elkaar kunnen vervangen. Mochten er ingrijpende technische problemen zijn in een gemeente, dan kan gebruik gemaakt worden van de faciliteiten van één van de andere gemeenten.

Overigens blijft ook binnen de samenwerking voorop staan dat uiteindelijk Raalte zelf eindverantwoordelijk is voor de informatiebeveiliging. Binnen de samenwerking bestaat te allen tijde de mogelijkheid dat Raalte eigen keuzen maakt. In interviews is genoemd dat Raalte over het algemeen meegaat in de gezamenlijke keuzen, maar incidenteel daarin enkele andere accenten plaatst. Vanuit DOWR wordt geschetst dat Raalte een duidelijke eigen visie heeft: in Raalte werkt vooral een 'rechtdoorzee-aanpak', afspraken met betrekking tot informatievoorziening moeten passen bij het dagelijks werk.

Al met al wordt ervaren dat samenwerking bijdraagt aan de kwaliteit en continuïteit van de informatiebeveiliging. Daarnaast wordt genoemd dat de samenwerking de dienst DOWR-i (de afdeling die verantwoordelijk is voor de ICT van de drie gemeenten) een aantrekkelijkere werkgever maakt.

[8] Dit blijkt uit de 'ICT-benchmark gemeenten 2022', die door M&I-partners is uitgevoerd. Een kleine nuance bij deze bevinding is dat Raalte, Olst-Wijhe en Deventer in deze benchmark als één organisatie zijn beschouwd. Daardoor bestaat de referentiegroep uit 100.000+-gemeenten.

4.2 Organisatorische borging van de informatieveiligheid

De verantwoordelijkheid voor informatiebeveiliging ligt bij de eerste lijn en daarmee de bestuurder. In Raalte is de burgemeester de portefeuillehouder en deze is tevens verantwoordelijk voor crisisbeheer. Primair is de proceseigenaar (doorgaans de domeinmanager) verantwoordelijk voor de informatievoorziening en eventueel daarmee verbonden risico's. In de organisatie wordt ervaren, zo blijkt uit de interviews, dat de portefeuillehouder een actieve rol vervult bij het bewaken en bevorderen van de digitale weerbaarheid. De burgemeester wordt gezien als aanjager van het onderwerp, hij vraagt geregeld aandacht voor het onderwerp binnen de organisatie en ook bij de raad benadrukt hij het belang.
De 'business,' de gemeente Raalte, moet zich verantwoordelijk voelen voor de veiligheid van de data en informatie die ze gebruiken. Die verantwoordelijkheid berust niet bij het samenwerkingsverband. In de interviews is gebleken dat dit uitgangspunt goed bekend is bij de medewerkers van de gemeente.

De Chief Information Security Officer (CISO) neemt deel aan het directieoverleg en het bedrijfsvoeringsoverleg. Deze functionaris legt verantwoording af aan het college, de facto aan de gemeentesecretaris. Belangrijke rollen in de uitvoering van de informatiebeveiliging zijn de Technical Information Security Officer, die de focus heeft op de technische beveiliging, de Information Security Officer voor de algemene veiligheid en de ENSIA-coördinator die zich bezig houdt met de ENSIA-audits . De Chief Information Security Officer heeft enerzijds de verantwoordelijkheid ten aanzien van directie en bestuur, anderzijds om het belang van informatiebeveiliging richting de werkvloer uit te dragen. Op operationeel niveau vindt maandelijks een kernteamoverleg informatiemanagement plaats. Op tactisch niveau vindt op gezette tijden een themasessie met het management plaats. Op strategisch niveau vindt maandelijks het Strategisch Informatie Overleg (SIO) met de FG, CISO en CIO plaats (met verslaglegging richting management). Dit SIO gaat in 2023 veranderen door het een integraal onderdeel te maken van het directieoverleg. Dot wordt periodiek geagendeerd.
Elk kwartaal vindt een portefeuillehoudersoverleg digitalisering plaats met de burgemeester, FG, CISO, CIO en informatiemanager.

Een groot deel van de implementatie van maatregelen ligt bij de DOWR-i organisatie. Uit de interviews blijkt dat er een zekere afstand wordt ervaren tussen de gemeentelijke uitvoering en DOWR. De eerste en tweede lijn acteren daardoor grotendeels gescheiden. Een belangrijke schakel is daardoor de informatiemanager van de gemeente. Zijn belangrijkste taak is het 'vertalen' van ICT (en informatieveiligheid) vanuit DOWR naar management, organisatie, en bestuur in Raalte.

Bij de bescherming van processen en dienstverlening stuurt DOWR op basis van (uitvoerings)plannen, die weer afgeleid zijn uit het IV-jaarplan. Genoemd wordt dat in het jaarplan informatiebeveiliging en privacy in samenhang worden uitgewerkt. Er is enig onderscheid tussen de onderwerpen, maar veel van de maatregelen zijn gelijk.

Uit de gesprekken blijkt dat de gemeente bij nieuwe processen en applicaties meestal risico-analyses uitvoert. Niet voor alle bestaande processen zijn deze analyses uitgevoerd. De gemeente heeft wel de wens om het geheel aan risico-analyse inzichtelijk te krijgen. In het financieel en sociaal domein is gestart met de ontbrekende processen in kaart te brengen aan de hand van risico-analyse. In die domeinen leeft het belang van informatieveiligheid en privacy het meest, zo wordt genoemd. Uit de interviews blijkt dat kritische processen rondom persoonsgegevens beter in beeld dan zijn dan kritische processen rond informatiebeveiliging in het algemeen. Er is genoemd dat proceseigenaren (domeinmanagers) aan de hand van de Baselinetoets BIO risicoafwegingen maken ten aanzien van hun processen. Deze toetsen, en een compleet risico-overzicht van processen en systemen, zijn in het onderzoek echter niet aangetroffen.

Vanuit privacy oogpunt wordt de achterstand aan uitvoering van de (uit AVG oogpunt) wettelijk verplichte risico-analyses ervaren als een risico. Er zijn 33 processen met een mogelijk hoog-risico (risico gebaseerd op register anno 2018) waar nog een risico-analyse op moet worden uitgevoerd. In

het najaar van 2022 bestond er een discrepantie tussen het aantal uren dat vanuit privacyfunctionarissen beschikbaar is en het aantal uren dat zij feitelijk nodig hebben. Er is toen een gebrek aan capaciteit op het gebied van privacy ervaren, waardoor de gemeente niet zoals gewenst aan de wettelijke verplichting kon voldoen. In 2023 is er budget beschikbaar gekomen voor personele uitbreiding en is de werving gestart.

4.3 Technische maatregelen

De informatiebeveiliging van Raalte is geïntegreerd in de DOWR-samenwerking. Binnen die context is er veel aandacht voor de 'technische borging' van het beleid. In de gesprekken is een groot aantal maatregelen de revue gepasseerd.

Op basis van het beleid worden diverse technische maatregelen geïmplementeerd. Daarbij spelen het dreigingsbeeld, de Baseline Informatiebeveiliging Overheid (BIO) normen en het vastgestelde beveiligingsniveau een rol, evenals de jaarrapportage van de CISO en het Jaarplan informatiebeveiliging en privacy.

De technische infrastructuur van Raalte, de processen en informsatiesystemen, wordt getoetst aan de BIO. De BIO wordt gebruikt om afwegingen te maken voor de beveiligingsmaatregelen. Deze beveiligingsmaatregelen worden jaarlijks geïnventariseerd aan de hand van een gapanalyse, waarmee wordt bepaald in hoeverre de gemeente voldoet aan de normen uit de BIO.

Het beveiligingsbeleid vindt ook zijn uitwerking in de operationele processen, zoals vulnerability management. Vulnerability management betekent dat er continu gezocht wordt naar kwetsbaarheden in de eigen systemen. Kwetsbaarheden worden inzichtelijk gemaakt en opgevolgd. Uit de interviews blijkt dat gebruik wordt gemaakt van eigen tools, maar ook van meldingen van de Informatie Beveiligingsdienst. De organisatie zet ook in op hardening, dat is uitzetten van ongewenste of niet gebruikte onderdelen van software waarmee kwetsbaarheden worden verkleind.

Uit de interviews blijkt dat maatregelen soms ook worden genomen op basis van actualiteit. Naar aanleiding van de oorlog in Oekraïne zet de gemeente nu 'geo-blocking' in, waardoor mensen (of computers) vanuit landen met een hoog cybersecurityrisico, zoals Rusland en Oekraïne, geen toegang meer hebben tot de gemeentelijke IT-infrastructuur.

Ook voor het detecteren van incidenten heeft de gemeente diverse technische maatregelen geïmplementeerd. DOWR maakt gebruik van een firewall die beschermt, monitort en controleert op wat er gebeurt op het gemeentelijk netwerk en de toegang daartoe. Met behulp van antimalware software wordt gescand op malafide code. Er wordt gebruik gemaakt van een Security Operations Center (SOC) en SIEM (Security Information Event Management) detectiemechanisme, waarmee bedreigingen kunnen worden gedetecteerd, geanalyseerd en er snel op kan worden gereageerd.

Er worden pentesten ingezet om de netwerken van DOWR te toetsen. Pentesten zijn testen waarbij de systemen of een specifiek systeem getoetst worden op kwetsbaarheden door ethische hackers. Uit de interviews blijkt dat de pentesten tot nu toe geen grote kwetsbaarheden in de gemeentelijke systemen vonden.

4.4 Borging van de veiligheid in processen

Voor de borging van informatiebeveiliging heeft de gemeente een groot aantal processen ingericht op basis van de BIO. In het kader van het onderzoek is onder andere het autorisatiebeheer genoemd. Uit de casusbesprekingen blijkt dat er verschillende rechten worden toegekend op basis van rollen en functies. Deze autorisaties worden aangevraagd en gewijzigd op basis van akkoord vanuit management. Ook worden de autorisaties regelmatig gecontroleerd en zelf gewijzigd bijvoorbeeld indien er geen gebruikt wordt gemaakt van bepaalde rechten. De diverse autorisaties zorgen ervoor dat informatie enkel toegankelijk is voor degenen het nodig hebben voor hun werk. In een aantal

processen, zoals Burgerzaken, faciliteert de scheiding van autorisaties daarnaast ook een vier-ogen-principe.

Ondanks de technische maatregelen kunnen incidenten voorkomen. De gemeente gebruikt hiervoor een security incident response proces. Dit proces gaat specifiek over beveiligingsincidenten, en bevat een escalatie/opschalingsroutes naar het CSIRT (Computer Security Incident Response Team) en daarna het crisisteam/-plan. De gemeente baseert de afhandeling van incidenten of risico op een incident op basis van een risico-inschatting. Zo keek de gemeente bij een groot beveiligingsrisico[9] in 2021 eerst naar wat het risico en de omvang was voor de DOWR organisatie. Op basis daarvan zijn er acties uitgezet en zijn de leden van de regiegroepen ICT, het directieberaad en de Chief Information Officers van DOWR geïnformeerd blijkt uit de interviews.

Zware incidenten die veel impact hebben op de organisatie, zoals het doorbreken van de digitale beveiliging en/of het hacken van de systemen, zijn vooralsnog niet voorgekomen. Maar lichtere incidenten, zoals (kleine) datalekken (zoals informatie naar een verkeerd mailadres verzenden) zijn eigenlijk onvermijdelijk, en gebeuren dus ook. Men vindt het vooral belangrijk dat de organisatie weerbaar is bij incidenten. In Raalte is hier vertrouwen in.

Voor het reageren in het geval van zware incidenten heeft de gemeente een business continuity plan, waarbij de samenwerkende gemeenten elkaar als uitvalsbasis kunnen inzetten voor de nodige processen. In het plan is vastgesteld welke processen binnen welke tijd weer in de lucht gebracht moeten worden na een verstoring in de beschikbaarheid of continuïteit de lucht gehouden moeten worden, bijvoorbeeld communicatie en publiekszaken. Ook zijn de eisen van de gemeente aan die processen vastgelegd. Die eisen zijn bepalend voor de volgorde waarin de systemen worden hersteld en de fysieke uitvalsbasis. Vanuit Deventer kan men naar Raalte uitwijken en andersom. Op alle drie de locaties is netwerktoegang voor de afzonderlijke gemeenten. De uitwijkmogelijkheid wordt jaarlijks getest, waarbij elk jaar verschillende varianten worden getest. Op basis van een voorgaande test werden nog enkele problemen ondervonden, die dankzij het testen zijn verholpen.

Voor het geval er incidenten optreden is er een back-up beleid, dat voorziet in processen om te ‘herstellen’. Er is onderscheid gemaakt tussen de cloud-producten[10] die de organisatie afneemt en on premise[11] producten. Het beleid garandeert dat back-ups zijn gescheiden en niet gekoppeld aan het netwerk. Daarnaast worden back-ups gespiegeld op twee locaties, de back-ups kunnen ook niet zomaar worden weggegooid. Er is een ‘sleutel’ van de beheerder én van de leverancier nodig. Het herstellen van back-ups wordt een paar keer per jaar getest bij het wijzigen of updaten van het pakket. De DOWR-organisatie is nog aan het uitzoeken of dat voldoende is, of dat dit frequenter en structureel gedaan moet worden.

Er wordt daarnaast gewerkt aan een Cybercrisisplan in DOWR-verband. Onderdeel daarvan zijn sleutelbesluiten: wie gaat wat doen in welke situatie en welke keuzes er gemaakt worden in diverse scenario's. In 2023 zullen er ook trainingen en oefeningen in dit kader plaatsvinden, inclusief (crisis)oefeningen op het thema informatiebeveiliging. De portefeuillehouder besteedt hier aandacht aan. Dit wordt belangrijk bevonden. Want, zo blijkt uit de interviews, als er in een crisis beslissingen in Deventer worden gemaakt hebben die automatisch invloed op Raalte.

Incidenten worden na afloop geëvalueerd. Uit de interviews blijkt dat bij incidenten twee zaken van belang zijn. In eerste instantie moet wat fout is gegaan rechtgezet worden en ten tweede moet achterhaald worden hoe het fout is gegaan. Geschetst wordt dat van incidenten, zoals datalekken

[9] Er was een ernstige kwetsbaarheid gevonden in Apache Log4j. Dit is software die veel gebruikt wordt in webapplicaties en allerlei andere systemen. Het NCSC waarschuwde voor potentieel grote schade en adviseerde organisaties daarom om zich voor te bereiden op een mogelijke aanval.

[10] Producten zoals programma’s en systemen die de gemeente via internet benadert. Deze zijn via de ‘cloud’ toegankelijk.

[11] On-premise producten zijn programma’s en systemen die de gemeente via eigen servers (hardware) op locatie toegankelijk maakt.

steeds wordt geleerd, er wordt bekeken of er iets structureel anders moet worden geregeld. Dat kan aanleiding zijn om werkprocessen aan te passen. Lessons learned van grote incidenten, onder andere bij andere gemeenten, worden besproken met het bestuur.

4.5 Cultuur en bewustzijn

In de aanloop tot de invoering van de AVG[12] is er binnen de organisatie veel over privacy gesproken, met name over datalekken. Genoemd wordt dat in dat kader een sfeer is gecreëerd waarin mensen bereid zijn om datalekken te melden. Ook incidenten worden tijdens werkoverleggen besproken en daar worden lessen uit getrokken. Uit de casusbesprekingen[13] blijkt dat medewerkers zich sterk bewust zijn van het belang van informatiebeveiliging en hun eigen rol daarin. Uit de interviews blijkt dat medewerkers niet alleen integriteitsverklaringen ondertekenen als onderdeel van het personeelsbeleid, ook wordt gesteld dat integer omgaan met (persoons)gegevens verankerd zit in de cultuur. Opgemerkt wordt dat het in de haarvaten van de afdeling Burgerzaken zit om vragen te stellen over veiligheid en privacy. Een voorbeeld daarvan is dat bij het mogelijk uitbesteden van het adresonderzoek aan Deventer, meteen veel vragen werden gesteld over wat een mogelijke uitbesteding betekent voor de gegevens. Ook uit de bespreking van Vergunningen blijkt dat er over het algemeen veel bewustzijn is rondom veiligheid en privacy. Zo zijn tijdens de casusbespreking verschillende onderwerpen in het kader van informatiebeveiliging ter sprake gekomen, die niet direct met het proces vergunningen te maken hebben maar waar medewerkers zich wel bewust van zijn.

Voor informatiebeveiliging wordt op verschillende manieren aandacht gevraagd in de organisatie. Een veel genoemde maatregel zijn de zogenoemde nano-leanings, een bewustwordingscampagne voor informatiebeveiliging en privacy. Elke drie weken krijgen de medewerkers een digitale les, waarin concrete aandachtspunten worden gegeven. Soms bevat die ook een test. Zo is er getest voor de alertheid op phishingmails. De les duurt meestal een paar minuten. De domeinmanagers krijgen overzichten van de respons onder de werknemers. Aangegeven wordt dat de algemene resultaten in de domeinen besproken worden en zo nodig aanleiding zijn voor een gesprek met medewerkers. Uit de interviews blijkt dat de nano-learnings als effectief worden ervaren voor het beveiligingsbewustzijn. Al bestaat ook het besef dat er medewerkers zijn die de nano-learnings als sleets ervaren, daarover wordt genoemd dat fysieke bijeenkomsten en meer klassieke trainingen mogelijk effectiever zijn. De gemeente is voornemens daar in 2023 meer ruimte voor te maken. In zijn algemeenheid wordt door medewerkers gesteld dat informatiebeveiliging in de haarvaten zit, maar dat het onder de aandacht brengen van het belang ervan wel een continu proces moet zijn.

De eerdere paragrafen in dit hoofdstuk hebben laten zien dat er in Raalte, of liever in DOWR-verband, sprake is van relatief veel technische maatregelen om de informatieveiligheid te garanderen. Naast de technische maatregelen zijn er ook veel processen en procedures vastgelegd die de informatieveiligheid dienen te versterken. Dat heeft consequenties voor het door de medewerkers ervaren gebruikersgemak. Sommige medewerkers spreken in dit verband wel over ‘rigide IT’. Verschillende betrokkenen, waaronder de portefeuillehouder, ervaren wat dit betreft een toenemende spanning. Incidenteel leidt dit er toe dat sommige medewerkers pogingen in het werk stellen de technische vereisten te omzeilen.

4.6 Over de raad

De gemeenteraad in Raalte is vooralsnog niet heel actief geweest als het gaat om privacy en informatieveiligheid. In de vorige raadsperiode zijn er jaarverslagen over deze onderwerpen ter kennisname met de raad gedeeld. Hier zijn door raadsleden nauwelijks vragen over gesteld. Verschillende respondenten noemen dat de samenwerking binnen DOWR, waaronder ICT en informatieveiligheid, door raadsleden overwegend als uitvoeringskwesties worden ervaren, waar zij als raadsleden weinig mee van doen hoeven te hebben. Alleen als er incidenten zijn, worden

[12] Algemene verordening gegevensbescherming
[13] Casusbesprekingen waarin processen Burgerzaken en Vergunningen zijn besproken.

raadsleden alert en zijn ze wel geneigd om vragen te stellen, zoals het incident bij de gemeente Hof van Twente. Zoals geconstateerd in dit onderzoek is er zelden sprake van incidenten binnen Raalte.

In het kader van het inwerkprogramma van de in 2022 nieuw gekozen raad heeft er medio november 2022 een uitgebreide bijeenkomst over digitalisering plaatsgevonden, met daarin veel aandacht voor informatieveiligheid. Verschillende raadsleden hebben aanvullende en verduidelijkende vragen gesteld. Tot een gedachtewisseling over de uitgangspunten die bij informatieveiligheid worden gehanteerd en de consequenties daarvan voor onderwerpen als de dienstverlening door de gemeente en de effectiviteit van de organisatie is het niet gekomen. Gezien de context en inrichting van deze bijeenkomst heeft de raad zich nu primair laten informeren.

5. Bestuurlijke reactie

[PM]

6. Nawoord

[PM].

Bijlage 1: Geïnterviewde functionarissen

Datum	Functie
15 september 2022	Manager Bedrijfsvoering
19 september 2022	Coördinator ENSIA-audit
19 september 2022	Gemeentesecretaris
20 september 2022	CISO / ISO
20 september 2022	Functionaris gegevensbescherming (FG) / Privacy Officer
21 september 2022	Informatiemanager
21 september 2022	Burgemeester
28 september 2022	Afvaardiging van de IT organisatie (DOWR) / groepsmanager DOWR-i / Teammanager DOWR-i en CTO
29 september 2022	Directeur (met name Ruimtelijk Domein)
4 oktober 2022	TISO / ISO

Datum	Casusbespreking	Deelnemers
17 november 2022	Vergunningen (omgevingsvergunning)	Vergunningsverlener (omgevingsvergunningen), beleidsmedewerker VTH, Procesregisseur, administratief medewerker vergunningen (/key user)
24 november 2022	Burgerzaken (inschrijven BRP)	Domeinmanager, gegevensbeheerder burgerzaken, beleidsmedewerker burgerzaken

Deelnemers convergentiesessie 12 december 2022
Coördinator ENSIA-audit
Privacy Officer
Informatiemanager

Bijlage 2: Bestudeerde documentatie

Documentnaam
Assurance Rapportage DigiD TPM - DOWR
Beleid Change Management DOWR-gemeenten
Beleid Incident Management en Response DOWR-gemeenten
Beleid Logische Toegangsbeveiliging DOWR-gemeenten
Beleidskader Informatieveiligheid DOWR 2017-2020
Collegeverklaring Raalte DigiD en Suwinet 2021 ENSIA
Collegeverklaring-ENSIA-2021-bijlage 2-Suwinet-Raalte
Collegevoorstel Uitvoeringsplan DOWR-i werkorganisatie
Collegevoorstel Uitvoeringsplan en beleidskader informatieveiligheid
Collegevoorstel Vaststelling i-Visie 2018 - 2022
Cybersecurity Crisisplan DOWR
Directieberaad IV-DOWR 2021
DOWR-I Cybersecuritycrisis (*gemeente X*)
GAP Analyse BIO 05-2021
Gemeente Raalte_WOZ 2021 ENSIA
i Visie 2018 - 2022 DOWR
ICT-Benchmark Gemeenten DOWR (2022)
ICT-beveiligingsassessments DigiD - aansluiting 1000313 (Raalte)
ICT-beveiligingsassessments DigiD - aansluiting 1002569 (Raalte)
ICT-beveiligingsassessments DigiD - aansluiting 1002973 (belastingloket DOWR)
Informatiebeveiligingsplan DOWR 2021
Jaarplan Privacy - Informatiebeveiligingsplan 2022
Jaarrapportage CISO 2021
Jaarrapportage FG 2021
Mapping maatregelen BIO naar Informatiebeveiligingsbeleid DOWR-gemeenten
Privacy en Informatiebeveiligingsplan 2023
Procesbeschrijving Hardening
Procesbeschrijving Logging en Monitoring
Procesbeschrijving Security Incident Response
Procesbeschrijving Vulnerability Management
Raadsvoorstel en -besluit Vaststelling i-Visie 2018 - 2022
Raalte Assurancerapport ENSIA 2021
Raalte Assurancerapport ENSIA 2021 GET
Rapport cyberaanval gemeente *x* (*datum*)
Rapport_DOWR – PENtest VERTROUWELIJK
Rapportage Dimpact TPM DigiD eSuite 2021 Raalte
Risico analyse VTH vastgesteld
Risicoanalyse SIEM-SOC
Risicoanalyse Vulnerability Management
Strategisch Informatiebeveiligingsbeleid DOWR-gemeenten 2020-2022
Themas i-Visie 2018 - 2022
Toelichting DOWR-I op adviezen in rapport cyberaanval gemeente x
Toelichting DOWR-I op adviezen in rapport cyberaanval gemeente y

Toezichtjaarverslag informatieveiligheid en privacy 2022 van de FG en CISO van Deventer, Olst-Wijhe en Raalte
Uitvoeringsplan Informatieveiligheid 2017-2020
Vastlegging Communicatie Log4j

Bijlage 3: Lijst met afkortingen en begrippen

Afkorting	Betekenis
AVG	Algemene Verordening Gegevensbescherming
BBN	Basisbeveiligingsniveau (1 – 3)
BIG	Baseline Informatiebeveiliging Gemeenten
BIO	Baseline Informatiebeveiliging Overheid
CISO	Chief Informatie Security Officer
CTO	Chief Technical Officer
ENSIA	Eenduidige Normatiek Single Information Audit
GeVS	Gezamenlijke Elektronische Voorzieningen Structuur
GGI	Gemeentelijke Gemeenschappelijke Infrastructuur
IBD	Informatiebeveiligingsdienst Gemeenten (VNG Realisatie)
ICT	Informatie- en Communicatie Technologie
FG	Functionaris Gegevensbescherming
ISMS	Information Security Management System
ISO	Information Security Officer
NIST Framework	National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity
PDCA	Plan-Do-Check-Act
SIEM	Security Information & Event Management
SO	Security Officer
SOC	Security Operations Center
TISO	Technical Information Security Officer

Begrip	Betekenis
Cybercriminaliteit	Doelbewust van binnenuit of buitenaf inbreuk maken op informatiesystemen van een organisatie met als doel financieel gewin of verstoren.
DDoS aanval	Een Distributed Denial of Service (DDoS) aanval is een aanval gericht op sabotage of verstoring van informatiesystemen waardoor deze (tijdelijk) niet meer beschikbaar zijn.
Informatiebeveiliging	Het proces van vaststellen van de vereiste beveiliging van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen.
Malware	Kwaadwillende software dat informatiesystemen probeert te verstoren.
Phishing aanval	Een aanval waarbij de aanvaller zich voordoet als iemand anders (een persoon of organisatie) met als doel persoonsgegevens of inloggegevens te vergaren.
Ransomware	Ook wel gijzelsoftware genoemd. Blokkeert het gebruik van een systeem of data via versleuteling met als doel losgeld te ontvangen.

Gemeente Raalte
Rekenkamercommissie