REKENKAMER

gemeente Weststellingwerf

gemeente Oost-Stellingwerf

gemeente Opsterland

Onderzoeksopzet

Informatiebeveiliging

September 2024

Achtergrond

In de afgelopen decennia hebben gemeenten hun werkwijze steeds meer gedigitaliseerd. Dit heeft geleid tot nieuwe risico's voor de veiligheid van informatie. Gemeenten worden namelijk steeds vaker geconfronteerd met digitale bedreigingen en cyberaanvallen die de continuïteit van hun dienstverlening in gevaar brengen en kunnen leiden tot datalekken. De schade die hierdoor ontstaat, is niet alleen financieel; datalekken en beveiligingsincidenten schaden ook het vertrouwen in de overheid. Sinds 2021 staan cyberrisico's bovenaan de lijst van de grootste bedrijfsrisico's volgens experts in risicomanagement. Dit geldt ook voor gemeenten. Zij beheren en verwerken namelijk veel persoonsgegevens en hun dienstverlening is steeds afhankelijker van de beschikbaarheid van digitale systemen. De kwetsbaarheid van gemeenten is gebleken uit nieuwsberichten en recente onderzoeken van rekenkamers.

Aanleiding

In het jaarplan 2024 is opgenomen dat de gecombineerde rekenkamers van Ooststellingwerf, Weststellingwerf en Opsterland (OWO) voornemens zijn om één nieuw onderzoek op te starten in 2024. In het najaar van 2023 hebben alle fracties van de drie gemeenteraden de mogelijkheid gekregen om via een online formulier onderwerpen voor onderzoek aan te dragen. De aangedragen onderwerpen zijn door de rekenkamer gecategoriseerd en met elke gemeenteraad afzonderlijk besproken in de zogenaamde najaarsoverleggen.

Het onderwerp informatiebeveiliging werd door zowel de drie gemeenteraden als de rekenkamer als een interessant onderwerp voor onderzoek aangemerkt.

Doelstelling en afbakening

Met dit onderzoek wil de rekenkamer in beeld brengen of de informatiebeveiliging adequaat is georganiseerd en geborgd bij de OWO-gemeenten.

Vraagstelling

De centrale onderzoeksvraag is:

Is de informatiebeveiliging van de OWO gemeenten adequaat georganiseerd en geborgd?

De centrale vraag is vertaald naar de volgende deelvragen:

► Beleid: wat is het beleid van de OWO-gemeenten op het gebied van informatieveiligheid; voldoet dit aan actuele standaarden (als de BIO en ENSIA) en zijn de gemeenten voorbereid op de BIO2 en ENSIA2?
► Uitvoering: Hoe wordt het Informatieveiligheidsbeleid uitgevoerd op bestuurlijk, organisatorisch, technisch, proces- en medewerkersniveau? Worden hierbij PEN-testen ingezet, zoja welke?
► Zijn gegevens bij de OWO gemeenten voldoende beschermd tegen toegang door onbevoegden? In hoeverre wordt getoetst of

de organisatie ‘in control’ is op het gebied van informatiebeveiliging en welke instrumenten worden hierbij gebruikt?
► Is de continuïteit van de gemeentelijke dienstverlening gewaarborgd in geval van grootschalige uitval of verstoring van ICT en hoe is dat geregeld? Weet de organisatie hoe te handelen bij een (ernstig) informatiebeveiligingsincident, hoe ziet het incidentmanagementproces eruit en wordt dit in de praktijk geoefend?
► Hoe gaan de OWO gemeenten om met risico’s en incidenten op het gebied van informatieveiligheid en in hoeverre toont de organisatie lerend vermogen (PDCA cyclus)?
► Bewustwording: hoe zorgen de OWO gemeenten voor bewustwording voor informatiebeveiliging bij medewerkers, bestuur, raad en samenwerkingspartners?
► Zijn de rollen en taken op het gebied van informatiebeveiliging voor medewerkers en het management duidelijk en hoe wordt er gestuurd in de gemeentelijke organisatie?
► Betrokkenheid raad: Hoe is de raad betrokken bij het informatieveiligheidsbeleid en is dit voldoende om de kaderstellende en controlerende rol te kunnen vervullen?

Aanpak

1. Kick-off en startbijeenkomst: presentatie van de onderzoeksopzet aan de raden van de OWO-gemeenten en startbijeenkomst met ambtelijk betrokkenen;
2. Beleidsonderzoek: Documentstudie naar het vastgelegde beleid m.b.t. informatieveiligheid, inrichting van de technische beveiliging, de aandacht voor het veiligheidsbewustzijn en de voorbereiding op de implementatie van nieuwe wet- en regelgeving. Interviews met sleutelpersonen zoals de portefeuillehouder in de colleges, gemeentesecretarissen, FG, CISO, Privacy officers, verantwoordelijken voor de technische beveiliging bij A&I, etc.
3. Verdieping in de praktijk: In focusgroepen inventariseren wij in hoeverre er in de verschillende beleidsdomeinen aandacht is voor het realiseren van de gewenste informatieveiligheid. We gaan uit van drie focusgroepen voor de OWO organisatie en drie raadsbijeenkomsten; één in elke gemeente.
4. Analyse en rapportage: In onze eindrapportage beschrijven wij de uitkomsten uit de verschillende fasen van het onderzoek en trekken daaruit algemene conclusies. De rapportage bevat een bestuurlijke samenvatting met concrete conclusies en aanbevelingen.

Planning en uitvoering

Het onderzoek wordt uitgevoerd in samenwerking met PBLQ .
Het onderzoek zal in oktober van start gaan. De rekenkamer verwacht het onderzoeksrapport in het eerste kwartaal van 2025 te kunnen aanbieden aan de gemeenteraden.