REKENKAMER
ERMELO | HARDERWIJK | ZEEWOLDE

Opzet en aanpak voor onderzoek lokale weerbaarheid

Gemeenten Ermelo, Harderwijk en Zeewolde

Aanleiding

Gemeenten zijn in toenemende mate afhankelijk van digitale systemen voor hun primaire dienstverlening aan inwoners en ondernemers. Deze digitale afhankelijkheid komt tot uitdrukking in uiteenlopende gemeentelijke processen, zoals het verwerken van uitkeringen, belastingen en het gebruik van persoonsgegevens en andere gevoelige gegevens. De urgentie van informatiebeveiliging is de afgelopen jaren verder toegenomen, mede doordat het digitale dreigingslandschap volgens het Cybersecuritybeeld Nederland 2025 complexer en onvoorspelbaarder wordt. Cyberaanvallen worden steeds geavanceerder, digitale afhankelijkheden nemen toe en zowel cybercriminelen als statelijke actoren richten zich op Nederlandse doelwitten. Recente incidenten, zoals de hack in Epe in maart 2026 waarbij 550.000 bestanden zijn gelekt, en het incident bij Odido waarbij ongeveer 6 miljoen mensen werden geraakt, onderstrepen dat cyberaanvallen grote gevolgen kunnen hebben. Voor gemeenten als Ermelo, Harderwijk en Zeewolde is de vraag daarom niet óf informatiebeveiliging belangrijk is, maar of de bestuurlijke, organisatorische en technische maatregelen voldoende samenhangen om cyberrisico's te beheersen.

Verkenning gemeenten Ermelo, Harderwijk en Zeewolde

De betrouwbaarheid, beschikbaarheid en vertrouwelijkheid van gemeentelijke informatie zijn geen uitsluitend technische aangelegenheid, maar raken direct aan publieke dienstverlening en bestuurlijke continuïteit. De Baseline Informatiebeveiliging Overheid (BIO), het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen, vormt hierbij een belangrijk normenkader. De BIO2 legt hierbij nadrukkelijker de focus op een risicogerichte benadering en het afstemmen van maatregelen op specifieke risico's. Daarnaast vraagt de komst van de Cyberbeveiligingswet, waarmee de NIS2-richtlijn wordt omgezet in nationale wetgeving, om verdere voorbereiding op digitale weerbaarheid waar de Rijksoverheid organisaties toe oproept. Op dit moment werkt de gemeenschappelijke regeling Meerinzicht (Regelt onder andere ICT en veel bedrijfsvoering processen voor de drie gemeenten) aan een bedrijfscontinuïteitsplan voor de gemeenten Ermelo, Harderwijk en Zeewolde. De implementatie van het plan zal naar verwachting in Q1 2027 plaatsvinden. Daarna kan de rekenkamer onderzoeken in hoeverre het geïmplementeerde beleid de organisaties technisch voldoende weerbaar maakt en in hoeverre de processen op orde zijn om gegevens en de continuïteit van gemeentelijke dienstverlening te beschermen.

Doel van het onderzoek

Tegen de achtergrond van toenemende digitalisering, groeiende cyberdreigingen en oplopende geopolitieke spanningen is het van belang dat de gemeenten voldoende (lokaal) weerbaar zijn tegen cyberaanvallen en de gevolgen daarvan. Een geslaagde cyberaanval kan namelijk leiden tot datalekken, verstoring van gemeentelijke processen, financiële schade, reputatieschade en verlies van vertrouwen van inwoners in de overheid. Het doel van het onderzoek is om de gemeenteraden inzicht te geven in de mate waarin de gemeenten hun informatiebeveiliging aantoonbaar op orde hebben. Hierbij gaat het om de vraag of risico's in beeld zijn, of er passende maatregelen zijn getroffen, of kwetsbaarheden tijdig worden opgemerkt en of de gemeenten voldoende voorbereid zijn op incidenten en herstel na een aanval, inclusief het continueren van kritieke processen. De centrale onderzoeksvraag luidt:

In hoeverre zijn de gemeenten Ermelo, Harderwijk en Zeewolde bestuurlijk, organisatorisch en technisch voldoende weerbaar tegen cyberaanvallen en in hoeverre zijn de preventieve, detectieve, corrigerende en herstellende maatregelen aantoonbaar op orde om persoonsgegevens, kritische processen en de continuïteit van gemeentelijke dienstverlening te beschermen?

Onderzoeksvragen

1. **Risicobeeld en beleid**
   Hebben de gemeenten hun belangrijkste informatiebeveiligingsrisico's, kwetsbaarheden en kritische processen voldoende in beeld en is op basis daarvan actueel beleid geformuleerd?

2. **Governance en verantwoordelijkheden**
   Hoe zijn rollen, verantwoordelijkheden en besluitvorming rond informatiebeveiliging georganiseerd, bijvoorbeeld rond college, directie, CISO, FG, privacy officer, proceseigenaren en leveranciers?

3. **Normenkader en naleving**
   In hoeverre sluiten beleid, processen en maatregelen aan op relevante kaders zoals BIO/BIO2, AVG, ENSIA en toekomstige verplichtingen vanuit de Cyberbeveiligingswet/NIS2?

4. **Kritische processen en systemen**
   Welke processen en systemen worden door de gemeenten als kritisch beschouwd en hoe worden deze beschermd?

5. **Preventieve maatregelen**
   Welke preventieve maatregelen zijn getroffen om ongeautoriseerde toegang, datalekken en verstoring van systemen te voorkomen, bijvoorbeeld rond autorisatiebeheer, multifactor-authenticatie, patchmanagement, netwerksegmentatie, back-ups, logging en leveranciersbeheer?

6. **Bewustwording en menselijk handelen**
   Hoe worden bestuurders, medewerkers en eventueel raadsleden ondersteund en getraind in veilig digitaal werken en wordt de effectiviteit van bewustwordingsmaatregelen, bijvoorbeeld rond phishing en social engineering, gemeten?

7. **Monitoring, detectie en opvolging**
   Hoe monitoren de gemeenten hun systemen op kwetsbaarheden en incidenten en hoe worden signalen, meldingen en bevindingen opgevolgd?

8. **Testen en verbeteren**
   Worden periodiek penetratietesten, kwetsbaarheidsscans, audits, tabletop-oefeningen of andere beveiligingstesten uitgevoerd en leiden de uitkomsten aantoonbaar tot verbetermaatregelen?

9. **Continuïteit van kritieke gemeentelijke dienstverlening**
   In hoeverre hebben de gemeenten bepaald welke gemeentelijke processen kritisch zijn voor de dienstverlening aan inwoners en ondernemers, welke continuïteitseisen daarbij gelden en welke nood-, uitwijk- en herstelmaatregelen zijn ingericht om deze processen tijdens of na een cyberincident voort te zetten?

10. **Bescherming van persoonsgegevens**
    Hoe borgen de gemeenten de bescherming van persoonsgegevens, met name in processen waarin gevoelige gegevens worden verwerkt, zoals het sociaal domein, burgerzaken en handhaving?

11. **Informatiepositie van de gemeenteraad**
    Op welke wijze worden de gemeenteraden geïnformeerd over informatiebeveiligingsrisico's, incidenten, verbetermaatregelen en resterende risico's, en is deze informatie toereikend om de kaderstellende en controlerende rol te vervullen?

12. **Middelen en prioritering**
    Zijn de beschikbare middelen, capaciteit en deskundigheid passend bij het risicoprofiel van de gemeenten en hoe worden investeringen in informatiebeveiliging bestuurlijk afgewogen?

13. **Lerend vermogen**
    In hoeverre leren de gemeenten van incidenten, audits, ENSIA-uitkomsten, externe

dreigingsinformatie en voorbeelden uit andere gemeenten en hoe wordt dit vertaald naar structurele verbetering?

Afbakening

Het onderzoek richt zich op de bestuurlijke, organisatorische en technische weerbaarheid van de gemeenten tegen cyberdreigingen. Dit onderzoek hoeft niet zelf een live hack of technische aanval uit te voeren.

Randvoorwaarden onderzoek

Het onderzoek wordt uitbesteed aan een (nog te selecteren) onderzoeksbureau. Om de offertes te kunnen vergelijken en de zorgvuldigheid te borgen, hanteert de rekenkamer (conform haar onderzoeksprotocol) de volgende randvoorwaarden:

- **Belangenverstrengeling en onafhankelijkheid:** De bureaus worden gevraagd om aan te geven of zij op het desbetreffende terrein (informatiebeveiliging) al werkzaam zijn of waren voor de gemeenten Ermelo, Harderwijk en/of Zeewolde. Bij een risico op belangenverstrengeling kan de opdracht niet aan het desbetreffende bureau worden verstrekt.
- **Eindverantwoordelijkheid en dossier:** De eindverantwoordelijkheid voor de uitvoering en rapportage blijft bij de rekenkamer. De externe onderzoekers rapporteren uitsluitend aan de rekenkamer en doen geen mededelingen over het onderzoek aan derden. Na afloop draagt het bureau het volledige onderzoeksdossier over aan de rekenkamer, die dit bewaart conform de termijnen van de Archiefwet (deze dossiers zijn niet toegankelijk voor derden).
- **Normenkader en start:** Om normatieve uitspraken te kunnen doen, hanteren de onderzoekers een normenkader dat vooraf ter vaststelling aan de rekenkamer wordt voorgelegd. Bij de start van het onderzoek vindt een gezamenlijke bijeenkomst plaats met de ambtelijke organisatie (waaronder de gemeentesecretaris) om inhoud, proces en werkafspraken af te stemmen.
- **Lerend onderzoek:** De rekenkamer zet bewust in op een reflectieve en verbetergerichte onderzoeksvorm waarin het lerend effect centraal staat. In de offerte ziet de rekenkamer graag goede voorstellen voor deze lerende en vooruitkijkende aanpak tegemoet.
- **Werkwijze bij interviews:**
    - Geïnterviewden ontvangen voorafgaand aan het gesprek de thema's die aan de orde komen.
    - De gesprekken zijn vertrouwelijk; er wordt een verslag op hoofdlijnen gemaakt (geen woordelijke weergave).
    - Binnen twee weken na het interview krijgt de respondent het verslag ter autorisatie voorgelegd.
    - De verslagen dienen als vertrouwelijk werkmateriaal, worden niet openbaar gemaakt, maar maken wél deel uit van het af te sluiten onderzoeksdossier dat volgens de Archiefwet wordt bewaard.
    - Een lid of de secretaris van de rekenkamer kan desgewenst als toehoorder bij de interviews aanwezig zijn.
- **Rapportage en wederhoor:** Het proces van rapporteren en wederhoor verloopt in strikte stappen:
    - *Ambtelijk wederhoor:* Er wordt eerst een conceptrapport opgesteld met uitsluitend het normenkader en de nota van bevindingen (dus *zonder* conclusies en aanbevelingen). De ambtelijke organisati krijgt minimaal twee weken de tijd om dit op feitelijke onjuistheden te controleren.
    - *Bestuurlijk wederhoor:* Daarna volgt een eindrapport mét conclusies en aanbevelingen, dat voor een bestuurlijke reactie aan de colleges van B&W wordt voorgelegd, eveneens met een responstermijn van minimaal twee weken.
- **Specifiek voor informatiebeveiliging:** Eventuele technische kwetsbaarheden die tijdens het onderzoek aan het licht komen, worden niet openbaar in de rapportages beschreven, maar uitsluitend vertrouwelijk teruggekoppeld aan de drie gemeenten en Meerinzicht.
- **Afronding en evaluatie:** Het onderzoeksbureau houdt rekening met ten minste één presentatie van het definitieve eindrapport in de raden of raadscommissies. Na afloop van het traject vindt er mogelijk een gezamenlijke evaluatie plaats over het onderzoeksproces en de samenwerking.

De rekenkamer stelt de volgende randvoorwaarden:

- Om normatieve uitspraken te kunnen doen hanteren de onderzoekers een normenkader, dat vooraf ter vaststelling aan de rekenkamer wordt voorgelegd.
- Eventuele technische kwetsbaarheden worden niet openbaar beschreven, maar vertrouwelijk teruggekoppeld aan de betrokken gemeenten.
- Er wordt een gezamenlijke startbijeenkomst belegd met de rekenkamer en de ambtelijke organisatie. De onderzoeksopzet, het normenkader en de werkafspraken worden hierin besproken.
- Het onderzoeksbureau houdt rekening met ten minste één presentatie van het eindrapport in de raad of raadscommissie.
- Het onderzoek is met name lerend bedoeld; in de aanpak van het onderzoek ziet de rekenkamer graag goede voorstellen daarvoor tegemoet.
- Van interviews wordt een schriftelijk verslag gemaakt dat ter autorisatie aan de respondent(en) wordt voorgelegd. Na afloop van het onderzoek worden deze verslagen niet bewaard.
- De aanpak moet realistisch gepland worden en passen bij de planning van de rekenkamer.
- Naast diverse overleg- en afstemmingsmomenten wordt rekening gehouden met een conceptnota en een eindrapport, inclusief een moment voor ambtelijk en bestuurlijk wederhoor.

De rekenkamer ontvangt bij interesse van het onderzoeksbureau graag een offerte (Uiterlijk 29 september) van maximaal 3 pagina’s, inclusief een specificatie van de geraamde kosten voor het onderzoek, op basis van de verwachte inzet van uren en het bijbehorende tarief. Bij interesse vanuit de rekenkamer wordt er een moment gepland voor een digitale pitch.

Planning

Onderzoeksfase	Periode
Offertetraject	Q3 2026
Selectie	Q4 2026
Startbijeenkomst en normenkader	Q2 2027
Uitvoering onderzoek	Q2 2027
Ambtelijk wederhoor	Q3 2027
Bestuurlijk wederhoor	Q3 2027
Definitief rapport	Q4 2027
Aanbieding aan raden	Q4 2027

Voor vragen over de opdracht kunt u contact opnemen via rekenkamerehz@ermelo.nl