

Onderzoeksvragen 2025

1. Algemene informatieveiligheid

- Heeft de gemeente op informatieveiligheid de risico's voldoende in kaart gebracht en op basis daarvan beleid geformuleerd?
- Hoe wordt de informatieveiligheid binnen de gemeente georganiseerd en welke maatregelen zijn er genomen om de veiligheid van gevoelige gegevens te waarborgen?
- Op welke wijze worden de gemeenteraden geïnformeerd over de risico's en beheersingsmaatregelen? En wat is wenselijk in het delen van dergelijke informatie?
- In hoeverre voldoet de informatieveiligheid van de gemeente aan de relevante wet- en regelgeving, zoals de Algemene verordening gegevensbescherming (AVG) en de Wet beveiliging netwerk- en informatiesystemen (Wbni)?
- Welke procedures en beleidsmaatregelen zijn er voor het beheer van gebruikersrechten en toegangscontrole tot kritieke informatiesystemen?

2. Beveiliging van kritische systemen

- Welke informatiesystemen worden als 'kritisch' beschouwd voor de werking van de gemeente, en hoe wordt de beveiliging van deze systemen gewaarborgd?
- Welke risico's worden er gelopen als de kritische systemen door ongeautoriseerde beïnvloeding van buitenaf uitvallen?
- Wat zijn de kwetsbaarheden in de bestaande informatiesystemen die het mogelijk maken om in te breken of ongeautoriseerde toegang te verkrijgen?
- Hoe worden de systemen gemonitord op potentiële veiligheidsincidenten en welke mechanismen zijn er voor incidentdetectie en -respons?

3. Risicoanalyse en dreigingen

- Welke interne en externe dreigingen worden momenteel geanalyseerd en beheerd om inbreuken in informatiesystemen te voorkomen?
- In hoeverre worden risico's zoals social engineering, phishing-aanvallen, malware-infecties en andere vormen van cyberaanvallen in kaart gebracht en tegengegaan?

4. Testen van infiltratie

- Is er een periodieke penetratietest of red-teaming uitgevoerd om de kwetsbaarheden van de informatiesystemen te identificeren en de effectiviteit van de beveiliging te testen?
- Welke incidenten of beveiligingslekken zijn er in de afgelopen jaren geconstateerd, en hoe zijn deze opgelost? Hoe wordt er bijvoorbeeld bij een datalek gecommuniceerd met de mogelijk betrokkenen binnen en buiten het gemeentehuis?

5. Opleiding en bewustwording van personeel

- Hoe worden medewerkers van de gemeente opgeleid in het herkennen van beveiligingsrisico's, zoals phishing en social engineering-aanvallen?
- Wat is de frequentie en effectiviteit van de trainingen die medewerkers ontvangen met betrekking tot informatieveiligheid?

6. Beveiliging van gegevens en privacy

- Hoe wordt de privacy van persoonsgegevens gewaarborgd binnen de informatiesystemen van de gemeente?
- Zijn er gegevensversleuteling en veilige communicatiekanalen aanwezig voor het uitwisselen van gevoelige informatie?

7. Incidentmanagement en crisiscommunicatie

- Hoe is het incidentmanagementproces ingericht voor het geval van een datalek of cyberaanval?
- Welke procedures zijn er voor crisiscommunicatie en hoe snel kunnen kwetsbaarheden worden geadresseerd?

8. Kosten beveiligingsmaatregelen

- Welke eenmalige en structurele kosten worden er gemaakt voor het beheren van risico's op gebied van informatieveiligheid en bescherming kritische processen en hoe verhouden zich die onderling en tot soortgelijke gemeenten?
-