Handboek voor het inrichten van de NIS2-Richtlijn bij de Gemeente

Dit handboek geeft handvatten van hoe te werk gaan bij de gedeelde taken die bij een gemeente horen. De Gemeenteraad is dan de baas over de gemeente maar moeten volgens afgesproken structuur verlopen.

Contents

Verantwoordelijkheid van Gemeenteraad, Burgemeester, Gemeentesecretaris/Algemeen Directeur

In het kader van de NIS2-richtlijn en de verantwoordelijkheden van de gemeentelijke overheid voor cyberbeveiliging, zijn de rollen en verantwoordelijkheden als volgt verdeeld:

Verantwoordelijkheid en Aansprakelijkheid

Gemeenteraad:

- De gemeenteraad is het hoogste bestuursorgaan van de gemeente en stelt het algemene beleid vast. De raad heeft de verantwoordelijkheid om ervoor te zorgen dat er een adequaat beleid voor cyberbeveiliging is, inclusief de naleving van de NIS2-richtlijn.

Burgemeester:

- De burgemeester heeft een belangrijke rol in de handhaving van de openbare orde en veiligheid, inclusief digitale veiligheid. De burgemeester kan worden gezien als de uitvoerder van het beleid dat door de gemeenteraad is vastgesteld. Bij incidenten of crises kan de burgemeester snel maatregelen nemen.

Gemeentesecretaris/Algemeen Directeur:

- De gemeentesecretaris (ook wel de algemeen directeur genoemd) is verantwoordelijk voor de dagelijkse leiding van de ambtelijke organisatie. Deze persoon zorgt ervoor dat het beleid, inclusief maatregelen voor cyberbeveiliging en naleving van de NIS2-richtlijn, daadwerkelijk wordt geïmplementeerd en uitgevoerd.

Aansprakelijkheid bij Nieuwe Verkiezingen

Wanneer er nieuwe verkiezingen zijn, kan de verantwoordelijkheid en aansprakelijkheid voor de naleving van de NIS2-richtlijn als volgt worden beschouwd:

1. Gemeenteraad: Blijft als orgaan verantwoordelijk voor het vaststellen van het beleid, ongeacht wie er zitting heeft. De nieuwe raad neemt de verantwoordelijkheid over van de vorige raad.

2. Burgemeester: Blijft verantwoordelijk voor de uitvoering van het beleid en de handhaving van de openbare orde en veiligheid, inclusief digitale veiligheid, totdat een nieuwe burgemeester wordt benoemd. De burgemeester heeft een continue verantwoordelijkheid.

3. Gemeentesecretaris/Algemeen Directeur: Blijft verantwoordelijk voor de operationele uitvoering van het beleid, inclusief de maatregelen voor cyberbeveiliging. Deze rol is doorgaans niet direct afhankelijk van verkiezingen, omdat de gemeentesecretaris een ambtelijke functie bekleedt.

Gedeelde Aansprakelijkheid

In de praktijk is de verantwoordelijkheid voor naleving van de NIS2-richtlijn vaak gedeeld:

- Strategische Verantwoordelijkheid: De gemeenteraad en burgemeester delen de strategische verantwoordelijkheid voor het vaststellen en handhaven van het beleid.

- Tactische Verantwoordelijkheid: De burgemeester en gemeentesecretaris zijn verantwoordelijk voor de tactische uitvoering van het beleid.

- Operationele Verantwoordelijkheid: De gemeentesecretaris zorgt voor de operationele uitvoering en naleving van het beleid door de ambtelijke organisatie.

Door deze stappen te volgen, kan de gemeente de naleving van de NIS2-richtlijn waarborgen en de digitale weerbaarheid versterken.

Advies

Voor de gemeente is het cruciaal om een duidelijke governance-structuur te hebben waarbij de verantwoordelijkheden en bevoegdheden voor cyberbeveiliging en naleving van de NIS2-richtlijn expliciet zijn vastgelegd. Dit helpt niet alleen bij de continuïteit tijdens verkiezingen, maar zorgt er ook voor dat er altijd duidelijkheid is over wie verantwoordelijk is voor welke aspecten van cyberbeveiliging.

Daarnaast is het belangrijk om regelmatig te evalueren en rapporteren over de naleving van de NIS2-richtlijn en de algehele cyberbeveiligingsstatus. Dit zorgt ervoor dat de gemeenteraad, de burgemeester en de gemeentesecretaris allemaal goed geïnformeerd zijn en dat de gemeente als geheel 'in control' is.

Bob-sessie over Bewustwording van de NIS2 op Strategisch, Tactisch en Operationeel Niveau voor de Gemeenteraad

1. Inleiding

Doel van de sessie:

Het doel van deze BOB-sessie is om de gemeenteraad bewust te maken van de NIS2-richtlijn en de implicaties ervan op strategisch, tactisch en operationeel niveau. Tevens zullen we bespreken welke vragen aan het college van Burgemeester en Wethouders (B&W) gesteld moeten worden om te verzekeren dat de gemeente in control is.

2. Beeldvorming (B)

Strategisch Niveau:

- Wat is de NIS2-richtlijn?

- De NIS2-richtlijn is een Europese regelgeving die de beveiliging van netwerk- en informatiesystemen van essentiële en belangrijke diensten versterkt.

- Waarom is de NIS2-richtlijn belangrijk voor de gemeente?

- De richtlijn verplicht gemeenten om maatregelen te nemen om hun netwerk- en informatiesystemen tegen incidenten te beschermen, wat cruciaal is voor de continuïteit van gemeentelijke diensten.

- Wat zijn de gevolgen van niet-naleving?

- Niet-naleving kan leiden tot boetes, reputatieschade en verhoogde kwetsbaarheid voor cyberaanvallen.

Tactisch Niveau:

- Welke systemen en processen vallen onder de NIS2?

- Alle kritieke IT-systemen en processen die essentieel zijn voor de dienstverlening van de gemeente.

- Hoe wordt de naleving van de NIS2 gemeten en gecontroleerd?

- Door regelmatige audits, risicobeoordelingen en nalevingsrapporten.

- Welke rol spelen verschillende afdelingen in de naleving?

- IT, juridische zaken, HR en de afdelingen die verantwoordelijk zijn voor de levering van essentiële diensten.

Operationeel Niveau:

- Wat zijn de dagelijkse implicaties voor gemeentelijke medewerkers?

- Medewerkers moeten zich houden aan strikte beveiligingsprotocollen, zoals wachtwoordbeheer en meldingsprocedures voor incidenten.

- Welke technische maatregelen moeten worden geïmplementeerd?

- Multifactor authenticatie, regelmatige software-updates, en versleuteling van gegevens.

- Hoe worden incidenten gedetecteerd en gemeld?

- Door middel van monitoringtools en een duidelijk incidentresponsplan.

3. Oordeelsvorming (O)

Strategisch Niveau:

- Hoe past de NIS2 in de bredere strategie van de gemeente voor digitale transformatie?

- NIS2 moet worden gezien als een essentieel onderdeel van de digitale transformatie en risicobeheerstrategie.

- Welke middelen en budget zijn nodig voor NIS2-naleving?

- Inzicht in de benodigde middelen voor technologie, personeel en training.

Tactisch Niveau:

- Hoe zorgt de gemeente voor voortdurende naleving van de NIS2?

- Door het instellen van een compliance officer en het regelmatig herzien van beveiligingsmaatregelen.

- Wat zijn de belangrijkste risico's die de gemeente moet beheren?

- Identificatie van de meest kritieke risico's en de ontwikkeling van plannen om deze te mitigeren.

Operationeel Niveau:

- Hoe wordt de training en bewustwording van medewerkers gewaarborgd?

- Regelmatige trainingssessies en bewustwordingscampagnes.

- Welke procedures zijn er voor incidentrespons en herstel?

- Een gedetailleerd incidentresponsplan en regelmatige oefeningen om de paraatheid te testen.

4. Besluitvorming (B)

Voorstellen en Amendementen:

1. Voorstel: Instellen van een NIS2-coördinator binnen de gemeente die verantwoordelijk is voor de naleving van de richtlijn.

- Amendement: De NIS2-coördinator rapporteert rechtstreeks aan de gemeentesecretaris en presenteert kwartaalrapporten aan de raad.

2. Voorstel: Ontwikkelen van een jaarlijks auditprogramma om de naleving van de NIS2-richtlijn te waarborgen.

- Amendement: De resultaten van de audits worden gedeeld met alle relevante afdelingen en besproken in een jaarlijkse veiligheidsreview.

3. Voorstel: Implementeren van een continu trainingsprogramma voor alle gemeentemedewerkers over cyberbeveiliging en NIS2-naleving.

- Amendement: Trainingen moeten ten minste halfjaarlijks plaatsvinden en er moet een certificeringsproces worden opgezet om de voltooiing te bevestigen.

5. Vragen aan het College van B&W

Strategisch Niveau:

1. Hoe integreert de gemeente de naleving van de NIS2-richtlijn in haar bredere digitale strategie?

2. Welke stappen zijn er genomen om de strategische risico's van cyberaanvallen te verminderen?

Tactisch Niveau:

1. Welke afdelingen en functies zijn verantwoordelijk voor de naleving van de NIS2-richtlijn?

2. Hoe vaak worden risicobeoordelingen en nalevingsaudits uitgevoerd?

Operationeel Niveau:

1. Hoe worden gemeentelijke medewerkers getraind in de vereisten en procedures van de NIS2-richtlijn?

2. Wat zijn de protocollen voor het melden en afhandelen van beveiligingsincidenten?

6. Conclusie

Samenvatting:

Het is cruciaal dat de gemeente een uitgebreide strategie en gedetailleerde procedures implementeert om aan de NIS2-richtlijn te voldoen. Door het stellen van de juiste vragen en het implementeren van duidelijke voorstellen en amendementen, kan de gemeenteraad ervoor zorgen dat de gemeente goed voorbereid is op de uitdagingen van cyberbeveiliging en continuïteit van dienstverlening.

Actiepunten:

- Aanstellen van een NIS2-coördinator.

- Ontwikkelen en implementeren van een auditprogramma.

- Opzetten van een continu trainingsprogramma.

Governance-structuur voor Naleving van de NIS2-Richtlijn in een Gemeente

1. Gemeenteraad

Rol:

- Vaststellen van het strategische beleid voor cyberbeveiliging en naleving van de NIS2-richtlijn.

- Toezicht houden op de uitvoering van het beleid door de burgemeester en gemeentesecretaris.

Verantwoordelijkheden:

- Goedkeuren van budgetten en middelen voor cyberbeveiligingsinitiatieven.

- Evalueren van jaarlijkse rapporten over de staat van cyberbeveiliging en naleving van de NIS2-richtlijn.

- Ingrijpen bij ernstige incidenten of niet-naleving door aanvullende maatregelen te eisen.

2. Burgemeester

Rol:

- Handhaving van het vastgestelde beleid en coördinatie van de strategische en tactische respons bij cyberincidenten.

- Vertegenwoordigen van de gemeente bij regionale en nationale cyberbeveiligingsinitiatieven.

Verantwoordelijkheden:

- Leiding geven aan de uitvoering van het cyberbeveiligingsbeleid.

- Samenwerken met de gemeentesecretaris om de implementatie van maatregelen te waarborgen.

- Rapporteren aan de gemeenteraad over de voortgang en eventuele problemen met betrekking tot cyberbeveiliging.

3. Gemeentesecretaris (Algemeen Directeur)

Rol:

- Dagelijkse leiding over de ambtelijke organisatie en operationele uitvoering van het cyberbeveiligingsbeleid.

- Fungeren als schakel tussen het strategische beleid van de gemeenteraad en de operationele uitvoering.

Verantwoordelijkheden:

- Implementeren van de vastgestelde cyberbeveiligingsmaatregelen en naleving van de NIS2-richtlijn.

- Toezicht houden op de ICT-afdeling en het Information Security Management Team (ISMT).

- Regelmatig rapporteren aan de burgemeester over de status van de cyberbeveiliging en naleving van de NIS2-richtlijn.

4. Information Security Management Team (ISMT)

Rol:

- Tactische en operationele coördinatie van alle aspecten van informatiebeveiliging binnen de gemeente.

Verantwoordelijkheden:

- Uitvoeren van risicoanalyses en kwetsbaarheidsbeoordelingen.

- Ontwikkelen en implementeren van beveiligingsmaatregelen.

- Beheren van incidentrespons en herstelactiviteiten.

- Rapporteren aan de gemeentesecretaris over incidenten, risico's en beveiligingsstatus.

5. IT-afdeling

Rol:

- Implementeren van technische beveiligingsmaatregelen en dagelijkse IT-operaties.

Verantwoordelijkheden:

- Uitvoeren van technische beveiligingsmaatregelen zoals firewalls, antivirus, en encryptie.

- Beheren van toegangscontroles en authenticatiesystemen.

- Uitvoeren van regelmatige back-ups en herstelprocedures.

- Monitoren van netwerken en systemen op verdachte activiteiten.

6. Externe Auditors

Rol:

- Onafhankelijke beoordeling van de naleving van de NIS2-richtlijn en de effectiviteit van de beveiligingsmaatregelen.

Verantwoordelijkheden:

- Uitvoeren van periodieke audits en penetratietests.

- Rapporteren van bevindingen aan de gemeenteraad en gemeentesecretaris.

- Aanbevelen van verbeteringen op basis van auditresultaten.

Governance-structuur Overzicht

```
Gemeenteraad
    |
    | --- Strategisch beleid
    |
Burgemeester
    |
    | --- Handhaving en coördinatie
    |
Gemeentesecretaris (Algemeen Directeur)
    |
    | --- Operationele uitvoering
    |
Information Security Management Team (ISMT)
    |
    | --- Tactische en operationele coördinatie
    |
IT-afdeling
    |
    | --- Technische implementatie
    |
Externe Auditors
    |
```

| --- Onafhankelijke beoordeling

```

## Vragen aan het College van B&W

Strategisch Niveau:

1. Hoe integreert de gemeente de naleving van de NIS2-richtlijn in haar bredere digitale strategie?

2. Welke stappen zijn er genomen om de strategische risico's van cyberaanvallen te verminderen?

Tactisch Niveau:

1. Welke afdelingen en functies zijn verantwoordelijk voor de naleving van de NIS2-richtlijn?

2. Hoe vaak worden risicobeoordelingen en nalevingsaudits uitgevoerd?

Operationeel Niveau:

1. Hoe worden gemeentelijke medewerkers getraind in de vereisten en procedures van de NIS2-richtlijn?

2. Wat zijn de protocollen voor het melden en afhandelen van beveiligingsincidenten?

Door deze governance-structuur en vragen te hanteren, kan de gemeenteraad ervoor zorgen dat de gemeente goed voorbereid is op de naleving van de NIS2-richtlijn en effectief kan reageren op cyberdreigingen.
```