Gemeente Roosendaal

Raadsvraag (art. 37)	Gesteld door: **Roosendaalse Lijst VLP Roosendaal CDA**
Datum	27 september 2024
Onderwerp	144-2024 Is de gemeente Roosendaal klaar voor naleven van extra wetgeving op gebied van cyber-Informatiebeveiliging (Nis2)
Portefeuillehouder	College B&W

De fractie heeft de volgende vragen:

Vanuit Europa komt veel regelgeving aan op gebied van digitale veiligheid aan specifiek voor lokale overheden zoals gemeenten. Met name de richtlijn Nis2 is bedoeld om cyberbeveiliging en digitale weerbaarheid te vergroten. Lokale overheden krijgen een wettelijke zorgverplichting voor digitale veiligheid en zullen zij voldoende budget moeten reserveren voor de implementatie van de Cyberbeveiligingswet.

De fracties van de Roosendaalse Lijst, VLP Roosendaal en CDA Roosendaal hebben hierover de volgende vragen:

1. Hoe gaat de gemeente Roosendaal om met informatiebeveiliging en hoe toegankelijk en betrouwbaar is het hierin?

2. Wat is de stand van zaken aangaande te treffen maatregelen om de benoemde Nis2 wetgeving optimaal te kunnen naleven (IB-governance, budget, capaciteit en te treffen technische maatregelen om cyberaanvallen te voorkomen alsmede controles hierop)?

3. Wat zijn de grootste risico's op het gebied van cyberdreiging voor de gemeente Roosendaal in relatie tot de continuïteit van de gemeentelijke dienstverlening en hoe wordt die aangepakt? Graag een toelichting.

4. Welke controles worden achteraf uitgevoerd om optimale verantwoording te kunnen afleggen?

5. Wordt er op VNG-niveau samengewerkt om cyberwetgeving ook voor de gemeente Roosendaal optimaal te laten landen? Ook hier graag een toelichting.

Namens de fractie(s) van Roosendaalse Lijst , VLP Roosendaal
CDA

Peter Raijmaekers

Wij beantwoorden de vraag als volgt:

1. Hoe gaat de gemeente Roosendaal om met informatiebeveiliging en hoe toegankelijk en betrouwbaar is het hierin?

De gemeente Roosendaal neemt informatiebeveiliging uiterst serieus.

Periodiek worden assessments uitgevoerd om de volwassenheid van de verschillende systemen te meten en te verbeteren. Denk daarbij aan processen van in- door- en uitstroom van personeel en autorisatieprocessen voor zowel fysieke als logische toegang tot gegevens.

Wij doen geen uitspraken in het openbaar over de exacte inrichting van onze infrastructuur en beveiliging om te voorkomen dat cybercriminelen daar misbruik van kunnen maken.

Graag willen de Chief Information Security Officer (CISO) en een Information Security Officer (ISO) in een besloten bijeenkomst aanvullende informatie verstrekken.

2. Wat is de stand van zaken aangaande te treffen maatregelen om de benoemde Nis2 wetgeving optimaal te kunnen naleven (IB-governance, budget, capaciteit en te treffen technische maatregelen om cyberaanvallen te voorkomen alsmede controles hierop)?

De gemeente Roosendaal volgt de adviezen van de Informatiebeveiligingsdienst van de VNG over de invoering van Baseline Informatiebeveiliging Overheid (versies 1 én 2) en NIS2.

Binnen de Concerncontrol werken een Chief Information Security Officer (CISO) en een Information Security Officer (ISO) voor 1,67 fte op de verschillende deelgebieden van informatiebeveiliging. De functionarissen zijn organisatorisch rechtstreeks onder de algemeen directeur ondergebracht, zodat zij onafhankelijk van en ten behoeve van de diverse organisatie onderdelen kunnen opereren.

De gemeente Roosendaal heeft een palet aan technische hulpmiddelen zoals een Security Operations Center, Intrusion Detection System, Intrusion Prevention System, firewalls, antivirusscanners, anti-spamfilters, Mobile Device Management, Multi-Factor Authenticatie, netwerksegmentering, pen-testen. Afwijkingen worden gemonitord en indien nodig worden maatregelen getroffen.

In samenwerking met de deelnemers van ICT WBW werken we aan een invoeringsdocument NIS2 om elke deelnemer klaar te stomen voor de NIS2.

3. Wat zijn de grootste risico's op het gebied van cyberdreiging voor de gemeente Roosendaal in relatie tot de continuïteit van de gemeentelijke dienstverlening en hoe wordt die aangepakt? Graag een toelichting.

Hoewel de technische hulpmiddelen ons helpen te verweren tegen een groot deel van de cyberaanvallen, blijft de grootste risicofactor de menselijk factor. De aanvallers worden steeds doortrapter en hun technieken zijn steeds moeilijker op te sporen. Continue (bij)scholing van medewerkers is daarom een speerpunt van onze digitale weerbaarheid. Alle medewerkers hebben toegang tot een e-learning omgeving voor cybersecurity en privacy om de medewerkers doorlopend bewust te houden van de tactieken en technieken die door de aanvallers worden gebruikt.

4. Welke controles worden achteraf uitgevoerd om optimale verantwoording te kunnen afleggen?

Periodieke controles op accounts in de Active Directory en periodieke controles op de autorisatie matrices van de bedrijf kritische applicaties. Jaarlijks voeren wij een GAP-analyse uit en leggen wij verantwoording af via de landelijke ENSIA-audit.

5. Wordt er op VNG-niveau samengewerkt om cyberwetgeving ook voor de gemeente Roosendaal optimaal te laten landen? Ook hier graag een toelichting.

De Informatiebeveiligingsdienst van de VNG ondersteunt en faciliteert gemeenten bij de invoering van NIS2. Daar maakt de gemeente Roosendaal zeker gebruik van.

Daarnaast werkt de gemeente Roosendaal samen met de deelnemers van ICT WBW aan een gezamenlijke aanpak voor het gereedmaken voor NIS2.

Wij vertrouwen erop U hiermede voldoende te hebben geïnformeerd.

Hoogachtend,

Burgemeester en wethouders van Roosendaal,

De secretaris, De burgemeester,