gemeente
NOORDOOSTPOLDER

MEMO aan Raad

Aan : De raad van gemeente Noordoostpolder

Van : Burgemeester en wethouders van de gemeente Noordoostpolder

Datum : 19 september 2024

Onderwerp : **NIS2- richtlijn en de Nederlandse Cyberbeveiligingswet**

Beleidsreferentie

- ⇒ Europese en Nederlandse wetgeving op het gebied van informatieveiligheid (NIS2-richtlijn, de Nederlandse uitvoeringswet en de Baseline Informatieveiligheid Overheid (BIO 2.01)
- ⇒ Raadsleden spelen een cruciale rol in het waarborgen van digitale veiligheid en informatiebeveiliging binnen hun gemeente. Het is essentieel dat zij zich bewust zijn van de verplichtingen en actief bijdragen aan de implementatie van de NIS2-richtlijn.

Inleiding

Gemeenten werken samen aan een digitale toekomst die voor iedereen werkt op basis van de Digitale Agenda 2024-2028. De steeds verdergaande digitalisering vraagt om nauwe samenwerking en standaardisatie. Het voorwoord van de agenda verwoord goed waar we nu staan: "*De digitale samenleving is nog steeds verrassend, innovatief, bruisend en verrijkend. Achter de voorkant van onze telefoon vinden we een wereld van kennis, ervaringen, contacten, cultuur, kennis en uitwisseling. Daarmee kunnen we individueel en samen de hele wereld aan. Maar er komt ook een waaier van minder mooie dingen op ons af. Zoals cybercrime, desinformatie, discriminatie, democratische ondermijning, polarisatie en genadeloze verdienmodellen die onze democratie en economie teisteren*".

Deze memo gaat in op die minder mooie dingen ofwel digitale risico's. Deze risico's zijn (deels) onzichtbaar en best abstract. Maar de gevolgen van een informatieveiligheidsincident kunnen verstrekkende gevolgen hebben, voor onze inwoners en voor de continuïteit van onze dienstverlening. Voorbeelden daarvan zijn de hack bij het Hof van Twente, gemeente Buren en de universiteit Maastricht. Het merendeel van de uitval van systemen en dienstverlening wordt echter veroorzaakt door onbedoelde fouten. Ook dat kan ontwrichtend zijn zoals in juli 2024 toen een cyberbeveiligingsbedrijf wereldwijd een storing veroorzaakte. En eind augustus toen onze dienstverlening deels stagneerde door een fout in de softwarecode bij het Ministerie van Defensie. Hiermee wordt zichtbaar hoe onmisbaar IT-systemen inmiddels zijn voor de continuïteit van dienstverlening van de overheid.

Regelgeving op het gebied van digitale weerbaarheid

Het is belangrijk dat we als individuen zelf, maar ook als gemeente, digitaal weerbaar zijn. Dit betekent weten wat de (digitale) risico's zijn, je bewust zijn van de afhankelijkheid van andere partijen hierbij en voorbereid zijn op de gevolgen die incidenten kunnen hebben. We treffen onder het motto 'ons eigen huis op orde hebben' allerlei maatregelen om onze organisatie tegen de digitale risico's te wapenen en onze informatie te beschermen. De herziene Europese Network and Information Security-directive, kortweg de NIS2-richtlijn, is van kracht met als doel om de cyberweerbaarheid in EU-lidstaten te verbeteren. De Nederlandse uitwerking van deze wet heet de cyberbeveiligingswet [1]

[1] En de daaruit voortvloeiende BIO 2.0(1) waarin de (verscherpte) beveiligingsmaatregelen zijn opgenomen.

en zal medio 2025 van kracht zijn. Het zorgen voor digitale veiligheid is hiermee een wettelijke plicht geworden.

Het is aanscherping van al bestaande maatregelen
Het is niet zo dat er nu niets is of dat we als gemeente niets doen aan informatieveiligheid. Er is al een Baseline informatiebeveiliging waaraan gemeenten zich via een resolutie van de VNG hebben gecommitteerd. Deze baseline en de daarin opgenomen controls en maatregelen zijn nu het kader voor onze informatiebeveiliging. Uw raad heeft daarnaast vorig jaar geld beschikbaar gesteld voor de invoering van monitoring en response. Dat betekent 24/7 detectie en snelle analyses van digitale dreigingen om in voorkomende gevallen direct te handelen. Dit is een belangrijke maatregel in het kader van cyberweerbaarheid. We hebben een programma om onze medewerkers bewust te maken van informatieveilig handelen en om privacy bewust om te gaan met persoonsgegevens. Al onze medewerkers vormen immers een belangrijke “human firewall”. Jaarlijks worden via de ENSIA-methodiek op diverse onderdelen (zelf)-audits gehouden. We implementeren een Information Security Management Systeem2 (ISMS) zodat de structurele aandacht voor informatieveiligheid en privacy beter geborgd is.

Er komt een toezichthoudende autoriteit en een meldplicht voor significante incidenten
Bestuurders zijn verplicht om de beveiligingsmaatregelen conform NIS2 goed te keuren en moeten toezien op de uitvoering van die maatregelen. Nieuw is dat er daarnaast een toezichthoudende Autoriteit komt, de Rijksinspectie Digitale Infrastructuur (RDI). De RDI kan zich richten op toezicht achteraf (interbestuurlijk toezicht), maar ook vooraf audits uitvoeren op de digitale beveiliging van gemeenten. Ambtelijk moeten de beveiligingsrisico’s geïdentificeerd zijn, risicobeheermaatregelen ingevoerd worden en periodiek beoordeeld worden. Significante cyberincidenten3 moeten geregistreerd en binnen 24 uur gemeld worden bij de toezichthouder en aan het Computer Security Incident Response Team (CSIRT). Voor gemeenten is dit waarschijnlijk de Informatiebeveiligingsdienst (IBD).

Investeren in digitale veiligheid
In de kern gaat het erom dat gemeenten vanwege de verregaande digitalisering moeten blijven investeren in hun digitale veiligheid en daarover verantwoording afleggen. Onze inwoners moeten erop kunnen vertrouwen dat hun gegevens bij ons veilig zijn. De eisen worden hoger, de digitale risico’s worden groter en de administratieve (verantwoording)lasten nemen toe. Uit de impactassesment van de Europese Commissie blijkt dat voor nieuwe entiteiten een toename van maximaal 22% aan ICT-beveiligingskosten nodig is om aan de eisen van de NIS2- richtlijn te voldoen. De werkelijke toename hangt af van de huidige systemen en netwerken al beveiligd zijn.

[2] Eveneens een verplichting binnen NIS2
[3] Voor grootschalige of complexe incidenten die van invloed zijn op onze gemeentelijke dienstverlening moet rekening gehouden worden met gemiddeld 480 minuten afhandeltijd.