PROVINCIE UTRECHT

Statenbrief

Aan Provinciale Staten

Onderwerp	Voorbereiding op NIS2
Datum	9-07-2024
Documentnummer	UTSP-538973261-923
Van	Victor Roos / Remco Schilderinck
Telefoonnummer	+31611737548 / +31639632317
E-mailadres	victor.roos@provincie-utrecht.nl / remco.schilderinck@provincie-utrecht.nl
Domein/opgave	CCO / BIO
Team	TCC / IEA
Portefeuillehouder	Van Schie, Bakker
Bijlage	1. Samenvatting rapport proeftoets NIS2

Geachte leden van Provinciale Staten,

Essentie / samenvatting:
Naar aanleiding van de invoering per oktober 2024 van de NIS2, nieuwe Europese wetgeving (richtlijn) op het gebied van informatiebeveiliging, heeft de provincie Utrecht onderzocht welke verbeteringen nodig zijn om te voldoen aan de NIS2. Dat is gedaan door de huidige staat van informatiebeveiliging te toetsen tegen de toekomstige vereisten. Met deze brief wordt u geïnformeerd over de resultaten van dit onderzoek en de stappen die de provincie Utrecht ter voorbereiding op de NIS2.

Inleiding:
De Europese richtlijn NIS (Network and Information Security Directive, 2016), in Nederland geïmplementeerd met de Wbni (Wet beveiliging netwerk- en informatiesystemen, 2018), is gericht op versterking van de cyberbeveiligingsweerbaarheid van sectoren en organisaties die verantwoordelijk zijn voor diensten die essentieel zijn voor de maatschappij. De NIS geldt niet voor decentrale overheden. Dat verandert met de komst van de opvolger van de NIS, de NIS2. Voor de provincie Utrecht (PU) betekent de NIS2 een beweging van de huidige zelfregulering naar doorlopend voldoen aan NIS2 en daarover verantwoording kunnen afleggen. De normen worden strenger en nationale toezichthouders kunnen boetes uitdelen en bestuursleden persoonlijk aansprakelijk stellen. De verantwoording betekent het continu valideren van beveiligingsmaatregelen, als onderdeel van een bewijsplicht over het afdoende beheersen van risico's. Naar aanleiding van de invoering van de NIS2 per oktober 2024 heeft de provincie Utrecht onderzocht welke verbeteringen nodig zijn om te voldoen aan de NIS2 door de huidige praktijk te toetsen tegen de toekomstige vereisten.

Uitgaande van de wettekst van de NIS2 en de communicatie vanuit het Rijk is nu al wel duidelijk welke impact de NIS2 zal hebben en wat deze van organisaties zoals de PU vragen. Kort samengevat stelt de NIS2 een drietal belangrijke verplichtingen:

1. **Zorgplicht**:
   De zorgplicht van de NIS2 houdt in dat de PU haar cybersecurity risico's zodanig beheerst, dat de maatschappelijke gevolgen van incidenten beperkt blijft. De PU is verplicht zelf een risicobeoordeling uit

te voeren, op basis waarvan zij passende maatregelen neemt om haar diensten zoveel mogelijk te waarborgen en de gebruikte informatie te beschermen.

2. **Meldplicht**:
   De meldplicht schrijft voor dat de PU incidenten binnen 24 uur moeten melden bij de toezichthouder. Het gaat om incidenten die de verlening van de essentiële dienst aanzienlijk (kunnen) verstoren. Het gaat niet alleen om incidenten bij de provincie Utrecht zelf, maar zeker ook incidenten bij haar toeleveranciers en ketenpartners.
3. **Verantwoordingsplicht**:
   Deze houdt in dat de PU verantwoording aflegt aan een externe toezichthouder over de naleving van de verplichtingen van de NIS2. Dat betekent dat de provincie Utrecht de effectieve werking van beveiligingsbeleid en -maatregelen kan onderbouwen met documentatie.

Veel is dus al duidelijk over de impact van de NIS2. Toch zijn er nog onzekerheden. De implementatiewet van de NIS2, de Cyberbeveiligingswet, is 21 mei in consultatie gegaan en wordt de komende maanden nader uitgewerkt in AMvB's en ministeriële regelingen. Zeker is wel dat de provincies onder de essentiële entiteiten vallen die intensiever toezicht krijgen. De toezichthouder Rijksinspectie Digitale Infrastructuur (RDI) heeft aangekondigd dat de bestaande toezichts- en verantwoordingsinstrumenten versterkt zullen worden voor de NIS2. Het ministerie van Binnenlandse Zaken (BZK) zal de Baseline Informatiebeveiliging Overheid (BIO) geschikt maken voor de NIS2 en wettelijk verplicht stellen (BIO 2.0, medio 2024). BZK zal met de VNG het instrument Eenduidige Normatiek Single Information Audit (ENSIA) voor gemeenten geschikt maken voor de NIS2 en wil het ook toepassen voor provincies en waterschappen.

Voor de sector overheid is de RDI de aangewezen toezichthouder die over de NIS2 en de Cyberbeveiligingswet gaat. Voor de sector transport is de Inspectie Leefomgeving en Transport (ILT) de toezichthouder. Overheden die onder beide sectoren vallen, zoals de provincie Utrecht, krijgen te maken met beide toezichthouders die onderling zullen afstemmen over inspecties en resultaten daarvan.

In bijlage 1 staan de belangrijkste bevindingen en aanbevelingen over de impact van de NIS2 op de provincie Utrecht en de stappen die nog gezet moeten worden ter voorbereiding op de inwerkingtreding van de NIS2. Wij kunnen deze informatie met u delen zonder het risico op cyberaanvallen te vergroten. De bevindingen en aanbevelingen onderschrijven wij en hebben wij vertaald naar het plan van aanpak. De organisatie zal dit jaar en volgend jaar langs dit plan concrete stappen zetten om aan de NIS2 te voldoen.

Wij vragen u kennis te nemen van de gevolgen die de NIS2 heeft op de provincie Utrecht en welke stappen wij zullen zetten om aan de NIS2 te voldoen en daarover jaarlijks te verantwoorden aan PS en de nationale toezichthouder.

Vervolgprocedure / voortgang:

Het versterken van de informatieveiligheid en privacybescherming is een continuproces. De digitale ontwikkelingen volgen elkaar in rap tempo op en dat vraagt om flexibiliteit en aanpassingsvermogen. Niet iets waar we als overheid, en de provincie in het bijzonder, heel goed in zijn. Nieuwe wetgeving of richtlijnen moeten ervoor zorgen dat we ons bewuster worden van de noodzaak tot aanpassing aan de snelle ontwikkelingen. We doen ons uiterste best om bij te blijven. Dat vraagt om investeringen zowel in techniek als in ons gedrag. Voor dat laatste is veel aandacht en dat zal noodzakelijk blijven. Zowel bestaande als nieuwe medewerkers houden we continu bij de les door het aanbieden van lesmodules, een wekelijkse mail met een stelling en phishing-mail acties. Het heeft onze aandacht en wij sluiten niet uit dat in de komende jaren hogere investeringen nodig zijn om in deze wedloop bij te kunnen blijven benen.

Wij hebben de directie gevraagd een plan van aanpak uit te werken voor sturing en aanpak op de onderwerpen Compliance, Governance, Kennis & Bewustwording en Borging ter voorbereiding op de aanstaande Cybersecuritywetgeving. Deze zal in de het derde kwartaal gereed zijn. Daarbij is in de uitwerking gekozen voor een onderscheid tussen centrale versus decentrale activiteiten.
In eerste aanleg zullen deze onderwerpen worden opgepakt binnen de mogelijkheden van de huidige formatie en beschikbare middelen. Wij zullen erop toe zien dat de organisatie in staat wordt gesteld om haar verantwoordelijkheid hierin te nemen. Dit is rand voorwaardelijk om te groeien in volwassenheid op het gebied van informatieveiligheid.

Er is gekozen voor een systematische aanpak, zodat de samenhang tussen alle activiteiten op het gebied van implementatie van cybersecuritymaatregelen onderling en concern breed, worden afgestemd en geborgd. Onderdelen die in het plan van aanpak in ieder geval aan bod komen zijn:

- Het op orde brengen van een aantal, centrale, rand voorwaardelijke processen willen uiterlijk in het tweede kwartaal van 2025 gereed hebben;
- Het borgen van toezicht die vanuit de NIS2-richtlijn van kracht wordt en de belangrijkste risico's op het gebied van dienstverlening met maatschappelijke impact identificeren (tweede kwartaal 2025);
- Het in kaart brengen van impact op hoofdlijnen, organisatorisch en financieel (vierde kwartaal 2024);
- Het toedelen van passende capaciteit en expertise om de organisatie in staat te stellen aan NIS2-richtlijn te kunnen gaan voldoen (tweede kwartaal 2025);
- Inrichten van een verplicht "intern meldpunt" (vierde kwartaal 2024).

In de tweede helft van 2024 zal met de verdere uitwerking van de Cyberbeveiligingswet, die naar verwachting in de eerste helft van 2025 van kracht wordt, meer duidelijkheid ontstaan. Via de reguliere planning en control producten, zomernota en jaarrekening, zullen we u informeren over de voortgang. Voor het eerst bij de zomernota 2025, jaarrekening 2024. Daarnaast zal dit onderzoek twee- tot driejaarlijks vanuit CCO worden herhaald om te toetsen waar we staan als provincie.

Gedeputeerde Staten van Utrecht,

Voorzitter,
mr. J.H. Oosters

Secretaris,
mr. drs. A.G. Knol-van Leeuwen