PROVINCIE UTRECHT

PROEFTOETS NIS2

Samenvatting
Rapport van bevindingen
Eenheid Concern Control

Stappen ter voorbereiding op de Europese richtlijn Network and Information Security Directive 2

Definitief
10 april 2024

Colofon

DATUM	18-04-24
VERSIE & STATUS	1.0 definitief
DOCUMENTNR	UTSP-538973261-925
PORTEFEUILLEHOUDER	André van Schie, Has Bakker
OPDRACHTGEVER	Johan Luiks, concern controller
AUTEURS & AUDITORS	ing. V. Roos MSc RE, Eenheid Concern Control (lead onderzoeker) M.J. van Zitteren RE, Q-RESULTANCY (secundant)
ONDERWERP	Samenvatting Rapport van bevindingen *Proeftoets NIS2 2023* provincie Utrecht
VERSPREIDING	PS commissie BEC

1 SAMENVATTING

De Europese richtlijn NIS (Network and Information Security Directive), in Nederland geïmplementeerd met de Wbni (Wet beveiliging netwerk- en informatiesystemen), is gericht op versterking van de cyberbeveiligings-weerbaarheid 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. De NIS2 is een reactie op de toegenomen blootstelling van Europa aan cyberdreigingen en het feit dat hoe meer we onderling verbonden zijn, hoe kwetsbaarder we zijn voor kwaadaardige cyberactiviteiten. De NIS2 moet uiterlijk oktober 2024 geïmplementeerd zijn door de EU-lidstaten. Het Rijk zal de lijn van de NIS2 zoveel mogelijk volgen in de vertaling naar de Wbni2.

Naar aanleiding van de invoering van de NIS2 per oktober 2024 en de gewenste voorbereiding daarop hebben wij voor de provincie Utrecht (PU) onderzoek uitgevoerd met de volgende centrale onderzoeksvraag:
Welke verbeteringen moet de PU doorvoeren op het gebied van informatiebeveiliging om te voldoen aan de NIS2?

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 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.

De zorg- en meldplicht van de NIS2 strekken zich uit over de ketens met toeleveranciers, sub leveranciers en partners (ecosystemen) waar de provincie gebruik van maakt voor haar taken en opgaven. Dat betekent dat de provincie Utrecht de risico's in haar ketens moet kennen en aantoonbaar (laten) beheersen. Het overstijgt enkelvoudig leveranciersmanagement en contractafspraken die uitgaan van vertrouwen. Voorbeelden van ketenpartners van de provincie Utrecht waar dit speelt zijn BIJ12, de omgevingsdiensten en -na verzelfstandiging- het trambedrijf.

Veel is dus al duidelijk over de impact van de NIS2. Toch zijn er nog onzekerheden. De nieuwe Nederlandse Wet beveiliging netwerk- en informatiesystemen (Wbni) is nog niet verschenen. 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 Wbni 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.

Naar aanleiding van de komst van de NIS2 is de koepelorganisatie IPO met de provincies bezig met de oprichting van het Computer Security Incident Response Team (CSIRT) voor provincies. Dit is een soort brandweer voor ernstige cyberincidenten die ook waarschuwt voor actuele dreigingen.

De NIS2 is van toepassing op informatietechnologie (IT) én operationele technologie (OT). OT binnen industriële netwerken, ook wel aangeduid als 'Industrial Automation and Control Systems' (IACS), speelt een centrale rol in het aansturen, monitoren en beheren van fysieke processen binnen organisaties. De provincie Utrecht gebruikt OT bij het regionaal verkeersmanagement, het trambedrijf, vaarwegen (bruggen) en in gebouwen. Het Nationaal Cybersecurity Centrum (NCSC) vraagt meer aandacht voor het weerbaar maken van OT vanwege toegenomen dreiging en afhankelijkheden in de keten die risicobeheersing ingewikkeld maken.

Voor OT gelden andere standaarden en normen over informatiebeveiliging dan voor IT. Bij de fysieke processen aangestuurd door OT liggen de risico's meer op het vlak van ongevallen, veiligheid en het milieu. De beheersing daarvan wordt cybersecurity genoemd. Rijkswaterstaat heeft samen met de waterschappen de norm Cybersecurity Implementatierichtlijn (CSIR) ontwikkeld door normen voor IT en OT te bundelen en te werken met weerstandsniveaus tegen een oplopende schaal van cyberaanvallers. Bij fysieke processen met OT waar sprake is van risico's met meer dan lage maatschappelijke impact, zal een hoger weerstandsniveau nodig zijn.

De werelden van IT en OT raken steeds hechter met elkaar verbonden. In het regionaal verkeersmanagement van de provincie zien we dit terug in de ontwikkeling van slimme mobiliteit. Verkeersregelingen (OT) staan niet meer op zichzelf, maar worden betrokken in een ecosysteem met dynamische regelkringen die reageren op drukte en data delen met platformen en apps (IT) voor het optimaliseren van verkeersstromen. Voor een goede beheersing van cybersecurity risico's is het nodig dat de PU deze benadert met een brede blik op de keten (partners en leveranciers) en de samenhang van IT en OT.

De belangrijkste bevindingen waartoe wij zijn gekomen op basis van het onderzoek vindt u hieronder in tabel 1, vergezeld door onze aanbevelingen. Bij het opstellen van de aanbevelingen hebben we meegewogen wat de deelnemers van de workshops ons hebben meegegeven. Wij realiseren ons dat de opvolging van deze aanbevelingen veel tijd in beslag neemt. Het is in het belang van de provincie om snel te starten en vooral niet te wachten op de Wbni (deze zal de NIS2 zoveel mogelijk volgen) en de BIO 2.0. Uitstel maakt de tijd om voor te bereiden op de NIS2 korter en de kans om geschikt al dan niet tijdelijk personeel te vinden kleiner. De inhoud van de NIS2 is sterk gebaseerd op regels. De ruimte die voor de organisatie resteert zit in de eigen verantwoordelijkheid en afweging rond de risico inschatting en de beheersing daarvan met maatregelen.

Tabel 1 – Hoofdbevindingen zorgplicht (A), meldplicht (B) en verantwoordingsplicht (C)

	Hoofdbevinding	*Aanbeveling*
A1	Gebrek aan structuur en doorwerking van beleid naar inrichtingseisen naar maatregelen.	Richt processen risicoanalyse, beheersen risico's met maatregelen en monitoren/verbeteren in en monitor deze.
A2	De risicobeheersing stagneert bij diepgaande risicoanalyses en het treffen van maatregelen.	Investeer in werken met leveranciersonafhankelijke risicoanalysemethodiek en monitor voortgang.
A3	Het huidige niveau van leveranciers-management is niet toereikend voor de NIS2 vereisten rond ketenbeheersing.	Versterk leveranciersmanagement naar regie op informatiebeveiliging in de keten.
A4	Centrale en decentrale plannen voor bedrijfscontinuïteit hangen weinig samen en worden weinig geoefend.	Breng meer samenhang in de plannen en oefen regelmatig het herstelvermogen met scenario's.
A5	Onduidelijke verdeling van verantwoordelijkheden tussen domeinen zal verantwoorden over NIS2 hinderen.	Maak het proces leidend en stel de eigenaar in staat risico's te beheersen.

	Hoofdbevinding	*Aanbeveling*
A6	Toezicht houden op cyberrisico's en voortgang maatregelen, een vereiste van de NIS2, is nieuw voor het CMT.	Zet jaarlijkse verantwoording aan PS en toezichthouder op, gekoppeld aan P&C-cyclus.
B1	Een centraal contact- en meldpunt voor cyberincidenten richting de toezichthouder en CSIRT ontbreekt.	Richt centraal contact- en meldpunt cyberincidenten in en leer van cyberincidenten.
B2	De huidige afspraken met toeleveranciers zijn ontoereikend voor de meldingsvereisten van de NIS2.	Maak afspraken met leveranciers voor het tijdig melden van cyberincidenten.
C1	Een kwaliteitssysteem voor informatiebeveiliging is nog niet in gebruik.	Neem een kwaliteitssysteem voor informatiebeveiliging/ cybersecurity in gebruik en verantwoord daarmee.

.