Hoofdlijnenverslag van de internetconsultatie

Ministeriële regeling beveiliging netwerk- en informatiesystemen IenW

(Internetconsultatie van 24 februari tot en met 29 maart 2021)

Het Ministerie van Infrastructuur en Waterstaat bereidt de ministeriele regeling (vanaf nu: regeling) beveiliging netwerk- en informatiesystemen IenW voor. Deze regeling wordt opgesteld ten behoeve van de beveiliging van netwerk- en informatiesystemen van aanbieders van essentiële diensten (AED's). De regeling is gericht op verhoging van de digitale weerbaarheid binnen de sectoren op het terrein van infrastructuur en waterstaat.

Het doel is het verhogen van de digitale weerbaarheid van AED's. Met een hogere digitale weerbaarheid kunnen incidenten zoveel mogelijk worden voorkomen en/of de impact ervan kan verkleind worden. Om het doel te bereiken zijn de maatregelen uit bijlage van artikel 3a van het gewijzigde Bbni (zie de link bij de overige documenten) verder uitgewerkt en toegelicht.

Met het opstellen van deze regeling kan beter worden aangesloten op best practices door het voorschrijven van een risicogestuurd Information Security Management System (ISMS) met bijbehorende maatregelen. De maatregelen gaan uit van de primaire verantwoordelijkheid van AED's zelf, maar geeft de sectorale toezichthouder meer houvast om te sturen op het niveau van de beveiliging en waar nodig ook in te kunnen grijpen. De maatregelen sluiten aan op best practices en/of gangbare normen zoals de ISO27001, ISO27002, IEC 62443 en de Baseline Informatiebeveiliging Overheid.

De reacties

Er kon worden gereageerd op deze regeling en de toelichting. Er zijn in totaal 7 reacties ingediend, hiervan zijn er twee openbaar. Indieners zijn:

- AED's uit de sectoren drinkwater en vervoer, luchtvervoer en vervoer over water (4)
- Een adviesbureau
- Particulieren (2)

1. Algemeen beeld van de reacties

Het doel van de regeling wordt door de meeste indieners onderschreven. Wel zijn er vragen over de effectiviteit en haalbaarheid van de Regeling, en ook worden er nog vragen gesteld en opmerkingen gemaakt over Reikwijdte, Normenkaders en Risicomanagement.

2. Hoofdlijnen van de inhoudelijke reacties

Hieronder volgen enkele toonaangevende reacties. De reacties geven uitsluitend de mening van de indieners weer.

Algemene opmerkingen over doel en effectiviteit van de Regeling

- Het is een goede zaak dat met deze regeling duidelijkheid wordt geschapen over de reikwijdte en het minimumniveau van de zorgplicht uit de Wet beveiliging netwerk- en informatiesystemen (Wbni, 2019). De regeling biedt de toezichthouder een toetsingskader en geeft de AED's helderheid over wat van hen verwacht wordt en of zij voldoen aan hun wettelijke zorgplicht voor netwerk- en informatiebeveiliging.
- Gezien het dreigingsbeeld zoals geschetst in het Cybersecuritybeeld NL van 2020 zou de voorgestelde regeling te vrijblijvend kunnen zijn en niet voldoende diepgang te hebben om vanuit de overheidsrol als toezichthouder sturing te geven aan het gewenste weerbaarheidsniveau van de AED's.
- Om de digitale weerbaarheid van AED's te verhogen dient de kennis en kunde bij de AED's voldoende op orde te zijn, en moeten zij voldoende overzicht hebben over en inzicht in de eigen ICT infrastructuur.
- De inspanningen die nodig zijn om aantoonbaar aan álle vereisten te voldoen moeten niet onderschat worden en zullen de nodige doorlooptijd vergen.
- De vraag rijst of er voldoende financiële middelen tegenover de eisen staan, omdat het voorstelbaar is dat sommige AED's nog niet volledig op de eisen en wensen in deze regeling zijn voorbereid.
- Nieuwe AED's hebben nog niet voldoende maatregelen kunnen nemen als hierboven gesteld, en de gevolgen van het daarmee moeten gaan voldoen aan de beveiligingseisen van de WBNI en het Bbni zijn voor deze organisaties veel groter dan het afwegingskader en de toelichting doen veronderstellen.

Reikwijdte

- In de regeling wordt verwezen naar sectorspecifieke kaders o.a. voor waterbedrijven en luchtvaart. Deze kaders zijn echter nog niet officieel vastgesteld waarbij tevens wordt aangegeven dat nog niet duidelijk is of deze kaders ook daadwerkelijk invulling geven aan de gestelde eisen voor de AED. Artikel 2 "reikwijdte" van de toelichting behoeft daarom meer duidelijkheid.
- Het is onduidelijk wat de definitie is van 'de essentiële dienst' in de zin: "…….Voor zover het de netwerk- en informatiesystemen betreft die gebruikt worden voor de essentiële dienst".
- De reikwijdtebepaling van artikel 2, eerste lid, van de regeling is niet duidelijk voor zover het vervoer betreft. Dit artikellid en de toelichting daarop graag aanpassen zodat duidelijk is dat vervoer over spoor en weg ook vallen onder deze regeling voor zover organisaties zullen worden aangewezen als vitale aanbieders.

Normenkaders

- Artikel 24 beschrijft dat afwijkingen conform sectorspecifieke normen zijn toegestaan, mits deze gelijkwaardig zijn. Dit biedt geen ruimte voor toepassing van andere normen dan de expliciet genoemde sectorspecifieke normen, of het toepassen van andere (internationale) wetgeving die in potentie conflicteert met deze regeling, maar toch een equivalent of beter resultaat geeft.
- Een aangepaste tekst wordt voorgesteld voor artikel 24, om te voorkomen dat er een moeilijk te onderhouden lijst van sectorspecifieke normen in de regeling komt.
- Vanuit de internetconsultatie wordt aangegeven dat de regeling aansluit op de gangbare normen ISO 27001 / 27002, IEC 62443 en Baseline Informatiebeveiliging Overheid (BIO). Dit is echter in het document niet of beperkt vast te stellen.
- Het is niet duidelijk of de maatregelen in de Regeling van toepassing zijn op de kantoorautomatisering en/of proces automatisering.
- De regeling bevat voor de spoorsector geen inhoudelijke beveiligingsnormen zoals die voor een aantal andere sectoren wel al gelden, deze dienen nog te worden ontwikkeld met alle actoren in de spoorsector.

Risicomanagement

- Kennelijk mogen AED's zelf het niveau en diepgang van de maatregelen bepalen. Het lijkt beter om concrete maatregelen in deze regeling te zetten met minimale eisen die de AED's zelf m.b.t. een ISMS en onafhankelijke beoordeling in stand moeten houden. De overheid kan hierop toezicht houden.
- *Definitie van "keten":* Het is onduidelijk wat er met 'de keten' van toeleverancier en afnemers wordt bedoeld en waar de grens ligt ter beoordeling.
- Met toevoeging van de term 'keten' wordt de reikwijdte van de te betrekken risico's zeer breed. Een deel van de keten is voor bedrijven niet of nauwelijks inzichtelijk en/of beheersbaar. Verzoek is om de term 'binnen de keten' achterwege te laten.
- *Frequentie van testen*: De frequentie wordt bepaald door het proces en de mate van risico. Dit proces kan vervolgens worden getoetst. De toetsbaarheid van dit artikel (23) kan beter tot zijn recht komen wanneer het artikel is geformuleerd op procesniveau.
- *Monitoring*: Het testen van monitoring is niet aan de orde; door toepassing van monitoring blijkt namelijk al in hoeverre dit werkt. Verzoek is om de vereisten rondom het testen achterwege te laten.
- *Periodieke actualisatie*: In de toelichting van dit artikel wordt gesproken van een gangbare periodiek van tenminste eenmaal per jaar: "Indien hierop wordt afgeweken wordt dit onderbouwd in de procedure". Voorgesteld wordt deze zin anders te formuleren.
- *Definitie "'kritiek" vs "hoog risico"*: Het is onduidelijk of een informatiesysteem dat door de regeling als 'kritiek' is gedefinieerd hetzelfde is als een informatie systeem dat door de AED als hoog risico (essentieel) is geclassificeerd.