# Wetsvoorstel (DOC 55 2635) betreffende de verplichting van het gebruik van unidirectionele netwerken – Synergrid Positie

25.03.2024

Synergrid en haar leden wensen hun standpunt uit te drukken over het wetsvoorstel betreffende de beveiliging van kritieke infrastructuren, dat het verplicht gebruik van unidirectionele netwerken voorstelt.

Een unidirectioneel netwerk, ook wel een datadiode genoemd, is een type netwerkverbinding dat alleen gegevensoverdracht in één richting toelaat. Dit betekent dat informatie van punt A naar punt B kan worden verzonden, maar niet terug van B naar A.

**Standpunt**

Netwerkbeheerders erkennen de noodzaak om hun kritieke infrastructuur te beveiligen, een proces dat voortdurend in ontwikkeling is. Echter, het verplicht stellen van unidirectionele netwerken garandeert niet noodzakelijkerwijs een verbetering van de beveiliging.

Alle netwerkbeheerders die lid zijn van Synergrid zijn aangewezen als essentiële operators onder de NIS1-wet en voldoen nauwgezet aan de opgelegde wettelijke verplichtingen. Zodra de NIS2-richtlijn in Belgisch recht is omgezet, zullen de netwerkbeheerders de nieuwe cyberbeveiligingsregels toepassen.

Daarnaast moeten Europese netwerkbeheerders voldoen aan andere verplichte cyberbeveiligingsregels. Deze Europese regels zijn bedoeld om netten die strategisch zijn voor de bevolking, bedrijven en uiteraard de Belgische staat, maximaal te beveiligen. Al deze regels zijn samengebracht op Europees niveau in wat de " Network Code Cybersecurity" wordt genoemd. Deze Europese code is bindend voor de netbeheerders op dezelfde manier als de Belgische wetgeving. Hierover zal later in het document meer worden besproken.

Gezien alle zeer strikte veiligheidsregels die reeds van toepassing zijn op netwerkbeheerders, lijkt het wetsvoorstel niet geschikt voor hen.

De verplichting om unidirectionele netwerken te gebruiken voor de netten is niet alleen technisch af te raden, maar de overstap naar unidirectionele netwerken zou ook een operationele hindernis vormen voor het goed beheer van de netwerken.

1. **Integratie met bestaande systemen:** Het invoeren van unidirectionele netwerken zou aanzienlijke aanpassingen van bestaande systemen en infrastructuren vereisen. Veel van onze huidige operationele systemen en processen zijn ontworpen voor en afhankelijk van bidirectionele communicatie. Het herontwerpen van deze systemen zou leiden tot aanzienlijke kosten en complexiteit, zonder een gegarandeerde verbetering van de beveiliging.
2. **Beperking van monitoring en onderhoud op afstand**: Monitoring en onderhoud op afstand zijn essentieel voor effectief netwerkbeheer en een snelle respons op storingen, zoals nodig is voor offshore-installaties. Unidirectionele netwerken beperken de mogelijkheid voor interventies op afstand, wat kan leiden tot langere downtime en hogere operationele kosten.

3. **Impact op automatisering en slimme netwerken**: De energietransitie en de ontwikkeling van slimme netwerken vereisen geavanceerde automatisering en gegevensuitwisseling. Unidirectionele netwerken hinderen de ontwikkeling van slimme netwerken, die essentieel zijn voor het beheer van hernieuwbare energiebronnen en het balanceren van vraag en aanbod in realtime. Onze operationele activiteiten vereisen bidirectionele communicatie. Dit is essentieel om onze netwerken in realtime te monitoren, te beheren en aan te passen.
4. **Kosten-efficiëntie:** De implementatie en het onderhoud van unidirectionele netwerken zouden aanzienlijke investeringen vergen, niet alleen in de technologie zelf maar ook in de opleiding van personeel en het herontwerp van operationele processen. Deze kosten zouden uiteindelijk worden doorberekend aan consumenten, zonder duidelijke meerwaarde in termen van netwerkveiligheid of -betrouwbaarheid.
5. **Beperking in de coördinatie van de netwerkbeheerdersrespons**: In geval van grote storingen of rampen is een snelle en effectieve communicatie tussen de verschillende delen van de energie-infrastructuur essentieel voor reparatiewerkzaamheden. Unidirectionele communicatie beperkt de mogelijkheden voor coördinatie en samenwerking tijdens kritieke situaties, wat het herstel kan vertragen en de negatieve impact op eindgebruikers kan vergroten.
6. **Innovatie en flexibiliteit**: De verplichting om unidirectionele netwerken te gebruiken zou innovatie belemmeren en het vermogen van netwerkbeheerders om snel en flexibel te reageren op nieuwe technologische ontwikkelingen en veranderende operationele behoeften beperken. Elke voorgesteld techniek moet duurzaam zijn en een risico-gebaseerde aanpak mogelijk maken. Gezien het continu evoluerende digitale landschap, is het noodzakelijk om de beste beschikbare technologieën te gebruiken die kunnen meegroeien met innovaties en toekomstige behoeften. Een beperkend beleid zou niet alleen de innovatiecapaciteit van operators beperken, maar ook het potentieel van nieuwe technologieën onbenut laten.
7. **Optimalisatie van middelen**: Het toevoegen van complexiteit zonder een duidelijke toename van de veiligheidsefficiëntie is met name niet wenselijk in de context van de energietransitie, waarvoor de teams en middelen van netwerkbeheerders al sterk worden bevraagd.

**Veiligheidsmaatregelen opbouwen in overeenstemming met het Belgische en Europese wettelijke kader**

De veiligheid van netwerken kan altijd worden verbeterd. Het beste bewijs hiervan is de snelle invoering van de NIS2-richtlijn, kort na de NIS1-richtlijn.

Het is belangrijk dat het streven naar versterking van de veiligheid van kritieke infrastructuren door de auteurs van dit wetsvoorstel in overeenstemming is met de wet tot omzetting van de CER-richtlijn en de wet tot omzetting van de NIS2-richtlijn.

Deze twee wetgevingen leggen nieuwe, strikte veiligheidsnormen op die de veiligheid van netwerken al aanzienlijk zullen versterken.

Zoals eerder vermeld, moeten de netwerkbeheerders naast deze nieuwe veiligheidsnormen ook voldoen aan de verplichte normen zoals voorzien in de Cybersecurity Network Code.

De netwerkbeheerders vragen om eerst de effecten van de implementatie van deze teksten te evalueren alvorens andere initiatieven zoals het gebruik van unidirectionele netwerken op te leggen, wat, zoals reeds werd benadrukt, indruist tegen een efficiënt, veilig, betrouwbaar en rationeel operationeel beheer van de netwerken.

De beheerders suggereren om de normen die momenteel worden omgezet aan te vullen met maatregelen of acties die gericht zijn op het verbeteren van de veiligheid van kritieke infrastructuren, zonder de operationele capaciteit van netwerkbeheerders in gevaar te brengen.

Drie overwegingen voor het aanvullen van het bestaande of binnenkort van kracht zijnde wettelijke kader:

1. **Versterkte cyberbeveiliging:** Implementatie van geavanceerde cyberbeveiligingsmaatregelen die rekening houden met de specifieke behoeften en risico's van de energie-infrastructuur.
2. **Flexibele technologische oplossingen**: Ondersteuning voor onderzoek en ontwikkeling van technologische oplossingen die zowel de veiligheid als de operationele efficiëntie verbeteren.
3. **Samenwerking en kennisdeling**: Aanmoediging van samenwerking tussen netwerkbeheerders, de overheid(en) en andere relevante belanghebbenden om beste praktijken en kennis op het gebied van infrastructuurveiligheid te delen.

**Besluit:**

De netwerkbeheerders erkennen het belang van het waarborgen van de veiligheid van hun infrastructuren. Zij benadrukken dat veiligheidsmaatregelen uitvoerbaar moeten zijn zonder hun vermogen om elektriciteit en gas op een veilige, betrouwbare en efficiënte manier te transporteren en te distribueren, in gevaar te brengen.

Een diepgaande en sectorspecifieke risicoanalyse is essentieel voor het ontwikkelen van een effectieve beveiligingsstrategie per sector. De netwerkbeheerders pleiten voor een evenwichtige aanpak die veiligheid, efficiëntie en innovatie combineert. Zij blijven openstaan voor samenwerking om een veerkrachtig energienetwerk te bouwen.

**Over Synergrid**, The Voice of the Belgian Energy Network

Synergrid is de spreekbuis van de Belgische elektriciteits- en gasnetbeheerders (*). Als zodanig is hij de spreekbuis van de sector bij de Belgische en Europese autoriteiten of iedere andere instantie die er een beroep op doet.

Synergrid vertegenwoordigt 9 ondernemingen die gas en elektriciteit leveren aan bedrijven en de bevolking in heel België. Samen met onze leden en aan de hand van innovatieve projecten helpen wij de klanten bij de energietransitie om de klimaatdoelstellingen te halen en de levenskwaliteit voor iedereen te verbeteren.

Synergrid ontwikkelt ook technische en milieunormen om betrouwbare netwerken te kunnen garanderen die voldoen aan de strengste veiligheidscriteria. Deze normen zijn bedoeld voor zijn leden, maar ook voor derden.

Naargelang de context zijn ze juridisch bindend of vormen zij te volgen best practices.
Synergrid ondersteunt haar leden bij het opzetten van nieuwe platformen voor flexibiliteit, zoals FlexHub (het enige platform in België voor flexibiliteitsbeheer) en het RTCP ('Real time communication platform').

Ten slotte is Synergrid het referentiepunt voor zijn leden op het gebied van arbeidsrecht, sociale betrekkingen en sectorale pensioenfondsen. De Federatie treedt ook op als patronaal woordvoerder van de sector binnen de sociale overlegorganen op nationaal niveau.

*(*)* Transmissienetbeheerders *(TNB's): Elia, Fluxys, en distributienetbeheerders (DNB's): Aieg, Aiesh, Fluvius, ORES, RESA, REW en Sibelga.*

Contact : Christine Declercq – Email : christine.declercq@synergrid.be