Blijkbaar regelt deze wet helemaal niets, de NIS2 richtlijn gaat over de beveiliging van netwerk- en informatie.
Maar wij doen alleen maar cyber, maar wat daaronder verstaan wordt?
Het is een mooie mode term, maar zegt helemaal niets.
Maar leg dat onze overheid maar eens uit.

artikel 16: hier wordt dezelfde denkfout gemaakt als bij de CER richtlijn implementatie waarbij het hokjes, dit is van mij of mijn sector denken en het verticaal bij zich houden van vermeende "verantwoordelijkheden" zwaarder weegt dan een fatsoenlijke toepassing van de wettelijke zaken uit de NIS2 richtlijn.
het lijkt er daarnaast sterk op dat de RDI (Rijksinspectie Digitale Infrastructuur) ter zijde wordt geschoven als toezichthouder.
Indien correct, had de overheid de naamswijziging van Agentschap Telecom wel achterwege kunnen laten.
Dezelfde versnippering, sector specifieke maar ook ministerie specifieke aanpak die voor de CER richtlijn geldt, geldt dus ook hier. Waarbij mijns inziens niet voldaan wordt aan de NIS2 eis van een nationale aanpak.
Misschien wel op papier, denkt de overheid, maar in praktijk zal daar helemaal niets van terecht komen.
De verkokering en doorgaans moeizame of ontbrekende wijze van samenwerking tussen ministeries zal dit ruimschoots verhinderen.

Artikel 17.1, tja schuif het maar weer voor je uit.
We halen de deadline van 18 oktober al niet, terwijl de eerste artikelen in dit wetsvoorstel gewoon letterlijke tekstuele kopietjes uit de nIS2 zijn, wete we nog niet eens wie het CSIRT gaat uitvoeren.
Hadden we die zeker onder de WBNI ook al niet, in strijd met de originele NIS richtlijn of wel?
Artikel 18, zelfde issue.
Artikel 19 idem.
Artikel 20, waarschijnlijk precies het probleem waarom dit wetsvoorstel er zo laat ligt.
Ik ben benieuwd en ook aardig verontrust om dit te lezen, de overheid heeft al moeite genoeg haar eigen zaken op orde te hebben en moet nu ook nog dit landelijk gaan bepalen en dat ook nog in "samenwerking" met alle ministeries die het aangaat.
Idem voor artikel 21, het is nogal vreemd dit neer te leggen bij veiligheid en justitie. Tenzij zij intern het NCSC dit laat doen, maar dan is de focus van die organisatie niet toereikend genoeg en de scope al helemaal niet.

artikel 22, 2e lid laatste volzin, tja dat krijg je als je veel te laat bent met je wetsvoorstel.
artikel 23 2e lid, oh nu hebben we het wel ineens over netwerk en informatiesystemen en niet cyber veiligheid. Maak je keuze of het een of het ander en wees er consequent in. Dan is deze verwoording passender dan cyber.
Artikel 23 3e lid vervang benadering door risico analyse
artikel 26 2e lid, door elkaar gebruik van terminologie, niet praktisch.
3e lid laatste zin: eis gewoon dat bij aanstelling ze dit direct hebben qua kennis, beetje jammer als bestuursleden bij elke nieuwe aanstelling 2 jaar krijgen om er aan te voldoen (zoals hier gesuggereerd wordt) dit komt de weerbaarheid van de organisaties niet ten goede.
5e lid, veel te zwakjes, een certificaat van deelname? Zit in klasje, valt in slaap en krijgt documentje. Toont op geen enkele wijze kennis aan Wassen neus dus.
6de lid, zoals de engelsen dat mooi zeggen, kick it in the long grass
8ste lid, jammer dat politieke leiding hierin buiten schot blijft. Gemiste kans.
Artikel 29 eerste lid voldoet niet ana de eisen van de NIS2 richtlijn waarin een eerste melding binnen 24 uur vermeld staat, volledige melding binnen 72 uur inderdaad. De 24 uurs termijn mist en heeft niets te maken met het 2e lid voor vertrouwensdiensten.
Artikel 37, kicking it in the long grass again
artikel 52 2e lid onder D, die verordening is gewijzigd, kijk even of daar niet het nieuwe 2023 nummer moet staan van de eIDAS 2.0
artikel 60 idem
artikel 64A in zake artikel 9 2e lid onder G AVG mist de wettelijke onderbouwing inzake welke nationale of unierechtelijke handeling dit toe zou staan, de CBW is daarvoor niet zelfstandig bevoegd anders zou een cirkel redenering ontstaan.