Hartelijk bedankt voor de uitwerking van de NIS 2. Hierbij geef ik mijn opmerkingen op het voorstel en vraag betrokken te worden bij de verdere verwerking.

Er wordt niet aangegeven waar de Nederlandse nis1 uitwerking afwijkt van die van andere landen. ALs het doel is om Europees meer zaken gelijk te trekken dan dat gebeurd is bij de NIS1. Kan een NIS2 alleen succes hebben door in beeld te zetten waar het mis is gegaan.

Het doel van de NIS2 is belangrijk, omdat dit doel laat zien dat de gemeenten hier een groot belang in hebben.

SDG' s zijn niet benoemd terwijl er wel degelijk impact op de SDG is. Zie SDG:

Er worden geen kansrijke beleidsopties genoemd. Ik kan mij niet voorstellen dat er op zo een belangrijk wetsvoorstel geen kansen zijn in beleid. Verzoek is om hier inzet op te plegen. Zeker nu het plan van het nieuwe kabinet veiligheid zo hoog op de agenda zet. In relatie tot dit punt is het ook vreemd dat er wel gesproken wordt over de gevolgen van deze niet genoemde opties?

In de doelen wordt veel aandacht besteedt aan de verschillen tussen lidstaten, maar er wordt niet gesproken over de lessen van de NIS1 en hoe deze aan te pakken. Ook wordt er niet gekeken naar hoe de wereld veranderd is en welke invloed dat zou moeten hebben. Graag analyseren wat de lessen zijn uit de NIS1 en analyseren hoe het veranderde cyberdreigingslandschap invloed heeft op de invulling van de NIS2.

Welke extra bepalingen stellen wij in Nederland voor om tot een hogere cyberbeveiligingsniveau te komen. Wat is onze ambitie? Er wordt aangegeven dat er ruimte wordt gelaten aan landen om extra zaken toe te voegen om zo tot een hoger cyberbeveiligingsniveau te komen. Aangezien Nederland een land is met een hoger digitaliseringsniveau, is een hoger ambitie met bijbehorende extra maatregelen onze morele plicht naar andere landen die nog niet op ons digitaliseringsniveau zijn.

Waar is de hulp voor het voldoen aan de NIS2 richtlijn georganiseerd? Er wordt gesproken over toezicht en over zorgplicht. Echter toezicht is achteraf en de zorgplicht wordt beschreven voor individuele organisaties richting hun eigen verantwoordelijkheden. Echter overheden als de provincie en de gemeente hebben ook een verantwoordelijkheid naar de organisaties binnen hun gebied. Er wordt niet gesproken hoe dit vorm zou moeten krijgen.

Er worden afspraken besproken op landelijk gebied. Echter juist door de sterke digitalisering van Nederland zijn afspraken op provinciaal en gemeentelijk niveau essentieel. Ook de sectorale aanpak schiet te kort bij grote incidenten in een provincie of een gemeente gezien de digitale

interafhankelijkheid van onze maatschappij. Denk ook aan hoe beveiliging georganiseerd is binnen organisaties. Niet meer als een middeleeuwse verdediging aan de muren, maar door segmentering binnen het bedrijfsnetwerk. Ditzelfde is nodig in Nederland. Het segmenteren van Nederland in provincies en gemeenten zodat crises zomin mogelijk de kans krijgen over te slaan naar andere gebieden.

Wat gemist wordt is de verantwoordelijkheid van lokale overheidsinstanties om niet alleen zelf bezig te zijn met de Nis2 maar ook hun verantwoordelijkheid te nemen naar andere organisaties die binnen hun gebied vallen onder de Nis2. Er is een zorgplicht om zelf te voldoen aan de nis2, maar ook om andere organisaties aan te moedigen en te ondersteunen bij het voldoen aan de nis2. Volgens de wet is veiligheid van inwoners en organisaties binnen gemeenten en provincies niet een taak van deze gemeentes en provincies. Tegelijkertijd wordt het wel gezien als verantwoordelijkheid. Deze NIS2 wet vraagt om het ook een wettelijke taak te maken voor gemeenten en provincies om te zorgen voor organisaties binnen hun gebied op het gebied van cyberveiligheid.

Is er gedacht aan het verder inregelen van csirt door dit niet alleen landelijk, maar ook op provincie en gemeentelijk niveau in te richten?

Met vriendelijke groet,

Joab de Lang