INPUT PAPER: OBSERVATIES & AANBEVELINGEN

v20240701

ten aanzien van wetsvoorstel Regels ter implementatie van Richtlijn (EU) 2022/2555 (NIS2) betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Europese Unie

A. Introductie

1. Arthur's Legal, Strategies & Systems opereert met name in de Europese Unie (EU), EER, VK, VS en (andere) NAVO bondgenoten en vrienden. We opereren, adviseren, maken mogelijk en faciliteren op gebied van essentiële combinaties van technologie, strategie, impact, ethiek, vrijheid, recht, governance en vertrouwen. Arthur's Legal focust op (inter)nationale en Europese Digital Decade 2030 strategie en beleidsaspecten op gebied van digitaal, duurzaam, veiligheid, digitale soevereiniteit, weerbaarheid en veerbaarheid, zowel voor de publieke sector, private sector en organisaties in andere sectoren.

2. Op het gebied van digitaal leiden ze bepaalde beleidsinitiatieven op EU niveau en elders, op gebied van digitale transformatie, data, computing, cybersecurity, soevereiniteit, veiligheid, datadelen, vertrouwen, dynamische verantwoordelijkheid en aansprakelijkheid. Arthur's Legal is expert-adviseur bij diverse Nederlandse ministeries als de Europese Unie organisaties waaronder mede begrepen de Europese Commissie. Arthur's Legal, Strategies & Systems is op dit moment danwel consortium partners, security advisory board member, ethical board member respectievelijk strategic advisory board member van meer dan 30 Europese projecten in de EU, EER en het VK over data, datadelen, vertrouwen, kritische infrastructuur, digitale ecosystemen – maar bijvoorbeeld ook autonome systemen – veiligheid, privacy, digitale identiteit, interoperabiliteit, risico's, weerbaarheid en andere relevante domeinen en dimensies in deze digitale tijden.

3. Als lid van de EU Alliance for Industrial Data, Cloud & Edge, waar alle EU lidstaten eveneens lid van zijn, samen met nog 49 private organisaties met hoofdkantoor in de EU, net als Arthur's Legal, Strategies & Systems, onder leiding van DG CNECT van de Commissie, leiden we zowel de Digital Sovereignty Taskforce, de Cybersecurity Taskforce en de Common Trust Taskforce.

4. Arthur's Legal, Strategies & Systems heeft ook al in het verleden bijgedragen – in sommige gevallen al meer dan 12 jaar – aan de vormgeving en richtinggeving van NIS, NIS2, CSA, CRA, GDPR, FFDR, DSA, DGA, DIR/eIDAS2 (Digitale Identiteit) en IEA (Interoperabiliteit), en is op dit moment onder meer expert-adviseur van de Commissie wat betreft de DA (Data Act). De risico-gebaseerde respectieve data-centrische en markt-centrische beleidsinstrumenten vormen één groot dynamisch ecosysteem van ecosystemen. De één ander niet los van de ander worden gezien.

5. Voor deze consultatie over het huidige Nederlandse NIS2 implementatiewetsvoorstel (hierna: 'Wetsvoorstel') willen we in dat licht graag de na volgende observaties en aanbevelingen inbrengen.

B. Observaties en aanbevelingen ten aanzien van Wetsvoorstel

1. Harmonisatie in en voor Nederland, en in en voor alle andere EU lidstaten:

Het hoofddoel van de NIS2 Richtlijn is om tot een hoog gezamenlijk Europees niveau te komen van cyberbeveiliging in de Europese Unie, voor en in alle 27 lidstaten inclusief Nederland. Dit mede om te zorgen dat organisaties die binnen de reikwijdte van NIS2 Richtlijn vallen, als ze in Nederland voldoen aan de Nederlandse NIS2 implementatiewet ook aan dat hoge, gezamenlijke basisniveau voldoen op basis van nationale implementatiewetten in andere lidstaten. En, vice versa.

Dat impliceert ook dat er zo weinig mogelijk afwijkingen en uitzonderingen in nationale implementaties dienen te worden opgenomen.

Voornoemde harmonisatie wordt wel genoemd in het concept MvT bij Wetsvoorstel maar de huidige inhoud van het Wetsvoorstel lijkt het primaire principe van harmonisatie niet als primair te hebben genomen. Er staan relatief veel afwijkingen en uitzonderingen in die lijken te zijn gebaseerd op bestaande, en daarmee gedateerde en niet al op de NIS2 Richtlijn en Digital Decade 2023 niveau gebrachte praktijken en wet- en regelgeving. Het is niet aan de NIS2 Richtlijn om zich aan te passen de bestaande praktijken en wet- en regelgeving. Het is echt andersom; de nieuwe wet zoals de NIS2 Richtlijn verhoogt het niveau van bestaande praktijken en wet- en regelgeving.

Het wordt voor Nederlandse organisaties die onder de NIS2 Richtlijn vallen die ook opereren in een of meerdere andere EU lidstaten wel erg lastig – inclusief kostbaar – gemaakt om op Europees niveau te opereren. Dit terwijl, nogmaals, het hoofddoel is om tot een hoog gezamenlijk Europees niveau te komen van cyberbeveiliging in de Europese Unie. Met het huidige Wetsvoorstel wordt dat hoofddoel niet gehaald.

Dat geldt ook voor EU organisaties die onder de NIS2 Richtlijn vallen in een of andere EU lidstaten waaronder ook Nederland.

2. **Alle Gevaren & Titel van Wetsvoorstel:**

De term 'cybersecurity' – en de aard en strekking van de NIS2 Richtlijn – reikt verder in een Engelse vertaling van de letterlijke vertaling ervan, cyberbeveiliging. De term 'cybersecurity' in de oorspronkelijke – Engelstalige – NIS2 Richtlijn is officieel vertaald in het Nederlands naar 'cyberbeveiliging', maar het is de vraag of het verstandig is om het Wetsvoorstel de 'Cyberbeveiligingswet' te noemen.

Dit onder meer omdat zoals hierboven al aangegeven het hoofddoel van de NIS2 Richtlijn om tot een gezamenlijk niveau te komen, maar vooral omdat het conform artikel 21 NIS2 Richtlijn gaat over het nemen van maatregelen die zijn gebaseerd op een benadering die alle gevaren omvat, en tot doel heeft netwerk- en informatiesystemen en de fysieke omgeving van die systemen tegen incidenten te beschermen. Het gaat dus – alleen al kijkend naar artikel 21 NIS2 Richtlijn – niet uitsluiten om cyberbeveiliging, maar ook om cyberhygiëne, bedrijfscontinuïteit, fysieke veiligheid, weerbaarheid en zo verder. Het is zaak om de titel van het Wetsvoorstel te wijzingen danwel al in een van de eerste artikelen van het Wetsvoorstel danwel in het eerste deel van de MvT duidelijk te maken dat het om die 'alle gevaren-gebaseerde' veiligheid gaat, zowel fysiek als anderszins.

Zo moet het onder meer duidelijk zijn en blijven dat het niet alleen om cyberbeveiliging gaat, en dat deze wet dus niet – qua perspectie of anderszins – het unieke domein moet gaan worden van CISO/ISO offices, informatiebeveiliging en dergelijke. Dan kan en mag niet de bedoeling zijn.

Kort en goed is de term cybersecurity niet accuraat en niet volledig, en in die zin wat misleidend.

3. **Van BIO en ISO27k naar NIS2 Good Practices:**

De term BIO, Baseline Informatiebeveiliging Overheid, geeft al aan dat de BIO de lading, aard en strekking van de NIS2 Richtlijn niet dekt. NIS2 gaat immers veel verder dan informatiebeveiliging. Het is op zich goed dat de Baseline Informatiebeveiliging Overheid (BIO) wordt verbeterd, geactualiseerd en verplicht gesteld, maar ze voldoet niet om aan het hoog gezamenlijk Europees niveau te komen onder de NIS2 Richtlijn. Zo dekt de BIO immers maar een paar componenten uit artikel 21 NIS2 Richtlijn. Dat geldt eveneens voor de ISO/IEC 27000 serie.

4. De nieuwe Honeypot: Online Registratievoorzieningen

Waar dingen van waarde zijn c.q. dingen van waarde worden gedeeld, is het goed toeven.

Het is natuurlijk al te voorzien en te voorspellen – en moet gewoon als al vaststaand feit worden gezien – dat de locatie(s) waar de aangegeven online Registratievoorzieningen worden ingericht en aangeboden een hoge mate van interesse zullen genereren. Het is de ideale locatie voor monitoring door, voorbereidingen door c.q. acties van actoren. Dat geldt zowel voor de fysieke locatie(s) ervan, als voor de online locatie(s), en zowel voor en via geautoriseerde organisaties en personen, zowel online als fysiek. Dit is bepaald een heel ander niveau dan een portaal voor het melden van lekken van persoonsgegevens.

Onder meer de Commissie (en JRC) hebben dit bijvoorbeeld zelf ondervonden toen zij in 2021 de European Cybersecurity Atlas online ontsloot (https://cybersecurity-atlas.ec.europa.eu/) ten behoeve van het bouwen van de EU Cybersecurity Competence Community. Binnen zeer korte tijd moest deze – om aanvallen in het domein van voornoemde categorieën – offline worden gehaald, en is sinds dien per saldo ook niet online beschikbaar (https://cybersecurity-atlas.ec.europa.eu/centres-in-europe).

We kunnen er zeker van zijn dat gelijke of gelijksoortige scenario's gaan spelen wat betreft de in het Wetsvoorstel genoemde online Registratievoorzieningen. Dit mede vanwege de huidige geopolitieke situatie maar ook gewoon vanwege het bekende permanente kat-en-muis spel.

5. Duiding en Duidelijkheid

Voor al die organisaties die direct of indirect onder NIS2 Richtlijn en het Wetsvoorstel vallen, en die zich nader willen voorbereiden geeft het Wetsvoorstel te weinig duiding en te weinig duidelijkheid. Andersgezegd is het per saldo nog altijd lastig om:

a. zich goed voor te bereiden, en up-to-date te blijven;

b. om te snappen hoe die (minstens) 10 technische, organisatorische en operationele maatregelen concreet in te vullen als genoemd in artikel 21 lid 2 NIS2 Richtlijn;

c. hoe die maatregelen op het juiste niveau te krijgen en houden op basis van proportionaliteit en evenredigheid als bedoeld in artikel 21 lid 1 ervan;

d. om te bepalen waar het Wetsvoorstel praktisch in danwel uit te pas loopt met andere nationale NIS2 implementatiewetten,

e. om te bepalen hoe het juiste niveau van verantwoordelijkheden kan worden aangetoond, en;

f. om de rechtspositie van bestuursorganen van essentiële en belangrijke entiteiten – zowel publieke, private als andere entiteiten die onder NIS2 Richtlijn en het Wetsvoorstel vallen – als die van de gerelateerde organisaties nuttig te bepalen.

Het feit dat de NIS2 Richtlijn al op 27 december 2022 officieel is gepubliceerd, daarvoor al goed-bekend was, de NIS2 Richtlijn Europees en dus ook in Nederland op 17 oktober a.s. van kracht wordt, en het huidige Wetsvoorstel pas – in concept – op 21 mei jl. is voorgelegd voor deze internet-consultatieronde is dit niet alleen zorgwekkend, en haalt het momentum eruit.

Het belemmert ook het op het juiste niveau krijgen – en houden – van de veiligheid (zowel nationaal, maatschappelijke, economische, persoonlijk, organisatorisch, kennis) in, voor en van Nederland, en die in, voor en van de EU, EEA, VK en andere bondgenoten en bevriende landen, online, in cyber, cyber-fysiek, en fysiek.

C. Bereid tot Nadere Ondersteuning en Bijdragen

Wij zijn en blijven graag bereid om nadere ondersteuning en andere bijdragen te leveren, inclusief om de bovenstaande observaties en aanbevelingen nader te helpen opnemen, praktisch te maken, en te zorgen dat de NIS2 Richtlijn en de uiteindelijke Nederlandse implementatiewet op juiste, solide en voor iedereen duidelijke manier wordt geïmplementeerd, gemonitord èn gehandhaafd.

Dat geldt ook voor het zorgen van overzicht, inzicht en vooruitzicht waar de NIS2 Richtlijn op een of andere wijze aan verbonden is, waardoor het beïnvloed wordt c.q. gaat worden, door welke andere EU wet- en regelgeving en andere beleidsinstrumenten (waaronder Europese programma's en samenwerkingen) ze versterkt wordt, en welke middelen en mogelijkheden dergelijke EU wet- en regelgeving beiden, ten behoeve van de missie en doelstellingen van de NIS2 Richtlijn en de Digital Decade 2030.

We zijn graag bereid het voorgaande desgewenst nader toe te lichten.

Amsterdam, 1 juli 2024 / Arthur's Legal, Strategies & Systems

Een aantal bronnen:

1. https://digital-strategy.ec.europa.eu/en/news/european-alliance-industrial-data-edge-and-cloud-presents-its-first-deliverables
   Roadmap (PDF access): https://ec.europa.eu/newsroom/dae/redirection/document/102590 met name de hoofdstuk 2 (Digital Sovereignty) en Annex 1 bij de Roadmap, en hoofdstuk 4 (Cybersecurity).
   https://www.arthurslegal.com/blog/the-roadmap-of-the-eu-alliance-industrial-data-edge-cloud-has-now-officially-been-presented-and-handed-over-to-the-commission/

2. https://www.concordia-h2020.eu/roadmap/
   Roadmap (PDF access): https://www.concordia-h2020.eu/wp-content/uploads/2021/10/CONCORDIA_Roadmap, in het bijzonder de hoofdstukken 2, 7, 8, 9, 10 en 11 (met, wat dat laatste hoofdstuk betreft - met overzichten – met name de paragrafen: Focus Areas Priorities National Stakeholder Group, en Inter-Pilots (CONCORDIA, SPARTA, ECHO, Cybersec4EU).

3. www.arthurslegal.com/welcome