Stichting Digitale
Infrastructuur Nederland

Reactie DINL Internetconsultatie CbW (cyberbeveiligingswet)

Juni 2024

Stichting DINL is in beginsel positief over deze wet. Het doel van de EU richtlijn, namelijk het bereiken van een hoger niveau van cyberweerbaarheid, is duidelijk herkenbaar. Er is terecht gekozen voor de risk- en principles-based aanpak, zodat organisaties de ruimte hebben om zelf risico's in te schatten en de bijbehorende passende maatregelen te kunnen nemen. Dat schept ruimte voor innovaties, voor eigen keuzes voor invulling in plaats van verplichtingen die niet voldoende bestendig zijn tegen de ontwikkelingen, en voor continue bijsturing op beleid.

Daarnaast is het goed dat het wetsvoorstel inzet op informatieverzameling en -sharing op het gebied van kwetsbaarheden, incidenten en dreigingsinformatie. Zonder betrouwbare, veilige en tijdige informatie kunnen organisaties zich niet optimaal voorbereiden op concrete dreigingen en risico's.

Ook is het rechtstreeks adresseren van bestuurders prijzenswaardig, daarmee kan worden voorkomen dat cyber security (opnieuw) een technische invuloefening wordt.

Tegelijkertijd roept deze aanpak vragen en nieuwe problemen op die in het wetsvoorstel naar ons oordeel nog onvoldoende worden geadresseerd.
In dit document noemen we enkele van deze knelpunten en doen suggesties voor verbeteringen. DINL heeft zich beperkt tot de grote lijnen. Wij herkennen ons voorts in de analyses en input van CvNL (Cyberveilig Nederland), en in die van NL Digital, hun gedetailleerde suggesties zijn eveneens zeer waardevol.

Samenloop, inspecties, ketens en bewijs

De gekozen principle- en risk-based aanpak, met open normen, heeft als voordeel dat organisaties een eigen invulling kunnen geven aan maatregelen voor risicobeheersing. Maar heeft als risico en nadeel dat er een grote verscheidenheid kan, en zonder beleid, zal ontstaan van manieren waarop die concrete invulling plaatsvindt. Erger is, dat daarom elke betrokken organisatie vanwege sectorale overlap en samenloop met andere cyber security wetgeving- en ook elke betrokken inspectie, eigen oordelen en "lijstjes" zullen ontwikkelen over wat er onder "gepaste maatregelen" moet worden verstaan, en wat er van partijen in ketens zal – en kan worden gevraagd.

Dat kan, en zal naar onze mening tot een forse extra regeldruk leiden.
Immers, tel de volgende factoren bij elkaar op:

- Er zijn overlappende wetten met cybersecurity eisen zoals DORA, de AVG, mogelijk de CRA.
- Er is samenloop en overlap van toezichthouders en sectorale inspecties en sectorale wetgeving.
- Het reeds bestaande en vaak toegepaste "right to audit" vanuit de AVG, dat zich ook richt op cyber security
- De behoefte aan zekerheid bij steeds meer ketenpartners
- Het ontbreken van in de EU geharmoniseerde audit- en rapportage standaarden

Maanweg 174
2516 AB, Den Haag
Nederland

Tel: +31 70 762 1070
E-mail: info@dinl.nl

- Een immer groeiende lijst van keurmerken die door belanghebbenden soms als “NIS2 compliant” worden verkocht.

Dat alles zal er onvermijdelijk toe leiden dat organisaties elkaar vaker gaan bevragen, doorlichten, inspecteren of beoordelen op gebied van weerbaarheid. Elk met de eigen – in plaats van een geharmoniseerde bril, simpelweg omdat zo’n bril niet door de overheid of toezichthouders wordt aangereikt.
Dat is onwenselijk. De groeiende stapel keurmerken illustreert het probleem: in plaats van duidelijkheid over de manier waarop wordt gekeken, wordt de oplossing steeds weer gezocht in nieuwe lijsten met eisen; terwijl zelden wordt gekeken naar de kwaliteit van beoordelingen, de rapportages, en daarmee de zekerheden die keurmerken in de praktijk aan interne- en externe stakeholders geven.

Organisaties moeten daarom *dringend* in staat gesteld worden om hun conformiteit aan te kunnen tonen zonder steeds opnieuw maatwerk te moeten leveren, of de effectiviteit van hun beheersingsmaatregelen steeds opnieuw te moeten laten toetsen.
Daar zijn in elk geval standaarden voor de beoordeling van conformiteit voor nodig , Ook zijn er kansen op het gebied van toepasselijkheid van keurmerken. Het EU EUCS is een voorbeeld van een keurmerk met brede, Europese werking, maar ook in NL moet de overheid zich verbinden aan harmonisering van keurmerken en certificeringen.

Aanbevelingen

Een inspanningsverplichting van de overheid om regeldruk tegen te gaan is hier beslist ontoereikend. Toezichthouders zetten weliswaar in op coördinatie en harmonisatie, maar vooralsnog zonder een op de wet gebaseerde taak- of doelstelling. Dat kan beter en explicieter, met de verplichting deze diversiteit en daarmee regeldruk te beperken.
In de wet moet daartoe de verplichting worden opgenomen om diversiteit in de gehanteerde normeringen voor beoordelingen tegen te gaan: i.e. bewijs en informatie over de invulling van gelijkluidende doelstellingen, en liefst ook beoordelingen van de effectiviteit van beheersing, moet – om te beginnen - in elk geval binnen het overheidsdomein herbruikbaar zijn.
In de MvT moet daarbij helder worden gesteld dat wildgroei van uitvragen : i.e. het vragen van verschillend bewijs van conformiteit voor overeenkomende veiligheidsdoelstellingen, ongewenst is, en zal worden tegengegaan door een actieve, coördinerende en harmoniserende beleidsrol van de verantwoordelijke ministeries.

De inspanningsverplichting moet zich in elk geval richten op het normeren van rapportagestandaarden op het gebied van conformiteit. Vergelijk de financiële jaarrekening die inzicht geeft in de mate van financial control van een organisatie: een dergelijke verklaring zal er moeten komen voor digitale control.

Ketenproblematiek

Vaak wordt de vraag gesteld: “Valt een ketenpartij zoals een toeleverancier ook onder NIS2?”, we zien dit ook in andere consultatiereacties terug. We onderschrijven dat de vraag in de wettekst en MvT onvoldoende helder wordt beantwoord.

Onze aanbeveling is, om in de MvT scherper onderscheid te maken tussen horizontale en verticale ketens, enbeter uit te leggen wat het onderscheid is als het gaat om ketenafhankelijkheden met entiteiten die al dan niet met de CbW te maken krijgen:

- Verticale ketens, zoals bij IT service stacks. Verplichtingen, aansprakelijkheden en soms maatregelen, kunnen ook contractueel worden vastgelegd, of worden afgedwongen via het right to audit.
- Horizontale ketens: een organisatie is afhankelijk van data en/of goederen van derden, maar heeft geen invloed op de conformiteit; bijvoorbeeld omdat er geen mogelijkheid is die

via aansprakelijkheden of contracten in te richten. Bijvoorbeeld: de informatiestromen tussen CSIRTS, die afhankelijk zijn van datasets van de overheid.

Of een ketenpartner zelf een CwB gereguleerde partij kan helpen, is voor de keten invulling eigenlijk niet relevant. Ons advies is om dat te benadrukken. Het gaat om realiseren van weerbaarheid in ketens, niet om te zoeken naar lacunes – of uitzonderingen op de wet.

Voor beide typen keten situaties is het noodzakelijk, zie de vorige paragraaf, dat er standaardisatie wordt gerealiseerd met betrekking tot bewijs van conformiteit, om te voorkomen dat partijen elkaar op verschillende manieren gaan bevragen mbt dezelfde risico's en eisen of afhankelijk van elkaar zijn zonder de mogelijkheid van rechtstreekse bevraging - maar toch onvoldoende inzicht hebben in de mate van conformiteit van de ketenpartner.

Cyberweerbaarheidsstelsel

Het is goed dat in dit wetsvoorstel zo'n centrale en stevige rol voor het cyberweerbaarheidsstelsel wordt voorzien. Maar de opzet levert vragen op die in het wetsvoorstel en MvT onvoldoende worden beantwoord

Ten eerste, gaat het voorstel voorbij aan de complexiteit van de governance van een stelsel met schakelorganisaties. Deze organisaties zijn expliciet geen overheidspartijen (anders zou opschalen van NCSC en DTC voldoen), maar ook geen commerciële partijen, immers dan zou de overheid gereguleerde organisaties verplichten om die diensten af te nemen bij de markt. Tegelijk zijn ze wel essentieel voor het realiseren van weerbaarheid, en zijn de CSIRTS, en ook voor hen noodzakelijke databronnen als Shadowserver, DIVD, onafhankelijk van overheid en commerciele belangen en moeten dat ook blijven.

Dan, begrijpen we dat alle bestaande OKTT's schakelorganisatie worden maar niet automatisch relevante partij. Schakelorganisaties worden immers niet genoemd in de wet. Dat betekent dat zij dus niet zonder meer informatie vanuit het NCSC zullen (blijven) ontvangen. En dus ook niet snel en doeltreffend die informatie daar kunnen krijgen waar hij hoort bij hun deelnemers, leden of constituenten. Dat kan leiden tot kapitaalvernietiging en een achteruitgang in informatievoorziening
We vinden het daarom belangrijk dat organisaties die nu al dreigingsinformatie doorzetten op basis van hun OKTT status en daar ervaring mee hebben opgedaan, met het oog op continuïteit niet alleen automatisch schakelorganisatie worden, maar ook relevante partij en in die hoedanigheid hun werkzaamheden voor hun sector kunnen voortzetten. Nu is hier nog een beleidsmatige toets voorzien, die toets kan voor bestaande organisaties dus worden overgeslagen want het zou onredelijk zijn om organisaties die jarenlang hebben geïnvesteerd in informatievoorziening conform wat de CbW nu formaliseert alsnog de status op formele/ procedurele gronden te ontnemen.
Dat geldt binnen onze sector specifiek voor de stichting NBIP en voor SURF, beiden de-facto facto sectorale CSIRTs ; het zou voor de sector een ongewenste ontwikkeling zijn als er een wijziging zou plaatsvinden anders dan die het gevolg is van generieke kwaliteitseisen.

Vragen, en zorgen hierover zijn, kortom:
- Hoe wordt continuïteit van dat stelsel geregeld, nu er open einden zijn voor wat betreft de financiering van partijen die klaarblijkelijk noodzakelijk zijn voor uitvoering van de wet?
- Hoe wordt geborgd dat bestaande OKTT's en schakelorganisaties relevante partijen worden in het nieuwe stelsel.
- Wat zijn de eisen die aan CSIRTS en bronnen zullen worden gesteld, en wie formuleert die eisen en ziet toe op naleving? Is dat voldoende neutraal en vrij van politieke invloed? Het gaat om organisaties die informatie met een hoge mate van vertrouwelijkheid moeten kunnen verwerken om hun rol goed te kunnen vervullen. De concept-wet lijkt vertrouwelijkheid soms te ondermijnen (zie ook CVNL reactie op dit punt).
- Hoe wordt een tweedeling voorkomen – i.e. wordt voorkomen dat slechts CwB gereguleerde organisaties toegang tot de informatie in het stelsel kunnen krijgen, (immers de gedachte

van de wet is bevorderen van weerbaarheid in de breedte, niet de gedachte dat de samenleving ook wel veilig zal zijn is als slechts organisaties die CwB plichtig zijn, de informatie mogen verkrijgen).

Verder is het belangrijk om een level playing field voor CSIRTS in NL en EU te borgen, zodat er geen sprake kan zijn van informatieachterstanden of andere abitraire uitzonderingsposities die ingegeven kunnen worden door politieke wensen.

Aanbevelingen:

- Neem de verplichting op voor de overheid om de continuïteit van het cyberweerbaarheidsstelsel te borgen, ook (en juist) als daar financiële middelen voor nodig zijn.
- Benoem ook de databronnen explicieter. Eventueel kan aansluiting bij de EU Cyber solidarity act worden genoemd, maar sorteer wel voor op een actiever aandeel van de NL overheid voor het eigen NL stelsel om te voorkomen dat de taken en uitvoering worden doorgeschoven naar de toekomst of worden afgeschoven op de EU.
- Neem bestaande OKTT's onverkort op in het stelsel
- Maak de toezichthouder RDI verantwoordelijk voor normering en beoordeling van de (cyber security) van CSIRTS, en leg de lat daarbij hoog.
- Borg het level playing field voor CISRTS, sta geen uitzonderingen toe met betrekking tot hun rechten en informatieposities
- Zorg er voor dat iedere organisatie in principe toegang heeft / krijgt tot het cyberweerbaarheidsstelsel; op basis van profiel en "subscriptions", en uiteraard ook op basis van een onafhankelijke (third party) beoordeling van de kwaliteit van hun vertrouwelijkheid mbt die informatie.
- Hanteer voor die vertrouwelijkheid de gangbare TLP-codering

Andere punten

Dan zijn er nog enkele andere punten die DINL zij opgevallen, we geven hierbij direct de aanbevelingen

- Beperk toezichthouders in hun mogelijkheden om in de warme fase van een incident informatie te vragen. Een getroffen organisatie heeft dan veel aan het hoofd, het is niet de rol van de toezichthouder om in die fase bijstand te verlenen; waarmee gedwongen communicatie met de toezichthouder in die fase al snel contraproductief wordt. De rol van de toezichthouder is met name in de fase voor- en na incidenten.

- Maak het delen van dreigingsinformatie vanuit inlichtingendiensten minder vrijblijvend. Waar een wil is, is een weg om voor NL organisaties essentiële belangrijke informatie te derubriceren. Ook daar telt de kwaliteit van de CSIRTS , Het belang van brede beschikbaarheid van die informatie moet vaker zwaarder wegen dan de inlichtingenpositie van de diensten zelf. Neem daartoe een tekst op met die prioritering in de MvT

- Benoem ook explicieter de optie om niet-commerciële schakelorganisaties die cyberweerbarheidsdiensten bieden op te nemen in het stelsel. Zulke diensten zijn essentieel, en koste wat kost moet voorkomen worden dat door bijvoorbeeld consolidaties alleen de grote commerciële aanbieders in deze behoefte kunnen voorzien, en er door ene te beperkte definitie geen plaats zou zijn voor niet-commerciële, open initiatieven.

- Het op voorhand aanleggen en beheren van een nieuw register van IP adressen lijkt ons riskant , de nut en noodzaak onvoldoende onderbouwd, en lastig te onderhouden. RIPE beheert reeds de toewijzing van IP adressen aan organisaties, en een extra verplichting en register gaat niet noodzakelijkerwijs tot betere kwaliteit leiden. Schijnzekerheid over de toewijzing van IP reeksen kan problemen juist vergroten. De CSIRTS zijn beter dan de overheid in staat vanuit hun directe relatie met hun leden of constituenten informatie daar te krijgen waar het hoort. Zet in plaats van het zoveelste register, steviger in op de

technische mogelijkheden van analyses van ketens. Neem een verplichting op om “meet” en verbeterprogramma’s structureel te financieren en operationeel te houden.

- Schep meer duidelijkheid over het voorkomen van dubbele, driedubbele of zelfs vierdubbele meldplichten: zoals meldingen na incidenten naar toezichthouders, ENISA, CSIRT, de AP. Een inspanningsverplichting voor de overheid om zo’n administratie te voorkomen is tot nu toe vrijblijvend gebleken, het is te vaak gebleven bij formulieren en voornemens.
  Met een resultaatverplichting kan er eindelijk een generiek format voor meldingen komen dat geschikt is voor de verschillende loketten. Neem daartoe de verplichting op om incidenten geautomatiseerd te kunnen melden.

- Zet steviger in op het cyclische, PDCA karakter van beleid, bijsturing op uitvoering en en de AmVB’s. Het is niet alleen voor de gereguleerde organisaties belangrijk om het cyber security beleid en uitvoering continu bij te sturen, dat geldt evenzeer voor het overheidsbeleid zelf. Neem daartoe een kortcyclische evaluatieverplichting op, en regel een vaste governance structuur met de CSIRTS en het maatschappelijke middenveld waarmee beleid en uitvoering worden geëvalueerd en bijgestuurd

DINL, juli 2024