Inbreng Stichting Digitale Infrastructuur Nederland voor de consultatie wijziging WBNI
Augustus, 2021

Inleiding

De Stichting DINL (hierna: **DINL, "wij"**) maakt graag gebruik van de mogelijkheid om te reageren op het voorstel tot wijziging van de WBNI.

Het doel van de wijziging van de WBNI is het NCSC in staat te stellen om voortaan ook aan andere organisaties - die geen vitale aanbieder zijn of deel uitmaken van de Rijksoverheid – dreigings- en incidentinformatie te verstrekken. Op basis hiervan kunnen deze organisaties maatregelen nemen om incidenten te voorkomen of de gevolgen daarvan beperken.

DINL is positief over de richting van het wetsvoorstel. De uitbreiding van het mandaat van het NCSC is noodzakelijk en urgent, zelfs cruciaal. Want het onderscheid tussen vitaal en niet-vitaal is steeds minder scherp te maken en de gevolgen van, door malicieuze actoren geëxploiteerde kwetsbaarheden in systemen, hebben steeds vaker onvoorziene maatschappelijke effecten. Ook andere organisaties dan de overheid en vitale aanbieders hebben daarom dringend behoefte aan actuele informatie over dreigingen en exploiteerbare kwetsbaarheden.

Het gaat hierbij ook om informatie die uitsluitend de overheid (NCSC) op grond van haar status als nationale CERT tot haar beschikking heeft of heeft gekregen en die bedrijven dus niet langs een andere weg kunnen verkrijgen. Die monopoliepositie is een probleem nu alleen het NCSC informatie over Nederlandse netwerken en systemen krijgt, maar deze informatie vervolgens niet kan delen. Door deze beperking hebben vele organisaties in Nederland zich lang niet voldoende effectief kunnen beschermen tegen actuele nieuwe dreigingen. Het feit dat deze kwestie erg lang een effectieve oplossing in de weg heeft gestaan, heeft de overheid beslist geen goed gedaan. Daarom is stichting DINL positief over het feit dat deze impasse nu wordt doorbroken.

DINL wil ook benadrukken dat grote haast geboden is met de invoering van dit wetsvoorstel. Iedere dag dat het NCSC haar rol niet kan pakken, en het LDS niet optimaal werkt, zijn bedrijven kwetsbaarder dan idealiter nodig. En lopen we als maatschappij het risico dat we daar stevige gevolgen van merken. Het is daarom verstandig om nu gezamenlijk te anticiperen op de mandaten en mogelijkheden die deze wet gaat bieden.

Verbeteringen LDS

Naast ons positieve oordeel is er ook kritiek op het voorstel, of liever gezegd, zijn er zorgen over de beperkte scope van de verbreding. Wij vinden het voorstel onvoldoende specifiek, en nog niet compleet. Wij zien de volgende zorgpunten en aanbevelingen graag terug in een aangepast wetsvoorstel.

1. De wet kan nu zodanig worden uitgelegd dat OKTT's nog steeds niet ongevraagd mogen informeren als het uiteindelijke target zich niet (ergens) geregistreerd heeft. Benoem daarom het ongevraagd informeren expliciet.
2. Borg, en mandateer en faciliteer een onafhankelijke rol van NCSC, zoals dat in andere lidstaten gebruikelijk is. NCSC behoort een organisatie te zijn die zelfstandig op het snijvlak opereert van BZK, EZK, V&J, Defensie, markt, en toezichthouders, zonder dat één van die partijen dominant is voor het beleid.
3. Het scenario waarin het NCSC rechtstreeks een organisatie buiten haar doelgroep mag benaderen is nog steeds beperkt. Zo moet er sprake zijn van nadelige maatschappelijke gevolgen, en het niet verstrekken moet tot ernstige verstoring van de beschikbaarheid van de dienstverlening lijden. Daarbij rijst de vraag waar exact de grens ligt.

4. Het aanwijzen van een OKTT via een ministeriële regeling is een zwaardere procedure dan de huidige. De Memorie van Toelichting stelt dat het Ministerie streeft naar werkzame oplossingen, maar de genoemde eerdere ervaringen stellen ons wat dat betreft niet gerust.
5. Er zijn onvoldoende garanties dat de NCSC zodanig wordt gefaciliteerd en gemandateerd dat alle noodzakelijke informatie (zie “bronnen") waar DSP’s behoefte aan hebben voor zichzelf en hun afnemers, kan en mag worden ontvangen, verwerkt en op tijd kan worden doorgestuurd.
6. Het NCSC moet worden gemandateerd, en zelfs worden verplicht om zich ook in te zetten voor de continuïteit van essentiële publieke bronnen, zoals DIVD, Shadow Server, alsmede een verplichting om te zorgen voor een aanbod van informatie naar behoefte van de OKTT’s en bedrijven.
7. Er behoort een verplichting te zijn om ratings (performance rapportages) over Nederlandse netwerken te faciliteren.
8. Een zorg betreft de definitie van “aanbieders", het risico bestaat dat de NIB-definitie leidend is. Daardoor zouden makers en handelaren van producten in plaats van diensten in sommige gevallen buiten de boot kunnen vallen.
   Ook is er sprake van een zekere getraptheid – waarbij de aanbieders die gelinkt zijn aan een andere organisatie/OKTT deze informatie enkel via deze organisatie/OKTT mogen ontvangen en niet direct van het NCSC.
   Wij prefereren een situatie waarbij het NCSC de vrijheid krijgt om zelf een route te kiezen in plaats van een bij wet voorgeschreven getraptheid.
9. Er behoort een verplichting te zijn voor periodieke evaluatie van het functioneren van het LDS, waarbij DSP’s (en andere ontvangers van informatie) een belangrijke stem hebben.
10. Naast de juridische of politieke blokkades die het goed functioneren van het stelsel kunnen blokkeren, bestaat ook het risico dat het NCSC zelf slachtoffer wordt van een aanval. Dat kan (opnieuw)) leiden tot een situatie waarin NCSC haar taken niet naar behoren en naar behoefte kan vervullen. Daarom vinden we het onverstandig om het NCSC als enige nationale CERT te laten fungeren. Zoals dat gebruikelijk is bij weerbaarheidskwesties hoort ook hier een backup, fallback of redundant scenario te zijn.
    Er moet daarom een mogelijkheid komen om andere CERT's een soortgelijke positie te geven als het NCSC. Dat is een situatie die in andere landen ook gebruikelijk is.

Toelichting op functioneren van het LDS voor providers

Om toe te lichten waar het inhoudelijk aan schort maken we een schets van het voor DINL relevante deel van het stelsel, zoals dat volgens DINL moet functioneren. DINL hecht daarbij grote waarde aan de volgende karakteristieken:

- Distributie via NBIP en andere “twee-traps” organisaties
- Ongevraagd informeren
- Ratings
- Bronnen
- Continuïteit

Wij noemen specifiek deze vijf aspecten, ten eerste, omdat die betrekking hebben op bedrijven in onze sector als actoren in het LDS. Ten tweede, omdat juist deze aspecten buitengewoon effectief blijken te zijn. En ten derde omdat ze door de huidige interpretatie van de WBNI, vertaald in beleid, en door tekortkomingen in de operationele uitwerking, niet bestaan of (nog) niet voldoende op stoom zijn. In de volgende sector lichten we deze aspecten toe.

Informatie via NBIP en andere tweetraps-organisaties

Als aanbieders van digitale infrastructuur hebben serviceproviders een sleutelrol in het bestrijden van kwetsbaarheid en verbeteren van weerbaarheid. De WBNI noemt DSP's maar het gaat om alle

soorten aanbieders, inclusief de kleine die niet expliciet onder de WBNI vallen maar wel belangrijke online functies faciliteren, of een rol blijken te hebben in complexe digitale ketens. Dat gaat bij hen niet alleen om de behoefte aan informatie voor een weerbare digitale infrastructuur zelf, maar om het faciliteren van hun afnemers, en daarmee het gehele digitale bedrijfsleven. De online systemen waarover we ons als maatschappij zorgen maken zijn immers te vinden op de servers van providers zoals aanbieders van hosting, cloud en IT diensten. Toegang tot die systemen is via het internet, door netwerken die digitale infra-bedrijven leveren en beheren. Distributie van kwetsbaarheidsinformatie via zulke aanbieders heeft daarom een enorm bereik.

Het NBIP, de coöperatieve sector organisatie die zulke informatie distribueert, bereikt met haar 200 deelnemers ca 45% van het gehele Nederlandse Internet en alles wat daarop draait. De Abuse-Hub van de vereniging ABuse-IX bedient ISP's en telecom providers.
Daarom legt DINL zoveel nadruk op het gevraagd en ongevraagd informatie delen via deze organisaties. NBIP heeft bijvoorbeeld een directe technisch-operationele lijn naar haar deelnemers. Die aangesloten deelnemers hebben op hun beurt een directe operationele lijn naar hun klanten en bereiken zo met twee korte stappen de tienduizenden bedrijven en miljoenen sites, systemen en toegangsnetwerken, waar het hier allemaal om draait. Waar klassieke informatiekanalen via de "voordeur" van een bedrijf zoals de info@-mail, klantenservice, of management, vaak omslachtig en te langzaam zijn hebben deze actoren, in deze ketens, allemaal een technisch handelingsperspectief. Ze weten waar de meldingen over gaat. Via die route kunnen en worden lekken, misbruik en kwetsbaarheden snel worden gemeld en gerepareerd.

Ongevraagd informeren
Daarnaast hechten we grote waarde aan het ongevraagd kunnen informeren. Een bekende vorm van ongevraagd informeren betreft CVD: coordinated vulnerability disclosure, zoals het DIVD dat doet. Daarnaast gaat het om het ongevraagd kunnen informeren van organisaties over hun prestaties op het gebied van schoonhouden van hun netwerken.

De reden dat DINL grote waarde hecht aan ongevraagd informeren is simpel: het is een hoeksteen van bestrijding van kwetsbaarheid. De meeste kwetsbaarheden worden namelijk gevonden bij bedrijven die zich er juist niet bewust van zijn dat ze kwetsbaar zijn, die moeten dan daarop worden geattendeerd door organisaties die de kwetsbaarheden (van buitenaf) zien.
Oorzaken van kwetsbaarheid zijn matig of slecht security management, maar veel vaker te wijten aan een ongelukkige samenloop van omstandigheden.[1] Een fout in een asset management systeem kan ertoe leiden dat een oude softwareversie op een systeem over het hoofd wordt gezien. Een patch die wordt teruggedraaid omdat het systeem na de patch niet meer functioneerde, word door een verkeerde inschatting niet als riskant gezien. Zo zijn er tientallen redenen waarom kwetsbaarheden kunnen bestaan. Dit is de reden dat organisaties als DIVD zo effectief zijn, en een cruciale rol hebben bij het op tijd vinden en melden van kwetsbaarheid[2]. De combinatie van – en samenwerking tussen DIVD en NBIP voor detectie en distributie van actuele kwetsbaarheids informatie, die ongevraagd aan bedrijven wordt verstrekt is cruciaal en moet centraal staan in de uitwerking. Het NCSC behoort ongevraagd informeren te faciliteren en zelfs te stimuleren.

Ratings
Uit onderzoek van TU Delft blijkt dat netwerken van operators met slechte prestaties op het gebied van schoon houden van hun netwerken, zogenaamde "internet bad neighbourhoods", sterk

[1] Zie de diverse publicaties van Prof. M. van Eeten (TuD) over dit onderwerp
[2] DIVD bleek een essentiële schakel bij het detecteren van de recente Kaseya kwetsbaarheid

correleren met de kans dat in zo'n netwerk abuse, of kwetsbare systemen worden aangetroffen. Het proactief, en (dus) ongevraagd periodiek informeren van de organisaties die zulke netwerken leveren en beheren, en (dus) al hun klanten in het netwerk kennen of minstens kunnen bereiken over de mate van badness, blijkt enorm effectief te zijn. Ook hier speelt een rol dat de betreffende organisaties zich vaak niet bewust zijn van hun matige prestaties, en dus niet om de informatie vragen. De combinatie van ratings, het NBIP en de bevindingen van TU Delft rond ongevraagd informeren, blijkt een gouden formule te zijn voor het bestrijden van misbruik, het verminderen van kwetsbaarheid en dus het verbeteren van weerbaarheid.

Bronnen
Voor het maken van ratings, de algemene verbetering van weerbaarheid en het adresseren van specifiek misbruik en kwetsbaarheden blijkt een breed spectrum aan weerbaarheidsinformatie noodzakelijk te zijn. Bronnen als The Shadowserver Foundation, Google Safe browsing, Facebook's feeds, Microsoft informatie, de bevindingen van het DIVD en vele anderen zijn daarvoor allemaal nodig. Ze zijn niet alleen complementair maar geven samen ook een goed beeld van badness, weerbaarheid en kwetsbaarheid. Voor het NCSC geldt: je kunt alleen overzicht krijgen als je al die informatie mag of kan ontvangen. En hoe kan je als NCSC ten tijde van crisis adviseren, als je geen overzicht hebt kunnen opbouwen?Een goed werkend LDS zorgt daarom voor de collectie, aggregatie en distributie van informatie uit veel bronnen. Het NCSC moet dus ook zo breed mogelijk informatie kunnen verzamelen, om vervolgens organisaties breed via het LDS te kunnen informeren.

Continuïteit
Ook moet het NCSC zich in kunnen zetten voor de continuïteit van de bronnen: i.e. de organisaties die de informatie verzamelen en aanleveren, zoals het DIVD, The Shadowserver Foundation en anderen. Immers, onze nationale digitale weerbaarheid hangt af van die informatie, we zijn dus ook afhankelijk van zulke publieke bronnen, soms gerund door vrijwilligers. Daar behoort dus ook een zekere mate van verantwoordelijkheid bij van de overheid. Veelzeggend is dat de EU recentelijk moest bijspringen om The Shadowserver Foundation, die een cruciale informatiebron runt waar NCSC gebruik van maakt (dus waar ook vitale sectoren van afhankelijk zijn), letterlijk voor faillissement te behoeden.

Daarnaast betekent continuïteit ook, dat een LDS met alle betrokken actoren, continu wordt verbeterd en uitgebreid. Immers, de statelijke actoren en criminelen zitten niet stil. Er zullen nieuwe bronnen moeten worden toegevoegd, er is behoefte aan voldoende middelen voor de bronnen, onderzoek, faciliteiten, operationele systemen en de continuïteit van de Publiek-Private samenwerking die het LDS feitelijk is.

Besturing NCSC
Naast de inhoudelijke punten m.b.t. het LDS, zien we ook risico's door de bestuurlijke ophanging van het NCSC. Wij vinden het essentieel dat er een meer onafhankelijke rol komt voor het NCSC. Juist door de huidige opzet werd het NCSC in haar rol beperkt, kan het NCSC haar essentiële rol als nationale CERT en actor onvoldoende invullen, en is de situatie in Nederland anders dan in andere lidstaten. De ervaring van de afgelopen jaren leert ons dat het NCSC als onderdeel van - en met de sterke besturing vanuit het ministerie van Justitie en Veiligheid - niet optimaal kan functioneren. Een sterke nationale CERT, als weerbaarheid- en cybersecurity organisatie moet zelfstandig kunnen acteren op het snijvlak van markt, ministerie van EZK, BZK, Defensie en V&J, toezichthouders, en in een sterk publiek-private setting.
Onze oproep is daarom om die noodzakelijke, meer onafhankelijke rol van NCSC in het wetsvoorstel te verankeren.

Conclusie
Deze wetwijziging geeft het NCSC meer ruimte. Maar dat gaat gepaard met aanzienlijk ingewikkeldere regels voor de uitvoering. De wetswijziging draagt bij aan een moeilijk te doorgronden juridisch kader rond de WBNI. Anders dan in de ons omringende landen heeft het ministerie de eigen uitvoeringswet zo opgesteld en vervolgens geïnterpreteerd, dat die impasses konden ontstaan. De huidige juridische interpretatie van de WBNI door het ministerie van J&V, in samenhang met andere wetgeving, heeft dus gezorgd voor een impasse die dit wetsvoorstel nodig maakt.
In combinatie met de sturing van het NCSC vanuit het ministerie van Justitie en Veiligheid brengt dit voorstel opnieuw een reëel risico met zich mee dat essentiële functies in het LDS alsnog niet mogelijk blijken te zijn. DINL is daarom van mening dat het voorstel onvoldoende garandeert dat de geschetste, gewenste uitwerking realiteit wordt, en blijft.
Het is gezien die juridische complexiteit verstandig om de verplichtingen van de overheid m.b.t. het LDS explicieter te maken. Verder is het organiseren van het LDS rond een monopolie, met een enkele CERT dat aangestuurd wordt door één ministerie, en daarmee single point-of failure wordt, om meerdere redenen onverstandig.

DINL streeft in het algemeen naar wetgeving die ook uitvoerbaar is, en waar, gezien het toenemende PPS karakter van uitvoering, die uitvoering ook minder vrijblijvend is voor de overheid zelf.
Graag denken we met het ministerie mee hoe deze uitvoeringswet nog beter kan worden toegespitst op de problemen die we gezamenlijk willen oplossen, en de gezamenlijke ambitie om de digitale weerbaarheid te verbeteren. En gezien de urgentie moet er ook geanticipeerd worden op deze ontwikkelingen.

Uiteraard zijn we beschikbaar voor een nadere toelichting, en voor acties die anticiperen op deze wet.

Met vriendelijke groet,

Michiel Steltman
Directeur DINL