Inbreng Stichting Digitale Infrastructuur Nederland voor de Internetconsultatie wijziging WBNI , betreffende de aanwijzing van DNS providers als AED's

September, 2022

Inleiding

De Stichting DINL (hierna: **DINL, "wij"**) maakt graag gebruik van de mogelijkheid om te reageren op het voorstel tot aanvulling van de WBNI, voor aanwijzing van DNS aanbieders als AED's. DINL reageert mede namens de VVR (Vereniging van registrars), waaronder de domain registrars die eerder door het Ministerie van EZK over deze voorgenomen wijziging zijn geïnformeerd.

In algemene zin verwonderen wij ons over een regulering die beoogt een risico te managen dat zich in de praktijk nooit heeft gemanifesteerd, en waarvan het niet erg aannemelijk is dat het zich überhaupt zal manifesteren. DNS is een van de meest robuuste, betrouwbare en veilige basistechnologieën van het Internet. Het heeft in de vele decennia dat het zonder overheidstoezicht door DNS providers in NL werd gerund nog nooit problemen opgeleverd. Er valt, kortom, eigenlijk niets te verbeteren aan de betrouwbaarheid van DNS en DNS providers in NL.
Dat wordt nog versterkt door het gegeven dat het bij incidenten bij de veiligheid en beschikbaarheid van specifieke domeinen eigenlijk nooit om storingen gaat op de DNS infra van providers zelf, maar om configuratiefouten in zones – die niet door de provider, maar door de afnemer worden onderhouden.

Tegelijkertijd herkennen we het gevoel van de EU, en de NL overheid dat het ontbreken van toezicht op een service die bij falen potentieel impact kan hebben op vitale ketens wat ongemakkelijk voelt. Met de EU NIS regulering is toezicht op DNS een fait accompli geworden. En nu staan we als sector en overheid gezamenlijk voor de opgave te voorkomen dat er onnodige lastendruk en kosten ontstaan voor providers die op zich nu al een perfecte service verzorgen, en dus blijkbaar de-facto al aan de reguleringsdoelen voldoen. En moeten we gezamenlijk zorgen dat er geen negatieve effecten van deze horizontale regulering op de markt ontstaan. Daarnaast is het zaak ons te richten op potentiële conflicten met- en negatieve effecten van de aankomende Europese NIS(2) reguleringen en de bijbehorende certificeringen die voortvloeien uit de combinatie van NIS2 en CSA, en de onderhavige DNS regulering.

In deze reactie sommen we onze zorgen en observaties op.

Omvangscriterium

Wat ons opvalt is dat de gekozen wijze van reguleren horizontaal is van karakter. Er is geen onderscheid naar het daadwerkelijk gebruik van de geregistreerde domeinen. Wij hebben daarom vraagtekens bij dat voorgenomen criterium, dat lijkt nogal arbitrair gekozen te zijn. Het komt er nu op neer dat wanneer 1 provider 400.000 .nl domeinen op z'n DNS servers heeft , er impliciet wordt gesteld dat er dan flinke impact kan zijn, maar dat er bij een incident bij een provider met 399.000 .nl domeinen niets is waar de overheid iets van zou moeten vinden.

De realiteit is dat er talrijke kleinere DNS providers zijn met een veel geringer aantal domeinen die gebruikt worden binnen ketens in energie, voedselproductie, zorg. Terwijl juist de grotere providers zich richten op de onderkant van de markt: doorgaans niet vitale toepassingen, lagere prijzen, waarbij de spreekwoordelijke bakker op de hoek dik tevreden is met een domein bij zo'n grote provider met een lagere prijs, en er bij eventuele uitval voor hem geen schade is.
Het ontbreken van die gerichtheid en differentiatie zorgt er voor dat de regulering feitelijk z'n doel voorbij schiet: het draait uit op een horizontale regulering die juist de partijen in niet-vitale ketens

treft, en de partijen die wel onderdeel zijn van vitale ketens, buiten schot laat. Dat kan niet de bedoeling zijn.

Verder begrijpen we niet goed waarom voor een inperking tot alleen .nl is gekozen. Essentiële diensten beperken zich niet zich niet tot het .nl. domein (of andere Europese TLD's). TLD's zoals .com, .shop, spelen ook in Nederland een belangrijke rol.

Daarnaast wordt er naar onze mening onterecht geen onderscheid gemaakt in het daadwerkelijke gebruik van domeinen. Geparkeerde domeinen : i.e. domeinen die wel geregistreerd zijn , en met een enkele, identieke verwijzing in de DNS zones zijn opgenomen (ze verwijzen naar een sales pagina e.d.), en dus niet daadwerkelijk door afnemers gebruikt worden, zouden moeten worden uitgesloten.

De scope van de regulering zou uit moeten gaan op het daadwerkelijk gebruik van domeinen in (vitale, essentiële) economische ketens, en daarmee, uit moeten gaan van een differentiatie in service levels. Dat sluit ook aan bij de opzet van de aankomende EU -CSA certificeringen, die in de NIS2 uitvoering een dominante rol zal gaan spelen: met levels basic, substantial en high.
Afnemers die vitale diensten draaien, en dus onder "High" zullen vallen, begrijpen heel goed dat er een gereguleerde DNS dienst moet worden afgenomen, tegen een bijbehorende prijs. Terwijl de eerder genoemde bakker of vereniging, kan volstaan met een domein in level "basic", met andere voorwaarden en lagere prijs. Met die aanpak zou het DNS regime veel beter aansluiten bij de EU regulering, en wordt de markt niet verstoord.

Certificeringsperikelen

Een andere zorg betreft de regeldruk in de praktijk. Veel voorbeelden laten zien dat intenties voor het laag houden van regeldruk in de praktijk compleet anders uitpakken, door, bijvoorbeeld, een eigen invulling door de toezichthouder.
In deze regulering worden bij de beoordeling van de impact de kosten voor de meldplichten vermeld. Verder wordt er gesteld dat, omdat er al sprake is van hoge kwaliteit bij de doelgroep (lees: ISO27001 certificeringen), er geen extra kosten voor providers zullen zijn, anders dan het documenteren van de bestaande praktijk.

Dat uitgangspunt : hergebruik van bestaande certificeringen en documentatie, vinden we prima. Alle providers in de doelgroep hebben inderdaad al bestaande certificeringen zoals de ISO27001.
Gegeven het feit dat met deze bestaande certificeringen de DNS services bij de doelgroep probleemloos en veilig draait, zou het kunnen overleggen van deze certificering voor deze groep dus inderdaad moeten kunnen volstaan. Anders houdt de stelling dat er geen sprake is van (extra) uitvoeringskosten, geen stand. Immers, in de praktijk komen de kosten van compliance niet voort uit het nemen van risicobeheersingsmaatregelen (die zijn inderdaad al genomen), maar uit de doorgaans forse overhead van audit trajecten en bijbehorende documentatie, als een toezichthouder specifieke eisen stelt aan dat bewijs. Dat kan al snel gaan om kosten van tienduizenden tot meer dan €100.000.
Wij lezen in deze uitleg en verantwoording van de lage uitvoeringskosten dan ook de impliciete toezegging in dat het kunnen overleggen van een gedocumenteerde ISO27001 certificering, in de praktijk zal volstaan voor de betreffende toezichthouder. Graag zien we daarom hiervan de extra, expliciete bevestiging in de regeling; c.q. ander bewijs dat in de praktijk niet alsnog nieuwe uitvoeringskosten als gevolg van nieuwe eisen bij het toezicht, zullen ontstaan.

Tegelijkertijd maken we ons als sector, dat zal niemand zijn ontgaan, grote zorgen over de naderende ontwikkelingen met betrekking tot het aangekondigde EUCS (European Cloud Scheme),

dat door ENISA wordt ontwikkeld. De meeste (DNS) providers zullen ook met dat EUCS te maken gaan krijgen, omdat de EU definitie van Cloud, erg breed is, en omdat veel registrars ook DSP's zijn. Het is echter nog onzeker of, en hoe , (andere) toezichthouders de EUCS certificering als adequaat voor meerdere andere reguleringen en toepassingen zoals deze, zullen hanteren. Dat maakt de inschatting dat er daadwerkelijk gebruik zal worden gemaakt van de bestaande regimes bij betreffende providers, ook vanuit deze ontwikkeling, onzeker.

Het EUCS maakt ook onderscheid tussen levels basic, substantial en high. Dat sluit aan bij ons eerdere punt dat er sprake zou moeten zijn van differentiatie naar gebruik van domeinen in de ketens, in plaats van de horizontale aanpak. Mocht het EUCS inderdaad in beeld komen voor betreffende providers, dan wordt de differentiatie naar type gebruik de norm voor diensten. Daarom zien we graag de toezegging tegemoet dat niet, als gevolg van deze DNS regulering, alle meer dan 400.000 domeinnamen, de-facto alsnog in "EUCS High" zullen gaan vallen omdat de gehele dienst, en daarmee alle domeinen in de dienst, ook die van afnemers die slechts voor basic of substantial zouden willen betalen, als essentieel waren aangewezen.
Tevens zien we met betrekking tot de voornoemde intentie tot hergebruik, ook graag de expliciete bevestiging, dat in de praktische uitwerking van deze voorgestelde scope verruiming, een eventuele verplichting voor EUCS certificering ook voor deze DNS regulering zal volstaan als bewijs van conformiteit.

Verder wijzen wij graag op het scenario dat zich zal aandienen als deze regulering ondanks de toezeggingen toch extra kosten gaat leiden. Ondernemers reduceren risico's voor hun klanten, maar ook voor zichzelf. Het is voorstelbaar, zelfs zeer waarschijnlijk, dat, als er sprake zou zijn van een nieuw / of een apart handhavingsregime met nieuwe regels, audits en dus met bijkomende hoge kosten, of voor "EUCS High", betreffende ondernemers moeite zullen doen om het aantal geregistreerde .nl domeinen onder de grens van 400.000 te houden, of te gaan brengen. Dat zou er toe kunnen leiden dat de regulering geen effect heeft, en dat betreffende ondernemers nog steeds geen gebruik kunnen maken van informatie en ondersteuning van NCSC en andere overheidsdiensten, geen meldingen zullen hoeven doen.

Kort en goed, stellen we voor om het voorstel op volgende punten aan te passen:

- Herzie het criterium 400.000 .nl domeinen. Differentieer , aansluitend bij de EU definities, naar gebruik van domeinen in basic, substantial en high
- Kijk niet alleen naar .nl, maar naar alle in NL gangbare TLD's , zodat een level playing field in de NL markt behouden blijft
- Neem het daadwerkelijk gebruik van geregistreerde domeinnnamen in ogenschouw, en sluit geparkeerde domeinen uit
- Met betrekking tot kosten en impact: Leg de stelling dat er van bestaande ISO certificeringen van providers gebruik gemaakt zal worden, expliciet vast, zodat niet later alsnog nieuwe regimes met bijkomende hoge kosten in beeld kunnen komen die alsnog voor hoge kosten gaan zorgen
- Als voor beoogde providers ook het EUCS zal gelden, borg dat EUCS certificering ook voor deze toepassing geldigheid zal hebben

Uiteraard zijn we beschikbaar voor een nadere toelichting, en voor het bespreken van de verdere details en uitwerking.

Met vriendelijke groet,

Michiel Steltman

Directeur DINL / mede namens de VVR