



Reactie van Internet Society Nederland op de internetconsultatie van de *Regeling veiligheid en integriteit telecommunicatie*

Een open, toegankelijk en betrouwbaar internet is onmisbaar geworden in onze samenleving. Voor Internet Society Nederland is het essentieel dat het internet die karakteristieken blijft behouden.

Met de komst van vijfde generatie mobiele netwerken is een aanscherping van de zorgplicht voor netwerkaanbieders een logische en goede stap. De voorgestelde beheersmaatregelen beschrijven doelstellingen om daartoe te komen en zijn wat dat betreft een stap in de goede richting. Echter, als beheersmaatregelen schieten ze op dit moment tekort.

De voorgestelde beheersmaatregelen zijn te generiek geformuleerd om effectief te kunnen zijn. Het ontbreekt aan elke vorm van normatieve verplichting en op basis van de huidige formulering is niet vast te stellen wanneer is voldaan aan de beheersmaatregelen. Woorden als 'minimaliseren', 'zo snel mogelijk', of 'actief toezien' geven enige richting maar geen enkele duidelijkheid of zekerheid. Het gevaar is dat met het aannemen van de beheersmaatregelen een schijnzekerheid veroorzaakt wordt. Ook ontbreekt het aan een heldere evaluatiebepaling, om de beheersmaatregelen periodiek te herijken; wat in een continu ontwikkelend domein als deze onontbeerlijk is. Het grootste probleem, tot slot, is dat niet duidelijk is welke concrete risico's, consequenties en andere impact de maatregelen moeten beheersen. Door die stap over te slaan en een aantal beheersmaatregelen voor te schrijven zonder aan te geven waarom, is niet alleen onduidelijk of deze doeltreffend zijn, maar ook of ze gerechtvaardigd zijn.

In het bijzonder vragen we aandacht voor de volgende zaken:

- De genoemde maatregelen lijken vrij willekeurig te zijn. Ze dekken in ieder geval niet alle relevante gebieden, risico's, mogelijk negatieve impact, en andere aspecten af. Verder zijn sommige maatregelen wat gedateerd, en zijn ook niet per definitie effectief: zo is bewustzijn/awareness niet meer zozeer een maatregel; het aanpassen van gedrag wel.
- Het is niet duidelijk wat de term 'beschermen' zoals, gebruikt in de concept-regeling, behelst. De notie van veiligheid en integriteit gaat veel verder dan alleen beschermen ('protect'). Het zou expliciet moeten worden gemaakt dat beheersmaatregelen ook in de andere fasen noodzakelijk zijn. Denk minimaal aan de klassieke vijf fasen (Identify, Protect, Detect, Repond, Recover), zoals het National Institute of Standards and Technology die hanteert - hoewel ook die in onze ogen niet volledig genoeg zijn. Elke fase noodzaakt andere maatregelen, en die moeten continue worden hergewaardeerd, uitgedaagd en aangepast.
- Het is goed dat de software-componenten worden genoemd, inclusief software-updates, maar zonder duidelijkheid en meetbaarheid voegt het als beheersmaatregel weinig toe. Het testen van een software-update in een testomgeving geeft an sich geen waarborgen over de runtime die de in productieomgeving zit. Verder is het aantal updates in deze netwerken zeer omvangrijk, en zullen deze eerst getest moeten worden op afhankelijkheden met ander delen van het netwerk of gerelateerde systemen.
- Een belangrijk specifiek punt waar meer duidelijkheid essentieel is, is de implementatie-eis bij C.2: dataretentie. Dataretentie, inclusief metadataretentie, is vanzelfsprekend en al geruime tijd een gevoelig domein, waar zeer zorgvuldig, gedoseerd en transparant mee moet

worden omgegaan. Zo is het niet duidelijk wat de exacte reden en grondslag en exacte belang is voor maatregel C2, of die wel correct is (inclusief nuttig, noodzakelijk, disproportioneel en beheersbaar), en of en hoe die grondslag wordt afgewogen tegen andere belangen.

- Voor de netwerkaanbieders zal niet duidelijk zijn wanneer zij de beheersmaatregelen naar behoeven geïmplementeerd hebben. Die onduidelijkheid is een probleem in zichzelf voor de netwerkaanbieders. Maar negatief geformuleerd betekent het bovendien dat elke netwerkaanbieder zelf kan stellen dat zij netjes aan de genoemde beheersmaatregelen heeft voldaan ('compliant is'). Omdat een minimumniveau, monitoring en sancties niet vastgesteld zijn, is de toezichthouder afhankelijk van de inschatting van de gecontroleerde partij. Dat vergroot de veiligheid en integriteit van deze vitale infrastructuur niet.

Dit alles overwegende, adviseren wij u het volgende:

- beargumenteer voor elke beheersmaatregel welk(e) specifieke risico, consequentie of impact de maatregel zou moeten beheersen en waarom die maatregel daarvoor het juiste en proportionele middel is;
- maak de beheersmaatregelen normatief en meetbaar;
- neem een evaluatiebepaling op die recht doet aan de ontwikkelingen in dit domein, bijvoorbeeld elke 6 maanden;
- maak duidelijk welke sancties er verbonden zijn aan het onvoldoende implementeren van de beheersmaatregelen;
- Leg de wijzigingen opnieuw voor ter consultatie.

Het staat buiten kijf dat het internet als vitale infrastructuur beschermd moet worden tegen kwaadaardige bedreigingen. Maar door de enorme hoeveelheid ruimte die de beheersmaatregelen nu laten en de schijnzekerheid die ze geven, is de betrouwbaarheid en veiligheid van het internet in onze ogen alsnog in het geding. Alleen door de risico's en beheersmaatregelen zorgvuldig en specifiek te formuleren, kunnen de ze echt bijdragen aan een sterker, veiliger en veerkrachtiger internet.

Namens het bestuur van de Vereniging Internet Society Nederland,

Alexander Blom

Deze reactie kwam tot stand met inbreng van expert Arthur van der Wees