Consultatie van het voorontwerp voor het

Besluit meldplicht cybersecurity

Reactie van KPN

KPN
Contactpersoon: Drs. W.M. Hoogeveen
Postbus 30 000
2500 GA Den Haag
maurice.hoogeveen@kpn.com

Kenmerk: RG/17/U/002

16 mei 2017

Inleiding en samenvatting

Cybersecurity is en blijft een grote uitdaging voor Nederland. Elke dag zijn er incidenten met hacks, spionage en (maatschappelijke) schade door cybercriminaliteit. KPN zet zich daarom ten volste in om onze diensten, producten en interne ICT te beschermen tegen cyberdreigingen.

De ontwikkelingen in het cyberdomein vragen om goede en realistische wetgeving om de vitale infrastructuren in Nederland te beschermen en maatschappelijke ontwrichting te voorkomen. KPN juicht het daarom toe dat de overheid hier steeds meer aandacht voor heeft.

Toch zijn er bij het concept Besluit meldplicht cybersecurity verschillende kanttekeningen te maken. Vanuit de rol die KPN heeft zullen wij ons richten op het deel van het besluit dat gaat over elektronische communicatienetwerken of –diensten/ICT. De belangrijkste opmerkingen staan onderstaand vermeld en worden verderop nader uitgewerkt.

Het conceptvoorstel mist een brede benadering van telecommunicatie- en internetrouteringsdiensten. In het voorliggende voorstel wordt niet onderbouwd waarom

1. De uitval van sms- en telefoniediensten en internetknooppunten bij één partij zal leiden tot maatschappelijke ontwrichting;
2. De bij punt 1 genoemde diensten wel meldplichtig zijn terwijl vergelijkbare diensten, hard- en softwareleveranciers in de ICT-keten en Over The Top (OTT)-diensten dat niet zijn.

Er zijn verschillende alternatieven voor sms- en telefoniediensten en internetknooppunten. Dat betekent dat er redundantie is die is gecreëerd door concurrentie in de markt. Dit is niet alleen op netwerkniveau, maar ook door het aanbod van diensten die in het voorliggende voorstel niet onder de meldplicht vallen. Een groot deel van de in Nederland gebruikte telecommunicatiediensten en internetroutering vindt bij deze alternatieve diensten plaats. In het geval van telefonie- en tekstdiensten zijn dit OTT-diensten zoals Whatsapp en Skype en in het geval van de routering van internetverkeer zijn dit bijvoorbeeld IP-transitdiensten en *private network interconnects*.

De voorgestelde regulering lijkt te ‘traditioneel’ te zijn opgezet. Het voorstel reguleert met name telecompartijen gevestigd in Nederland, terwijl een groot deel van vergelijkbare diensten door internationale partijen wordt aangeboden, elders plaatsvindt en buiten de wettelijke verplichting valt. Daarbij wordt groot deel van de keten in deze voorgestelde regulering niet ondervangen, zoals de hard- en software die essentieel is voor sms- telecom- en internetdiensten.

Het gevolg hiervan is dat telecompartijen te maken krijgen met nog een aanvullende meldplicht, waardoor de administratieve lasten worden verhoogd. De andere bovengenoemde partijen ondervinden deze lasten niet. Dit creëert een verder ongelijk speelveld. Deze meldplicht lijkt daar in eerste instantie gering aan bij te dragen, maar voegt nog een laag regelgeving toe aan de zwaar gereguleerde telecomsector, dat niet in verhouding staat met partijen die vooral OTT-diensten aanbieden en daarmee direct concurreren met telecompartijen. Daarbij creëert de meldplicht een schijnveiligheid,

omdat met dit voorstel slechts een deel van de communicatiedienstverlening in Nederland met meer dan één miljoen gebruikers een meldplicht krijgt opgelegd.

Suggesties KPN:

- Onderbouw de gemaakte keuzes voor partijen en diensten die onder de meldplicht vallen nader. Kijk hierbij beter naar marktontwikkelingen, redundantie in infrastructuren en alternatieve vergelijkbare diensten;
- Reguleer partijen en diensten niet wanneer er voldoende alternatieven bestaan, in redundantie en/of alternatieve diensten;
- Gelijke regels voor gelijke diensten: bij regulering SMS/telefonie ook regulering van vergelijkbare OTT-diensten, idem voor alternatieven voor internetknooppunten en vertrouwensdiensten;
- Maak hard- en softwareleveranciers die die essentieel zijn voor het leveren van telefoon-, sms- en internetdiensten aan eindgebruikers ook meldplichtig;
- Vertrouwensdiensten moeten ook meldplichtig worden gemaakt, omdat er anders een ongelijk speelveld is tussen Nederlandse leveranciers van vertrouwensdiensten en buitenlandse leveranciers.

Het conceptbesluit beperkt zich tot een enkele sector en mist een brede benadering

Het conceptvoorstel betoogt dat sommige processen zo vitaal zijn voor de Nederlandse samenleving dat uitval of verstoring tot ernstige maatschappelijke ontwrichting leidt en een bedreiging vormt voor de nationale veiligheid.[1] Het voorstel wijst vervolgens partijen aan in de sector elektronische communicatienetwerken of –diensten/ICT met één miljoen gebruikers op telefoon-, sms- of internettoegangsdiensten. Vanuit deze redenering en zoals grotendeels aangegeven in het voorstel, zouden dit KPN, VodafoneZiggo, T-Mobile Tele-2 en Eurofiber zijn. Op het gebied van de afhandeling van het internetverkeer wordt gekozen om internetknooppunten (AMS-IX en NL-ix) onder de meldplicht te laten vallen.

Er wordt terecht verwezen naar de toenemende onderlinge verwevenheid van vitale infrastructuur, waardoor blijvende aandacht voor het verhogen en borgen van de weerbaarheid van de vitale infrastructuur noodzakelijk is.[2] Echter, in de uitwerking wordt verwezen naar een lijst van vitale sectoren uit 2012,[3] waarbij de verwevenheid van de sector elektronische communicatienetwerken of-diensten/ICT, evenals die van internetknooppunten met andere sectoren niet nader wordt blootgelegd. Er zijn in de markt verschillende vergelijkbare diensten, maar die op een technisch andere manier functioneren. Deze diensten bedienen op zichzelf een (groot) deel van de markt en dienen tevens als substituut voor telefonie, SMS, en internetknooppunten. Daarbij zijn er op infrastructuurniveau alternatieven beschikbaar.

Alternatieve diensten SMS en telefonie

Alternatieve diensten voor telefonie en SMS zijn OTT-diensten zoals Skype (telefonie) en Whatsapp (tekst). De laatstgenoemde wordt meer gebruikt dan SMS-diensten en zou in dezelfde redeneringslijn van het beoogde voorstel (boven één miljoen Nederlandse gebruikers) ook als vitaal moeten worden aangemerkt. Echter, OTT-diensten en telefonie/SMS kunnen elkaar ook opvangen wanneer één van deze diensten niet meer functioneert. OTT-diensten zijn namelijk afhankelijk van een (mobiele) internetverbinding, onafhankelijk van spraak of SMS-diensten. De drempel tot het gebruik van deze diensten is daarbij erg laag.

Het voorliggend voorstel kiest echter, zonder te beargumenteren, om alleen netwerkgebonden diensten te reguleren. Dit terwijl, zoals bovenstaand aangegeven, er ook niet-netwerkgebonden (OTT)-diensten zijn die vrijwel dezelfde dienst leveren. Ook wordt niet aangetoond dat bijvoorbeeld het uitvallen van SMS-dienstverlening bij één partij zal leiden tot ernstige maatschappelijke ontwrichting. Het feit dat er alternatieven zijn op zowel netwerk- als dienstniveau wordt hierbij niet meegenomen. Als de uitval van SMS ontwrichtend is, dan zou de mogelijke uitval van een vergelijkbare dienst die in Nederland op grotere schaal wordt gebruikt (Whatsapp) mogelijk leiden tot nog grotere ontwrichting. Bij OTT-diensten als Skype is dit minder het geval, maar het is wel een alternatief voor telefonie.

[1] Voorontwerp voor het Besluit meldplicht cybersecurity, pagina 4
[2] Idem.
[3] Deze wordt overigens sinds 2015 geupdate, maar is nog niet klaar. Deze bevat belangrijke wijzigingen ten aanzien van de versie uit 2012.

Alternatieve diensten internetknooppunten

Ook voor internetknooppunten zijn alternatieven beschikbaar. Het voorliggend voorstel beargumenteert dat internnetknooppunten tot *mogelijk* 25 procent van het Nederlandse internetverkeer afhandelen. Dat betekent dat ongeveer driekwart van het Nederlandse internetverkeer via andere kanalen naar hun eindbestemming wordt gerouteerd. Dit gaat bijvoorbeeld via IP-transitdiensten en *private network interconnects*. Er zijn in de markt dus voldoende alternatieven voor het afhandelen van internetverkeer. Het voorliggend voorstel gaat hier niet op in en legt niet nader uit waarom internetknooppunten wel aan de meldplicht moeten voldoen en IP-transitdiensten, bijvoorbeeld, niet.

Daarbij wordt in het voorliggende voorstel betoogd dat het uitvallen van één van de twee Nederlandse internetknooppunten (AMS-IX of NL-ix) ontwrichtende gevolgen kan hebben voor de Nederlandse maatschappij. Los van het door het voorliggende voorstel zelf al aangegeven beperkte marktaandeel van het internetverkeer dat via deze knooppunten loopt en de bovenstaand aangegeven alternatieven, is het niet aangetoond dat bij uitval van de genoemde internetknooppunten de capaciteit van andere knooppunten onvoldoende zou zijn om het internetverkeer op te vangen.[4] Zowel AMS-IX als NL-ix hebben een (veel) grotere aangesloten poortcapaciteit in Tb/s dan het feitelijke verkeer dat dagelijks wordt verwerkt.[5] Daarnaast kunnen partijen ook terugvallen op IP-Transit diensten als alternatief. Het is daarom niet voor de hand liggend dat uitval van één van de knooppunten tot maatschappelijke ontwrichting zal leiden. Het in het voorstel opgenomen criterium om internetknooppunten met een poortcapaciteit van 8 Tb/s als meldplichtig aan te wijzen is daarbij niet onderbouwd en lijkt willekeurig gekozen. Onduidelijk is ook of deze volume geldt voor activiteiten die in Nederland plaatsvinden of dat deze ook geldt voor buitenlandse activiteiten van de internetknooppunten.

Hard en softwareleveranciers

Het voorliggend voorstel stelt dat de partijen die niet een directe dienst aan eindgebruikers aanbieden, maar die wel essentieel kunnen zijn in de keten van het verlenen van telefoon-, sms- en internetdiensten aan eindgebruikers, onder de reikwijdte van de meldplicht vallen. KPN is daarom van mening dat wanneer een dienst via voorliggend besluit wordt gereguleerd, de meldplicht met de bovengenoemde ketenredenering ook moet gelden voor de leveranciers van hard- en software die essentieel zijn voor het leveren van telefoon-, sms- en internetdiensten aan eindgebruikers. Dit zijn bijvoorbeeld leveranciers van browsers, modems en routers. Op dit moment is het niet mogelijk om deze partijen melding te laten maken van bijvoorbeeld een hardware- of softwarekwetsbaarheid, terwijl dit in sommige gevallen daadwerkelijk de dienstverlening van aanbieders van telefoon-, sms- en internetdiensten kan verstoren. Om te zorgen dat de bovengenoemde diensten zo veilig mogelijk blijven is het nodig dat deze informatie zo spoedig mogelijk met partijen met vitale infrastructuur worden gedeeld. Als dit niet gebeurt dan dekt de meldplicht cybersecurity niet de volledige keten.

---

[4] Voorontwerp voor het Besluit meldplicht cybersecurity, pagina 11.

[5] https://ams-ix.net/: piekverkeer: 5.513 T/bs, connected capaciteit 23.4014 T/bs; https://public.nl-ix.net/: piekverkeer: 1.77 T/bs, connected capaciteit 9.5 T/bs.

Vertrouwensdiensten

Belangrijke digitale diensten zijn vertrouwensdiensten zoals PKI-overheid, beveiligingscertificaten en authenticatiediensten. Wanneer deze diensten worden geconfronteerd met een cybersecurityincident, dan kan dat grote gevolgen hebben voor de veiligheid en integriteit van deze diensten met als mogelijk gevolg het tot stilstand komen van een groot deel van de digitale dienstverlening van de private- en overheidssector. Nederland is tijdens de Diginotar-affaire bekend geworden met dergelijke incidenten. Het is daarom opmerkelijk dat dergelijke diensten niet zijn opgenomen in de voorliggende AMvB. Met name omdat Nederlandse bedrijven die vertrouwensdiensten leveren deels meldplichtig zijn, terwijl buitenlandse concurrenten deze verplichting niet hebben. Ook hier is het nodig om dezelfde regels op te leggen aan dezelfde soort diensten om het gelijke speelveld en de veiligheid te borgen.