Ministerie van Economische Zaken en Klimaat
Staatssecretaris van Economische Zaken en Klimaat
Hare Excellentie mevrouw Mona Keijzer

UW REFERENTIE
CONTACTPERSOON Afdeling Governance, Risk & Compliance
TELEFOON
DATUM 16 december 2020
ONDERWERP Consultatie Regeling veiligheid en integriteit telecommunicatie

Hooggeachte mevrouw Keijzer,

Hierbij treft u de reactie van T-Mobile Netherlands BV (**T-Mobile**) op de consultatie van de 'Concept-Regeling veiligheid en integriteit telecommunicatie tbv internetconsultatie versie 6 november 2020' (de **Regeling**).

Inleiding

Vanaf eind 2018 is T-Mobile actief betrokken bij de totstandkoming van de Regeling. Vanaf het begin hebben wij ons sterk gemaakt voor een aanpak op basis van een gezamenlijke risico afweging gefundeerd op een industrie 'best practice'. Concreet hebben wij de *Information Risk Analysis Methodology* (IRAM)[1] methode van het *Information Security Forum* (ISF)[2] aangedragen.

De interdepartementale Taskforce Economische Veiligheid (**Taskforce**) heeft TNO een analyse laten uitvoeren die zij 'risicoanalyse' noemt. T-Mobile interpreteert de methode van TNO echter als een dreigingsanalyse. De uitvoering van de dreigingsanalyse is voor ons niet transparant geweest en de uitkomst is ook een andere dan uit onze risicoanalyse is gekomen.

[1] https://www.securityforum.org/tool/information-risk-assessment-methodology-iram2/
[2] https://www.securityforum.org/

T-MOBILE NETHERLANDS BV
Adres: Waldorpstraat 60, 2521 CC Den Haag
Postadres: Postbus 16272, 2500 BG Den Haag
Telefoon: +31 (0)6 1409 5000 | Fax: +31 (0)6 1409 5024 | Internet: www.t-mobile.nl
Bank: Commerzbank Amsterdam 73.39.59.717 | KvK: Den Haag, 33265679

In het vervolgtraject heeft TNO maatregelen gedefinieerd om de geconstateerde dreiging voor de Staat der Nederlanden te mitigeren tot een door de Staat geaccepteerd niveau. De maatregelen worden aangeduid als *aanvullende* maatregelen. De aanvullende maatregelen komen bovenop de maatregelen die T-Mobile al neemt op basis van artikel 11a.1 lid 1 van de Telecommunicatiewet (Tw).

De Taskforce heeft slechts beoordeeld of de reeds door de MNO's genomen maatregelen in opzet voldoende effectief zijn tegen de betreffende dreiging. Er is geen onderzoek gedaan naar de werking van de door T-Mobile gehanteerde baseline tegen de dreiging. Op basis van deze theoretische exercitie worden er aanvullende maatregelen vereist, zonder dat op enig moment is gebleken dat de werking van de door T-Mobile gehanteerde baseline onvoldoende is.

Om van dit stelsel van maatregelen een consistent geheel te maken hebben wij ons ook hier sterk gemaakt om een bestaande Industrie 'best practice' te gebruiken, bijvoorbeeld ISO/IEC 27002, NIST SP 800-53 of Baseline informatiebeveiliging Overheid[3] (BIO).

De Taskforce heeft echter besloten met deze Regeling een eigen en geheel nieuwe Nederlandse standaard te ontwikkelen, specifiek voor dit onderwerp. Hieronder vindt u in meer detail onze belangrijkste bezwaren, uitgewerkt per onderwerp.

De Regeling is niet gebaseerd op open standaarden

De informatiebeveiliging van T-Mobile is gebaseerd op verifieerbare open standaarden en industrie 'best practice'. Dit heeft verschillende voordelen. Op deze manier liften we mee met de internationale community die de standaarden steeds herijkt en naar een hoger niveau tilt. Daarnaast hebben ons buitenlands moederbedrijf en onze leveranciers kennis van deze standaarden en spreken daardoor dezelfde taal. De Regeling is niet gebaseerd op een dergelijke standaard en bevat ook geen link naar een internationale standaard. Dat maakt deze regeling tot een nieuwe, specifiek ontwikkelde standaard.

[3] https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/informatieveiligheid/kaders-voor-informatieveiligheid/baseline-informatiebeveiliging-overheid/

Deze nieuwe en specifiek ontwikkelde standaard in de Regeling zal door de overheid apart onderhouden moeten worden om aan te blijven sluiten bij de ontwikkelingen in het veld van informatiebeveiliging en de constant veranderende dreigingen. Dit onderhoud van de standaard brengt kosten met zich mee die ons inziens niet door de overheid kunnen worden afgewend op T-Mobile.

Voor deze regeling is een specifieke scope van maatregelen gekozen die zouden passen bij de huidige dreiging. Mocht daar in de toekomst verandering in komen dan zal de Regeling aangepast, en vermoedelijk uitgebreid, moeten worden, wat weer extra kosten en inspanning met zich meebrengt. Fysieke maatregelen zijn bijvoorbeeld nu niet meegenomen. Deze zijn niet van toepassing verklaard voor de dreiging die ten grondslag ligt aan deze Regeling. Zij vormen echter wel een belangrijke pijler tegen andere dreigingen en het is niet ondenkbaar dat deze in een toekomstige versie van deze Regeling alsnog van toepassing worden.

Het niet gebruiken van open standaarden gaat tegen het beleid van de overheid zelf in[4]. De Nederlandse overheid hanteert een openstandaardenbeleid omdat open standaarden bijdragen aan interoperabiliteit en leveranciersonafhankelijkheid. Het gebruik van open standaarden in ICT-systemen bespaart bovendien kosten en verlicht administratieve lasten. In de Regeling is volgens T-Mobile onvoldoende gemotiveerd waarom nu van dit beleid wordt afgeweken.

Doordat er geen open standaard ten grondslag ligt aan de Regeling verschilt de diepgang van de beschreven maatregelen van elkaar. Voor encryptie worden in de Regeling bijvoorbeeld gedetailleerde (overigens onvolledige) toetsbare criteria gehanteerd. Voor screening ontbreken zulke criteria. Daarnaast zal T-Mobile de regeling moeten vertalen naar een taal die ons moederbedrijf en onze leveranciers ook spreken, wat bij een industrie ‘best practice’ niet nodig is.

Bij aanbestedingstrajecten van de overheid wordt normaal gesproken gebruik gemaakt van een basisnormenkader (BIO) dat gebaseerd is op een open standaard zoals in het hierboven genoemde beleid wordt bedoeld. Uit een recent ontvangen marktverkenning van het ministerie van Justitie & Veiligheid blijkt dat voor dezelfde reikwijdte als deze Regeling een analyse is gemaakt van het

[4] https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/standaardisatie/open-standaarden/

vereiste beveiligingsniveau voor een vitaal systeem met weerstand tegen statelijke actoren waar informatie wordt verwerkt op het niveau van ‘departementaal vertrouwelijk'. Uit die analyse komt een andere set van maatregelen naar voren dan in deze Regeling. Kennelijk hanteert de overheid andere normen als klant dan als toezichthouder voor dezelfde reikwijdte: BIO als klant, maar de Regeling wanneer zij toezichthouder is. Hierdoor kan een situatie ontstaan dat een implementatie van de(zelfde) dienstverlening voor Justitie en Veiligheid op basis van de BIO wordt afgekeurd door het Agentschap Telecom.

Rule based

Artikel 3, sub 3 van de Regeling stelt *“In afwijking van het tweede lid kan de minister op aanvraag van de netwerkaanbieder ontheffing verlenen van een of meer implementatievereisten binnen een beheersmaatregel”.* Een dergelijke “Rule based” regeling zal de innovatie binnen T-Mobile en de sector in het algemeen tegenwerken. Dit draagt het risico in zich dat bepaalde MNO’s zich zullen beperken tot het uitvoeren van wat door de Staat verplicht is gesteld, zonder verdergaande stappen te nemen.

In de huidige situatie onderzoeken wij al constant of onze beveiligingsmaatregelen efficiënter en effectiever kunnen, ook indachtig artikel 11.1a Tw. Daarnaast houden wij de ontwikkelingen op het gebied van nieuwe dreigingen nauwlettend in de gaten en zullen wij maatregelen die niet efficiënt of doeltreffend zijn vervangen door andere maatregelen.

De ontheffingsprocedure zoals in de Regeling staat, betekent effectief dat deze innovatie-drive nu bij de overheid komt te liggen, omdat een ontheffing op een naleving die niet op een open standaard is gebaseerd onvoldoende zekerheid levert voor onze eigen innovatieve plannen. Ook zal dit proces een vertraging van 12 weken oplopen in afwachting van een reactie van de Minister. T-Mobile is erg benieuwd hoe de Minister deze afweging gaat maken en of het kostenaspect en de concurrentiepositie van T-Mobile daarin worden meegenomen. Daarnaast zal de Minister ook de verder genomen maatregelen, die niet in de Regeling staan, moeten meenemen in de afweging zodat het volledige stelsel van maatregelen, holistisch wordt beoordeeld op de effectiviteit en er niet slechts naar een individuele maatregel wordt gekeken. Dat zou immers voorbij gaan aan de “layered defence”-benadering die veel partijen in de markt gebruiken.

Wat T-Mobile betreft ligt het meer voor de hand om MNO's achteraf te controleren op het bereiken van gestelde doelstellingen, waarbij een "pas-toe-of-leg-uit" op een open standaard een goede baseline is. Hiermee maakt de overheid maximaal gebruik van de innovatieve kracht van de marktpartijen en is er sprake van een samenwerking tussen overheid en marktpartijen, in plaats van een overheid die door haar zelf gedefinieerde maatregelen oplegt. Deze aanpak sluit ook volledig aan bij het beleid van de overheid inzake de BIO.

Wat de doelstellingen zijn volgt overigens niet uit de Regeling. Deze zouden wat ons betreft sowieso nog toegevoegd moeten worden om te verduidelijken waartoe bepaalde maatregelen dienen. Uiteraard kunnen die doelstellingen dan ook worden gebruikt voor toetsing achteraf of MNO's met de genomen afwijkende maatregelen (pas-toe-of-leg-uit) voldoende invulling geven aan de doelstellingen.

Evaluatie moment ontbreekt

In de toelichting bij de Regeling staat "*Indien op een gegeven moment de indruk bestaat dat bepaalde implementatievereisten niet meer goed passend zijn als gevolg van nieuwe technologische ontwikkelingen, kan op den duur ook overwogen worden de regeling aan te passen*." Wij stellen voor om een jaarlijkse formele periodieke evaluatie van de maatregelen die in de Regeling staan onderdeel te maken van de Regeling. Op dat moment kan worden vastgesteld of de maatregelen, de scope en opzet nog passen bij het korte en lange termijn dreigingsbeeld.

Gezien de snelheid van de veranderingen in het dreigingslandschap en de stand van de techniek enerzijds en de doorlooptijd van het proces om te komen tot passende maatregelen anderzijds, is een formeel evaluatie proces van toegevoegde waarde om tijdig te kunnen inspelen op trends. De totstandkoming van deze Regeling nam al 2 jaar in beslag. De doorlooptijd is een issue, zeker in combinatie met het "Rule Based" punt hierboven, waarbij slechts kan worden geïnnoveerd op basis van toestemming vooraf.

T-Mobile is ook van mening dat de regeling zelf een evaluatiemoment verdient. Worden de doelstellingen behaald en blijkt de Regeling in de praktijk werkbaar? Zo zal een tussentijdse evaluatie kunnen vaststellen of deze systematiek past bij de snelle en complexe wereld waarin we

opereren en waar we nu bezig zijn maatregelen aan te passen op dreigingen en techniek van morgen. Een evaluatiemoment zou bijvoorbeeld een jaar na publicatie van de Regeling kunnen plaatsvinden.

Hoe om te gaan met veranderende dreiging

De optelsom van de 3 hierboven beschreven punten: de Regeling is niet gebaseerd op open standaarden, is 'Rule based' en bevat geen evaluatie moment, maakt de Regeling een statisch document. Dat sluit niet aan op de dynamische wereld van de telecommunicatie waar de technische ontwikkelingen zowel aan de kant van de aanvaller als aan de kant van de netwerkaanbieder zeer snel gaan. Dit vertraagt een tijdige reactie op veranderende dreigingen en werkt als een remmende factor op de innovatie van nieuwe diensten en beveiligingsmaatregelen en is daarmee ook niet te rijmen met de ratio achter art. 11a.1 Tw. Daarnaast speelt nog dat we geen of nauwelijks zicht hebben op de dreiging die de overheid in dezen ervaart. Door structureel dreigingsinformatie vertrouwelijk uit te wisselen kunnen wij efficiënter op de belangen van de overheid in spelen. Wij hebben diepgaande (internationale) kennis en ervaring van telecomnetwerken en weten dus als geen ander hoe die effectief en efficiënt te beveiligen tegen dreigingen die de overheid ons aanreikt.

Geen vergoeding voor kosten

In de toelichting bij de Regeling staat *"De netwerkaanbieders hebben een inschatting gemaakt van de regeldruk: tezamen bedragen de eenmalige investeringen ca 17 à 21 mln, de structurele jaarlijkse kosten bedragen ca 8 à 10 mln*". De in de Regeling genoemde aanvullende beveiligingsmaatregelen komen in veel gevallen bovenop de maatregelen die T-Mobile al neemt vanuit de risicoafweging op de continuïteit van de eigen bedrijfsvoering, en de zorgplicht op grond van artikel 11a.1 Tw. In een aantal gevallen wordt T-Mobile door de overheid gedwongen te beschermen kritieke gegevens te bewaren, terwijl daar voor de bedrijfsvoering geen noodzaak toe is. T-Mobile vraagt zich bovendien af of de Minister wel bevoegd is T-Mobile te dwingen tot deze kosten, en meent (los van de bevoegdheidsvraag) dat aan alle kosten vanuit deze Regeling tegemoet moet worden gekomen in het kader van een nadeelcompensatie (zonder aftrek). Op dit moment wordt, gebaseerd op het Besluit veiligheid en integriteit van telecommunicatienetwerken, nog op geen enkele manier tegemoet gekomen aan een vergoeding van investeringen die moeten worden gedaan voor het nemen van aanvullende maatregelen.

Het niet gebruiken van een open standaard werkt op diverse punten kostenverhogend en zal uiteindelijk in de marktprijzen gaan doorwerken. Naast de onderhoudskosten van het constant vertalen en aan laten sluiten op internationale standaarden die klanten, leveranciers en moederbedrijven vragen, zullen leveranciers ook hun prijzen verhogen om specifieke compliance activiteiten op deze nieuwe regeling te ontplooien.

Implementatie datum

"*De netwerkaanbieder draagt uiterlijk 1 oktober 2022 zorg voor het treffen van noodzakelijke beheersmaatregelen als bedoeld in de eerste kolom van de bijlage*." Hierbij is uitgegaan van een publicatie op 1 oktober 2020. Door vertraging van het proces is die datum niet gehaald, de deadline voor deze consultatie is immers al 16 december 2020. Tevens komen er potentieel uit de consultatie nog belangrijke punten waardoor nog meer vertraging ontstaat. We stellen voor om de in de Regeling opgenomen ingangsdatum aan te passen en vast te houden aan een termijn van 2 jaar vanaf definitieve publicatie. Door alle onzekerheid op dit dossier kan T-Mobile niet beginnen met implementatie van de thans voorgeschreven aanvullende maatregelen voordat e.e.a. definitief is.

Toetsingskader

Op dit moment ontbreekt een toetsingskader. In combinatie met de verschillende diepgang en het niet gebruiken van open standaarden is het voor T-Mobile en de sector moeilijk om in te schatten of men aan de regeling voldoet. De ruimte voor interpretatie die zo ontstaat creëert geen gelijk speelveld tussen de MNO's. Daarnaast maakt het ontbreken van een toetsingskader het extra moeilijk om in het kader van een meningsverschil enige vorm van geschilbeslechting toe te passen.

In de uitvraag *regeldruk beveiligingsmaatregelen telecom van 27 mei 2020* is sprake van "*Om dit te kunnen toetsen verwacht de toezichthouder 2 x per jaar hiervoor een inspectie uit te voeren*." In deze Regeling staat echter niets over toetsingsmomenten of de frequentie daarvan. Wat is momenteel het voornemen van de toezichthouder voor het toetsen van deze aanvullende maatregelen en hoe wordt dit vormgegeven?

Met vriendelijke groet,
Martijn Ronteltap
Director Governance Risk & Compliance