BCPA

BCPA reageert graag naar aanleiding van het wetsvoorstel 'Wet melding inbreuken elektronische informatiesystemen'. BCPA ('Business Communication Providers Alliance') is een samenwerkingsverband van BT Nederland N.V., Colt Technology Services B.V. en Verizon Nederland B.V. op het gebied van regelgeving en toezicht.

Deze aanbieders leveren (netwerk)diensten aan grote ondernemingen en overheidsinstanties. Security- en risk management diensten vormen een belangrijk onderdeel binnen het diensten portfolio van BT, Colt en Verizon. Betrouwbare netwerken en communicatiediensten zijn in het grootzakelijke marktsegment cruciaal.

BCPA deelt de ambitie van de rijksoverheid om de digitale veiligheid waar mogelijk te vergroten. BCPA waardeert de publiek-private samenwerking binnen de overheid en de vitale sectoren op dit terrein. Niettemin roept het wetsvoorstel enkele vragen op.

1. Wie moet melden?

Het wetsvoorstel is van toepassing op bij algemene maatregel van bestuur aan te wijzen aanbieders van nader aan te wijzen producten of diensten. Het zal gaan om producten of diensten die van zodanig belang zijn voor de Nederlandse samenleving dat onderbreking van de beschikbaarheid of betrouwbaarheid daarvan kan leiden tot ernstige maatschappelijke gevolgen. De vraag welke producten of diensten en welke aanbieders dit precies zal betreffen moet nog worden beantwoord.

Het ligt voor de hand dat wordt aangesloten bij het in 2009 geactualiseerde overzicht[1] van alle vitale sectoren, producten en diensten. Gezien de snelheid waarmee veranderingen plaatsvinden binnen de sector telecom/ICT moet de vraag welke elementen binnen deze sector vitaal zijn opnieuw worden beantwoord. De telecom/ICT sector ontwikkelt zich in hoog tempo zodat het denkbaar is dat bepaalde producten of diensten die in 2009 als vitaal zijn gekwalificeerd dit thans niet langer zijn (en andersom).

1 Tweede inhoudelijke analyse bescherming vitale infrastructuur;
http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2010/02/26/analyse-bescherming-vitale-infrastructuur.html

2. In welke gevallen moet worden gemeld?

Blijkens de wettekst moet gemeld worden 'een inbreuk op de veiligheid of een verlies van integriteit van (...) informatiesysteem waardoor de beschikbaarheid of betrouwbaarheid van een product of dienst in belangrijke mate wordt of kan worden onderbroken.' Deze omschrijving biedt BCPA onvoldoende inzicht in de reikwijdte van deze meldplicht.

In de Memorie van Toelichting wordt uitgelegd dat de meldplicht in dit wetsvoorstel alleen ziet op een 'daadwerkelijke inbreuk op de veiligheid en op een daadwerkelijk verlies van integriteit van een elektronisch informatiesysteem. Het wetsvoorstel ziet niet op verstoringen waarbij geen sprake is van een dergelijke ICT-inbreuk, zoals DDoS-aanvallen'.

Ook deze term 'ICT inbreuk' is onvoldoende helder. Van een ICT inbreuk is kennelijk geen sprake wanneer slechts de bereikbaarheid van een ICT dienst (zwaar) wordt aangetast. Wanneer systemen worden aangetast kan wel worden gesproken van een ICT inbreuk. Uit de Memorie van Toelichting lijkt te volgen dat hoe langer een inbreuk duurt, hoe meer sprake is van een ICT-inbreuk:

> *'veelal zal het bij deze (*DDoS, toevoeging BCPA*) aanvallen bovendien om een tijdelijke beperking van de bereikbaarheid gaan. Hierdoor is de maatschappelijk ontwrichtende werking in deze gevallen in het algemeen veel beperkter dan in geval van daadwerkelijke ICT-inbreuken.'*

BCPA vreest dat het begrip 'ICT inbreuk' in de praktijk lastig hanteerbaar zal blijken te zijn. Het verdient aanbeveling om de reikwijdte van de meldplicht scherper af te bakenen.

3. Waar moet worden gemeld?

Voor aanbieders van openbare elektronische communicatienetwerken en -diensten in Nederland gelden binnenkort vier verschillende elkaar deels overlappende meldplichten met drie verschillende loketten[2]. Dit voorstel voegt nog een meldplicht toe aan het rijtje. Ook de Europese wetgever bereidt wetgeving voor[3]. Nederland loopt dus voor de muziek uit met de onderhavige meldplicht. Voor aanbieders die in meerdere

2 Vgl. artikel 11a.2 Tw., artikel 11.3a Tw., artikel 14.6 lid 2 Tw. en - nog niet in werking getreden - artikel 34a Wbp.

3 ontwerp van een Netwerk- en Informatiebeveiligingsrichtlijn (NIB-richtlijn, COM(2013) 48

landen actief zijn en voor wie verschillende meldplichten gelden, zoals BT, Colt en Verizon, is geharmoniseerde regelgeving binnen Europa echter van groot belang.

BCPA dringt aan op stroomlijning van meldprocedures. In een crisissituatie zal alle aandacht van een getroffen aanbieder in beginsel uitgaan naar de maatregelen ter beëindiging van de crisis. Er zal weinig tijd zijn voor bestudering van een flink uitdijende lappendeken aan wetgeving met betrekking tot meldplichten. Aanbieders moeten in een crisissituatie snel kunnen handelen. Het verdient dan ook aanbeveling om een enkel loket in te richten in plaats van drie. Het bestaande loket meldplicht telecom[4] volstaat wat BCPA betreft. Dit loket kan alle mogelijke meldingen in ontvangst nemen en deze waar nodig doorleiden naar de bevoegde instantie.

4. Vertrouwelijke informatie

Artikel 4 van het onderhavige wetsvoorstel bepaalt dat de aanbieder desgevraagd 'alle overige gegevens' verstrekt die nodig zijn om risico's in te schatten of om de aanbieder bij te staan. Op grond van artikel 6 kunnen de verstrekte gegevens worden gebruikt voor het geven van informatie en advies aan andere aanbieders, aan een computercrisisteam en aan het publiek.

BCPA meent dat deze verplichting tot het verstrekken van informatie met waarborgen moet worden omkleed. Alleen die gegevens die evident noodzakelijk zijn in het kader van de voorlichtende taken van het NCSC zouden onder het bereik van deze bepaling moeten vallen. Onduidelijk is voorts waarom alleen in geval van een verstrekking van gegevens aan het publiek is bepaald dat de gegevens niet herleidbaar mogen zijn tot afzonderlijke aanbieders, producten of diensten (in artikel 6). Waarom geldt deze restrictie niet wanneer informatie wordt doorgeleid naar andere aanbieders?

De Memorie van Toelichting vermeldt dat organisaties waarvoor de meldplicht gaat gelden niet terughoudend zouden moeten zijn met het verschaffen van informatie. De vertrouwelijke omgang met informatie moet dan wel goed geregeld zijn.

4 http://www.meldplichttelecomwet.nl

5. Het nut van meldplichten

BCPA onderschrijft als gezegd de ambitie van de rijksoverheid om de digitale veiligheid waar mogelijk te vergroten. Het nut van de vele meldplichten zal moeten blijken. Het is wenselijk dat de effectiviteit van de meldplichten wordt geëvalueerd. Op basis van de resultaten van een evaluatie kan worden besloten over het instandhouden of het afschaffen van de meldplichten.
