

BCPA

Ministerie van Veiligheid en Justitie
Directie Wetgeving en Juridische Zaken
Postbus 20301
2500 EH Den Haag

Amsterdam, 4 maart 2015

Betreft: consultatie Wet gegevensverwerking en meldplicht cybersecurity

Geachte dames en heren,

Hierbij reageer ik namens BCPA naar aanleiding van het op 22 januari jl. gepubliceerde wetsvoorstel gegevensverwerking en meldplicht cybersecurity¹.

BCPA is een samenwerkingsverband van de in Nederland actieve dochterondernemingen van BT Group, Colt Technology Services en Verizon Enterprise Solutions. Deze aanbieders leveren wereldwijd netwerk- en IT-oplossingen aan multinationals, overheidsinstellingen en grote ondernemingen.

BCPA waardeert de uitbreiding van het wetsvoorstel met regels over de verwerking van persoonsgegevens door het NCSC en met regels over de verstrekking door het NCSC van vertrouwelijke gegevens aan derden. De aangebrachte verbeteringen hebben de kritiek van BCPA op het wetsvoorstel echter niet volledig kunnen wegnemen.

¹ Wet houdende regels over het verwerken van gegevens ter bevordering van de veiligheid en de integriteit van elektronische informatiesystemen die van vitaal belang zijn voor de Nederlandse samenleving en regels over het melden van ernstige inbreuken

BCPA

De kritiek van BCPA betreft de volgende drie onderwerpen:

1. de onduidelijke reikwijdte van de meldplicht,
2. de lappendeken van meldplichten, en:
3. het nut van meldplichten in het algemeen.

Hieronder volgt een bespreking van deze onderwerpen.

1. De reikwijdte van de meldplicht

Wie moet melden?

De vitale aanbieders en de concrete producten en diensten, die onder het bereik van de verplichting komen te vallen, zullen worden aangewezen bij algemene maatregel van bestuur. BCPA wordt graag in de gelegenheid gesteld om zich uit te laten over de vraag welke producten en diensten in dit verband als vitaal moeten worden aangemerkt. De toelichting bij artikel 1 stelt terecht dat de meldplicht niet per se voor alle vitale aanbieders hoeft te gelden.

Wat moet worden gemeld?

De meldplicht ziet op een daadwerkelijke inbreuk op de veiligheid of een daadwerkelijk verlies van integriteit van een elektronisch informatiesysteem. De gekozen formulering biedt onvoldoende inzicht in de reikwijdte van de meldplicht. In de toelichting wordt een uitwerking aangekondigd. Zonder uitwerking hangt deze meldplicht in de lucht. BCPA stelt het op prijs dat de telecomsector bij de uitwerking zal worden betrokken. Gezien de haast die de minister kennelijk ervaart begrijpt BCPA niet goed waarom de uitwerking op zich laat wachten. Wij komen hier op terug.

2. Lappendeken van meldplichten

In de telecomsector is een wildgroei van meldplichten ontstaan. De toelichting stelt een efficiënte inrichting van processen in het vooruitzicht. Verschillende processen zullen worden gestroomlijnd. Een eerste bezwaar in dit verband is dat niet duidelijk wordt gemaakt hoe deze processen in de praktijk zullen worden vormgegeven. Aanbieders hebben behoefte aan heldere regels en processen. Zij moeten in een crisissituatie snel kunnen handelen. Het wetsvoorstel voorziet niet in deze behoefte.

Een tweede bezwaar is dat vooruit wordt gelopen op de EU-richtlijn over netwerk- en informatiebeveiliging (NIB-richtlijn). De noodzaak van een Nederlandse regeling, vooruitlopend op de EU-richtlijn, was van meet af aan afwezig. Volgens de minister kan niet worden gewacht op Europese besluitvorming. De haast die de minister kennelijk ervaart blijkt echter niet uit zijn tempo. Er zijn bijna vier jaren verstreken sinds de motie Hennis-Plasschaert werd aangenomen door de Tweede Kamer. De uitwerking van dit wetsvoorstel laat nog altijd op zich wachten. Kennelijk is de urgentie toch niet zo hoog. De urgentie is zeker niet zo hoog dat de EU-richtlijn niet kan worden afgewacht.

BCPA ziet een goede reden om wel te wachten op de EU-richtlijn: het belang van geharmoniseerde wetgeving binnen de Europese Unie. Dit belang wordt sterk gevoeld door aanbieders die internationaal opereren, zoals BT, Colt en Verizon. Wanneer dit belang uit het oog wordt verloren moeten deze aanbieders wegwijz proberen te worden in een lappendeken van verschillende cybersecurity meldplichten in verschillende EU-lidstaten. In Nederland was al een lappendeken van meldplichten inzake cybersecurity, continuïteit en datalekken ontstaan. Het wordt op deze manier steeds lastiger voor internationale aanbieders om te kunnen voldoen aan de vele verplichtingen.

BCPA pleit voor uitstel van de onderhavige meldplicht totdat de NIB-richtlijn van kracht zal zijn. Voorkomen moet worden dat de nu voorgestelde meldplicht al na korte tijd dient te worden gewijzigd.

3. Het nut van meldplichten

BCPA waardeert de ambitie van de rijksoverheid om de digitale veiligheid te vergroten. Het nut en de effectiviteit van de verschillende meldplichten zijn echter niet evident. BCPA pleit daarom voor een verplichte evaluatie van meldplichten en van de onderhavige meldplicht in het bijzonder. Op basis van de resultaten van een evaluatie moet worden besloten over de toekomst van meldplichten.

4. Conclusie

BCPA deelt de zorg van de overheid met betrekking tot de digitale veiligheid. De bevoegdheid om (aanvullende) meldplichten op te leggen moet niettemin terughoudend worden aangewend, met oog voor de effectiviteit van de verplichtingen. De vraag in hoeverre meldplichten daadwerkelijk effectief zijn moet nog worden beantwoord. Harmonisatie van verplichtingen binnen de EU is van groot belang.

Ik vertrouw erop u met het bovenstaande voldoende te hebben geïnformeerd. Deze reactie bevat geen vertrouwelijke informatie.

Met vriendelijke groet,



Niels van Veen,
secretaris BCPA