VNO NCW

MKB Nederland

Zijne excellentie
mr. dr. K.H.D.M. Dijkhoff
Demissionair staatssecretaris van Veiligheid en Justitie
Postbus 20301
2500 EH DEN HAAG

Briefnummer
17/10.791/Ma/Ven

Onderwerp
Concept reactie consultatie

Den Haag
13 juli 2017

Telefoonnummer

E-mail

Excellentie,

VNO-NCW en MKB-Nederland maken graag gebruik van de mogelijkheid te reageren op het conceptvoorstel voor de cybersecuritywet. Dit voorstel behelst de implementatie van de Europese richtlijn voor netwerk- en informatiebeveiliging (NIB-richtlijn) die tot doel heeft om de digitale veiligheid voor vitale infrastructuren en digitale dienstverleners te versterken. Tevens zijn de bepalingen uit het wetsvoorstel gegevensverwerking en meldplicht cybersecurity (WGMC) beleidsneutraal in het wetsvoorstel opgenomen.

Wij hebben bij twee eerdere gelegenheden uitgebreid gereageerd op de consultatie van de WGMC. Belangrijke overwegingen daarin waren dat bij de meldplicht hulp en bijstand voorop staan en dat is voorzien in een regeling die vertrouwelijke omgang met de gevoelige informatie waarborgt. De vertrouwelijke omgang met gevoelige informatie verbetert en versterkt de samenwerking tussen partijen, waardoor deze beter zijn geïnformeerd en zich beter kunnen wapenen tegen allerlei vormen van digitale aanvallen en dreigingen. Dit alles draagt bij aan de gewenste *just culture*, i.e. een cultuur die aanmoedigt om cyberincidenten vrijwillig te melden.

Vooruitlopend op de invoering van de WGMC hebben bedrijven uit de vitale infrastructuur de handschoen reeds opgepakt en krijgt de publiek-private samenwerking op het gebied van cybersecurity meer en meer gestalte, veelal binnen NCSC-verband. Wij dringen erop aan de implementatie van de NIB-richtlijn zo vorm te geven dat deze positieve ontwikkeling wordt versterkt en voortgezet.

In dit verband vragen we in het bijzonder uw aandacht voor de volgende zaken:

Vertrouwelijkheid van informatie moet zijn geborgd
In artikel 19 is vastgelegd hoe wordt omgegaan met de verstrekking van vertrouwelijke gegevens door het NCSC. De bijzondere openbaarheidsregeling is van groot belang; de gedeelde informatie is immers bedrijfsvertrouwelijk en veelal zeer gevoelig van aard. Deze informatie moet niet via een WOB-verzoek of anderszins openbaar gemaakt kunnen worden. Dit zou de betrokken bedrijven uiterst kwetsbaar maken voor gerichte aanvallen en kan, indien het informatie van bedrijven uit de vitale infrastructuur betreft, in het slechtste scenario zelfs leiden tot risico's voor de nationale veiligheid en tot maatschappelijke ontwrichting.

Artikel 19 is vrijwel identiek overgenomen uit de WGMC. Echter, met de Cybersecuritywet krijgt niet alleen het NCSC, maar ook de bevoegde autoriteit de beschikking over deze informatie. Immers, ingevolge deze wet moeten incidenten zowel bij het NCSC als direct bij de bevoegde autoriteit worden gemeld en ook moeten beide worden geïnformeerd over de getroffen tegenmaatregelen en de maatregelen om herhaling te voorkomen. Daarnaast is in artikel 23 de mogelijkheid opgenomen dat de bevoegde autoriteit aanbieders van essentiële diensten een beveiligingsaudit oplegt om te onderzoeken dat de aanbieder heeft voldaan aan haar zorgplicht. De rapporten hiervan worden verstrekt aan de bevoegde autoriteit. Het is cruciaal dat onder het regime van de Cybersecuritywet geborgd blijft dat deze informatie niet door derden kan worden opgevraagd via een WOB-verzoek.
Wij verzoeken daarom dat de bijzondere openbaarheidsregeling van artikel 19 in het voorontwerp uitdrukkelijk wordt verruimd naar alle bevoegde autoriteiten, naar het CSIRT voor digitale diensten en voorts van overeenkomstige toepassing wordt verklaard op artikel 15 en 23. Ook verzoeken wij dat in de memorie van toelichting apart aandacht wordt besteed aan het belang voor de digitale veiligheid van deze verruimde bepaling.

Eén meldingssysteem voor verschillende meldplichten
Bedrijven zijn of worden met een groot aantal verschillende meldplichten geconfronteerd die betrekking hebben op dezelfde omstandigheid of gebeurtenis en die elk hun eigen formats en tijdlijnen kennen. Dit brengt een forse administratieve belasting voor het bedrijfsleven met zich. Er zijn gevallen bekend waarin binnen het getroffen bedrijf meer mensen bezig waren met de melding aan de verschillende toezichthouders, dan met het oplossen van het incident zelf. Dat is een ongewenste

situatie. De ingevolge de Cybersecuritywet te melden incidenten zullen in voorkomende gevallen ook moeten worden gemeld aan de Autoriteit Persoonsgegevens.

VNO-NCW en MKB-Nederland ondersteunen het in de Memorie van toelichting opgenomen voornemen om dubbele meldplichten zodanig vorm te geven dat bedrijven met één handeling aan beide meldplichten kunnen voldoen. Wij dringen erop aan ook nader te onderzoeken of overige meldplichten, waaronder die bij de Autoriteit Persoonsgegevens, kunnen worden meegenomen in een intelligent meldingssysteem waardoor bedrijven slechts één keer hoeven te melden.

Zorgplicht uitwerken in overleg met het bedrijfsleven

Naast een meldplicht voor incidenten met aanzienlijke gevolgen, bevat het wetsvoorstel ook de verplichting voor aanbieders van essentiële diensten en digitale dienstverleners om passende maatregelen te nemen om de risico's voor de beveiliging te beheersen en de gevolgen van incidenten te voorkomen en te minimaliseren (de zorgplicht).
Vanuit het perspectief van rechtszekerheid is het in veel gevallen wenselijk dat deze algemene bepalingen en normen worden uitgewerkt in sectorale AMvB's en/of richtsnoeren. Aansluiting bij in de sector gangbare, veelal internationale normen en/of werkwijze is noodzakelijk. Tevens moet worden geborgd dat de AMvB's voldoende flexibiliteit bieden en toekomstbestendig zijn. Bedrijven moeten daarom de mogelijkheid hebben om op basis van het 'pas toe of leg uit'-principe af te wijken van voorschriften die de uitwerking van de zorgplicht betreffen. Zo ontstaat voldoende ruimte voor een innovatieve of vernieuwende invulling gericht op het verder versterken van de digitale veiligheid.

Om te zorgen dat deze sectorale AMvB's goed aansluiten bij de praktijk verzoeken wij dat deze AMvB's zo veel mogelijk in nauw overleg met de betreffende sectoren worden opgesteld en dat ze – zodra ze gereed zijn – in publieke consultatie worden gebracht.

NCSC geen toezichthoudende rol

VNO-NCW en MKB-Nederland ondersteunen de gemaakte implementatiekeuze om het NCSC niet te belasten met toezicht en handhaving. De positie van het NCSC als centrum van kennis en expertise op het gebied van cybersecurity blijft hiermee overeind en de vaak intensieve samenwerking tussen overheid en bedrijven uit de vitale infrastructuur wordt door deze keuze niet gefrustreerd. Wij achten het van belang, dat bij de melding van inbreuken die aanzienlijke gevolgen kunnen hebben voor de continuïteit van de dienstverlening (de 'bijna-ongelukken'), hulp en bijstand van het NCSC voorop blijven staan.

Definities digitale dienstverleners verhelderen
Kenbare en duidelijke definitie van digitale dienstverleners en de subcategorieën (i) online marktplaats, (ii) onlinezoekmachine, (iii) cloudcomputerdiensten zijn nodig voor een succesvolle implementatie. Het moet voor bedrijven vooraf duidelijk zijn of ze onder de reikwijdte van deze wet vallen of niet. Niet in de laatste plaats omdat deze bedrijven ook door de toezichthouder kunnen worden aangesproken en tegen boetes kunnen aanlopen. Naar onze opvatting moet in het voorontwerp vooral een nauwe definitie van digitale dienstverlener worden gehanteerd. Het bedrijfsleven zal steeds nieuwe initiatieven en innovatieve digitale diensten ontwikkelen die niet altijd makkelijk te vangen zijn in één definitie. Het moet niet zo zijn dat een te ruime definitie er debet aan kan zijn dat dergelijke innovatieve initiatieven onbedoeld belemmerd zouden worden. In de memorie van toelichting zou de definitie daarom zo veel mogelijk moeten worden verduidelijkt door voorbeelden op te nemen wat wél en vooral ook wat niet onder de reikwijdte van het voorontwerp valt. Wij verzoeken dat het voorontwerp op dit punt wordt verhelderd.

Nederlands beveiligingsniveau als dé Europese benchmark
Met betrekking tot de digitale dienstverleners merken VNO-NCW en MKB-Nederland op dat deze bedrijven zich aantoonbaar zeer bewust zijn van het directe belang van een goede beveiliging van hun netwerken. Inbreuken op de beveiliging van hun netwerk- en informatiesystemen raken immers direct aan hun verdienmodel. Het beveiligingsniveau in Nederland is internationaal gezien zeer goed te noemen.
Aangezien de NIB-richtlijn ten aanzien van deze bedrijven uitgaat van Europese maximumharmonisatie dringen VNO-NCW en MKB-Nederland erop aan om het in Nederland gebruikelijke beveiligingsniveau bij de digitale dienstverleners tot inzet te maken van de onderhandelingen in Europa over de zgn. implementing acts.
Daarmee kan de positie van het Nederlandse bedrijfsleven worden versterkt en wordt bewerkstelligd dat de normen voor digitale veiligheid in de EU als geheel naar een hoger niveau kunnen worden getild.

Light touch approach
VNO-NCW en MKB-Nederland vinden het van belang dat de in de richtlijn opgenomen light touch approach (waar onder maximum harmonisatie, ex post toezicht) ten aanzien van digitale dienstverleners terugkomt in het wetsvoorstel.
Met betrekking tot de zorgplicht merken VNO-NCW en MKB-Nederland op dat deze voor digitale dienstverleners significant lichter moet worden dan voor de essentiële diensten. Dit kan bijvoorbeeld door alleen te verplichten tot het beschrijven van

scenario's van grote veranderingen in kritische systemen en de toezichthouder hierop ex post te laten controleren.
Uitdrukkelijk is in overweging 49 van de richtlijn opgenomen dat digitale dienstverleners de vrijheid behouden om maatregelen te nemen die zij passend achten ter beheersing van de risico's voor de beveiliging van hun netwerk- en informatiesystemen. Dit betekent dat flexibiliteit voor deze bedrijven behouden moet blijven en voorkomen moet worden dat de implementing acts een rigide keurslijf vormen.

Vrijwillige meldingen in behandeling nemen
In artikel 15, tweede lid wordt gesteld dat een vrijwillige melding van een incident met aanzienlijke gevolgen niet door de desbetreffende instantie in behandeling wordt genomen op het moment dat het die instantie onevenredig of overmatig zou belasten. Deze bepaling nodigt in onze optiek niet uit tot het doen van een vrijwillige melding, terwijl deze juist wel bijdragen aan het realiseren van de gewenste *just culture*.

Aansprakelijkheid
In de richtlijn is opgenomen dat melding van een beveiligingsincident niet leidt tot verhoogde aansprakelijkheid (artikel 14 lid 3 en artikel 16 lid 3). VNO-NCW en MKB-Nederland gaan ervan uit dat dit uitgangspunt wordt overgenomen.

Hoogachtend,

directeur Economische Zaken