Ministerie van Veiligheid en Justitie
De heer S.A. Blok
Postbus 20301
2500 EH DEN HAAG

Woerden, 14 juli 2017

Betreft : Reactie Nederland ICT op het 'concept-wetsvoorstel implementatie EU-richtlijn netwerk- en informatiebeveiliging (Cybersecuritywet)'
Kenmerk : LdB/AdJ/JB/MiZ

Geachte heer Blok,

Met aandacht heeft Nederland ICT kennis genomen van het concept-voorstel voor de cybersecuritywet. In dit voorstel implementeert u de Europese richtlijn voor netwerk- en informatiebeveiliging (NIB-richtlijn). Tevens heeft u bepalingen uit het wetsvoorstel gegevensverwerking en meldplicht cybersecurity (WGMC) beleidsneutraal in het wetsvoorstel opgenomen.

Nederland ICT is dé brancheverenigingvoor bedrijven in de ICT-sector, waaronder de bedrijven die behoren tot de categorie vitaal in de telecommunicatiesector en ICT-dienstverleners die onder de categorie Digitale Service Providers van het concept-voorstel vallen.

De digitale infrastructuur is hét fundament van onze digitale economie. Nederland heeft een uitmuntende, open, betrouwbare, veilige internet- en telecominfrastructuur die tot de absolute wereldtop behoort. De digitale infrastructuur van Nederland vervult als digitale mainport tevens een cruciale rol in wereldwijde datastromen, digitale verdienmodellen en innovatieve diensten en producten die oplossingen bieden voor tal van (toekomstige) maatschappelijke uitdagingen.

Pompmolenlaan 7
3447 GK Woerden

T 0348 49 36 36
info@nederlandict.nl
www.nederlandict.nl

NL 53 ING B 0662590546
KvK 30174840

NEDERLAND ICT

Gezien de vitale rol die de digitale infrastructuur speelt in de Nederlandse economie, zetten bedrijven zich maximaal in om de veiligheid en continuïteit van deze infrastructuur te waarborgen. De NIB-richtlijn richt zich op de niet vitale delen van de digitale infrastructuur. Nederland ICT geeft dan ook graag haar zienswijze op de ter consultatie voorgelegde stukken.

In Nederland zijn er ongeveer 37 meldplichten. Meldplichten verschillen in gevraagde informatie, tijdslijn waarbinnen deze informatie moet worden aangeleverd en sancties indien deze tijdslijn niet gehaald wordt. Voor bedrijven die onder verschillende regimes vallen, brengt dit een zeer forse administratieve last met zich mee. Het kan voorkomen dat een bedrijf meer tijd besteedt aan het doen van meldingen dan aan het afhandelen van het incident. In het onderliggende voorstel is het voornemen opgenomen om een dubbele meldplicht in te voeren. Nederland ICT acht dit een onwenselijke situatie. **Nederland ICT dringt er op aan om te onderzoeken of het Digital Trust Center op termijn kan worden gebruikt als CSIRT om zo maar een enkele melding te hoeven doen. Het DTC zou niet belast moeten worden met toezicht en handhaving.**

De te melden incidenten zullen vaak ook aan de Autoriteit Persoonsgegevens gemeld moeten worden. **Nederland ICT dringt er op aan om 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.**

Een ander zeer belangrijk punt is de vertrouwelijkheid van meldingen en gegevens. Gezien de gevoeligheid en vertrouwelijke aard van deze gegevens, moeten ze niet via een WOB-verzoek openbaar gemaakt kunnen worden. In artikel 19 is de omgang met gegevens door het NCSC geregeld. Een regeling met betrekking tot de bevoegde autoriteit ontbreekt echter, waardoor de verplichte melding bij de bevoegde autoriteit wel via een WOB-verzoek opvraagbaar is. Ingevolge artikel 23 kan de bevoegde autoriteit een beveiligingsaudit opleggen aan de aanbieder. Het auditrapport moet worden aangeboden aan de bevoegde autoriteit en kan via een WOB-verzoek opgevraagd worden. Dit kan grote consequenties hebben voor de beveiliging van deze bedrijven, daar er inzicht wordt gegeven in interne processen, architectuur en gebruikte infrastructuur. Nederland ICT dringt er op aan om de bijzondere openbaarheids-regeling van artikel 19 te verruimen naar alle bevoegde autoriteiten en van overeenkomstige toepassing te verklaren op artikel 23.

Naast een meldplicht voor incidenten met aanzienlijke gevolgen, bevat het wetsvoorstel ook de verplichting voor aanbieders van essentiële diensten en digitale dienstverleners, passende maatregelen te nemen om de risico's voor de beveiliging te beheersen en de gevolgen van incidenten te voorkomen en te minimaliseren. Nederland ICT wijst erop dat het nemen van deze passende maatregelen inherent aan het aanbieden van deze diensten is. Inbreuken op de veiligheid hebben vaak direct invloed op het verdienmodel.

Afsluitend, een duidelijke definitie van digitale dienstverleners is niet voorhanden, vooral voor de zgn. 'cloud providers' is dat problematisch omdat zich hierbinnen een vrij grote groep van origine Nederlandse aanbieders concentreert. In Denemarken worden bedrijven per brief op de hoogte gesteld dat ze zijn aangemerkt. **Nederland ICT dringt er op aan duidelijkheid te scheppen over welke bedrijven onder deze wet gaan vallen, voordat handhaving gaat plaatsvinden.**

Uiteraard is Nederland ICT graag bereid een mondelinge toelichting te geven op haar zienswijze.

Met vriendelijke groet,
Nederland ICT

Directeur