# INTERNETCONSULTATIE
# CONCEPT-BESLUIT MELDPLICHT CYBERSECURITY

Status per 20170515

| | | |
|---|---|---|
| 1. | **INLEIDING / HISTORIE** | Datalekken en Cybersecurity incidenten komen sinds een aantal jaren steeds vaker en heftiger voor. In de media wordt regelmatig bericht over beveiligingsincidenten en over nieuwe voorstellen ter aanscherping van de regelgeving met betrekking tot de bescherming van digitale informatie. Zo werd afgelopen vrijdagavond 12 mei 2017, de wereld opgeschrikt toen duizenden organisaties in tientallen landen het doelwit waren van een van de grootste cyberaanvallen ooit. Dit heeft wederom geleid tot de discussie over de noodzaak voor en de mogelijkheid van effectieve, technisch onafhankelijke reguleringsinstrumenten die de integriteit van informatiesystemen waarborgen.<br><br>Het wetsvoorstel Gegevensverwerking en Meldplicht Cybersecurity *('Wgmc')*, dat nu bij de eerste kamer ligt en de Europese 'NIB-Richtlijn' sluiten hierbij aan en roepen verschillende beveiligingseisen voor een informatiemaatschappij in het leven en een meldplicht voor ernstige ICT-incidenten.<br><br>'Het Besluit meldplicht cybersecurity' *('Bmc')* waar het in deze consultatie over zal gaan, wijst de aanbieders en producten en diensten aan waarvoor die meldplicht gaat gelden. Meldingen worden behandeld door het Nationaal Cyber Security Centrum *('NCSC')*. |
| 2. | **MELDPLICHT** | Het Wetsvoorstel introduceert een meldplicht bij het *NCSC*. De meldplicht geldt als er sprake is van een (mogelijke) inbreuk op veiligheid en daadwerkelijk verlies van integriteit van een elektronisch informatiesysteem. Hierbij gaat het om alle soorten data inclusief persoonsgegevens. De verplichting tot melden bestaat alleen indien de inbreuk gevolgen heeft of kan hebben op de beschikbaarheid of betrouwbaarheid een dienst of product en dit tevens in belangrijke mate kan leiden tot maatschappelijk ontwrichting.<br><br>De meldplicht heeft alleen betrekking op aanbieders van vitale producten of diensten. |
| 3. | **DOEL MELDPLICHT** | Het NCSC heeft als rol het waarborgen en zorgen voor een hoog kennisniveau van netwerk- en informatiebeveiliging. De meldplicht zorgt voor de benodigde informatie waarmee de NCSC (i) een tijdige inschatting kan maken van de impact van een mogelijke ICT inbreuk en of er sprake is van maatschappelijke ontwrichting, en (ii) hulp kan bieden aan de getroffen organisatie en anticiperen op mogelijk bredere effecten van een dergelijke inbreuk. Deze hulp kan bestaan uit (a) advies en informatie en (b) technische ondersteuning.<br><br>De doelstelling van het Wetsvoorstel is maatschappelijke ontwrichting door ICT-inbreuken te beperken of te voorkomen. |

| | | |
|---|---|---|
| 4. | **CONCEPT-BESLUIT MELDPLICHT** | De meldplicht geldt alleen voor aanbieders van producten of diensten waarvan de beschikbaarheid of betrouwbaarheid van vitaal belang is voor de Nederlandse samenleving. Het Bmc wijst de vitale aanbieders en producten en diensten aan ten aanzien waarvan de verplichting geldt, zoals opgenomen in artikel 6 van de Wgmc.<br><br>De beoordeling of een proces vitaal is, wordt gemaakt wanneer maatschappelijke ontwikkelingen daar aanleiding toe geven. In dit besluit zijn specifieke producten en diensten aangewezen waarvan beschikbaarheid en betrouwbaarheid van essentieel belang zijn om maatschappelijke ontwrichting te voorkomen. Hierbij is ook (i) de mate van afhankelijkheid van informatiesystemen in overweging genomen, (ii) de impact of sociaaleconomische gevolgen bij een aanzienlijke verstoring van de beschikbaarheid, (iii) de betrouwbaarheid van dat product of dienst en (iv) de duur van het incident en het aantal personen dat hierdoor wordt geraakt.<br><br>De volgende sectoren zijn aangewezen door het Bmc:<br><br>Drinkwater, Energie, Financiën, Mainport Rotterdam, Mainport Schiphol, Nucleair, Elektronische communicatienetwerken of – diensten / ICT, Digitale Overheid<br><br>Ondanks dat dit een goed begin is, is deze lijst niet toereikend. Zo zijn de (i) Elektronische communicatienetwerken of – diensten / ICT niet toereikend en (ii) ontbreekt de gezondheidszorg in zijn geheel.<br><br>(i) **Algehele digitale infrastructuur:** de reikwijdte van de door het besluit aangewezen Elektronische communicatienetwerken of – diensten / ICT is te beperkt om adequate beveiliging van kritieke infrastructuur te ondersteunen. De algehele digitale infrastructuur zou dan ook onder de meldplicht moeten vallen en niet alleen de aanbieders van elektronische communicatienetwerken ten behoeve van telefoons-, sms-, of internettoegangsdienst aan minimaal 1.000.000 eindgebruikers en de internetknooppunten als bedoeld in artikel 4, onder 13, van Richtlijn (EU) 2016/1148.<br><br>Immers de mate van afhankelijkheid van deze informatiesystemen in de samenleving is groot. Dit is des te meer van belang, nu de digitale infrastructuur in zijn geheel met elkaar verbonden is en er meerdere manieren zijn om hier middels een cyberaanval binnen te komen. Daarnaast is er is vandaag de dag geen organisatie of gebruiker - waaronder ook de vitale aanbieders als genoemd in Bmc - meer te bedenken die niet in grote mate afhankelijk is van verschillende informatiesystemen die nu buiten de meldplicht vallen. Bij een incident zal de impact en daarmee de sociaaleconomische gevolgen enorm zijn. Zo hebben we afgelopen vrijdag mogen ervaren, dat de algehele (bedrijf)processen geheel kunnen worden platgelegd. Niet alleen de vitale aanbieders zijn in grote mate afhankelijk van deze systemen, ook andere aanbieders met grote maatschappelijk impact kunnen hierdoor worden geraakt. |

| | | |
|---|---|---|
| | | (ii) **Gezondheidszorg:** ook de gezondheidszorg heeft geen plek gekregen in het besluit. Dit terwijl zorginstellingen volledig afhankelijk zijn van digitale systemen, die overigens in veel gevallen ook nog eens sterk verouderd zijn zit vanwege praktische, technische, organisatorische c.q. budgettaire redenen). Dit is afgelopen vrijdag maar weer benadrukt tijdens de grootste ransomware cyberaanval tot nu toe, waar Europol burgers heeft afgeraden ziekenhuizen te bezoeken indien het niet hoogst noodzakelijk is, waarbij het duidelijk is dat deze ransomware slecht een vingeroefening is en de gezondheidszorg in het bijzonder en de maatschappij in het algemeen erger kan verwachten. Daar komt bij dat de gezondheidszorg veelal op oude, kostbare systemen draait, die niet altijd geüpdatet is met de nodige securitypatches. Dit kan mensenlevens kosten en vertrouwen extreem schaden. De mate van afhankelijkheid van informatiesystemen in de gezondheidzorg is dan ook groot, de impact of sociaaleconomische gevolgen zijn aanzienlijke en de integriteit van de gezondheidszorg is dan ook van levensbelang. |
| **5.** | **CONCLUSIE** | Cybersecurity is een dynamisch en complex samenspel van dimensies, overlappende spanningsvelden en conflicterende rechten en plichten waar alles met elkaar verbonden is. Vitale aanbieders dienen dan ook in hoge mate te worden beschermd. Wgcm probeert hierin te voorzien, maar is nog niet toereikend om adequate bescherming te bieden. Er dient kritisch te worden gekeken naar de algehele digitale infrastructuur, nu alles met elkaar verbonden is en de vitale aanbieders hier eveneens afhankelijk van zijn. Daarnaast valt niet in te zien waarom de gezondheidszorg niet is meegenomen als vitale aanbieder, nu de gezondheidzorg in sterke mate afhankelijk is van informatiesystemen, die systemen veelal op relatief verouderd legacy niveau zit (meestal op praktische, technische organisatorische c.q. budgettaire redenen), en de samenleving op haar beurt hier sterk afhankelijk van is. |