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

BCPA

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

BCPA

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.

BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

Post Bits of Freedom
Postbus 10746
1001 ES Amsterdam

Bank 55 47 06 512
KvK 34 12 12 86

M
E
W https://www.bof.nl

Ivo Opstelten
Minister van Veiligheid en Justitie
Postbus 20301
2500 EH DEN HAAG

Betreft
Reactie op consultatie Wetsvoorstel melding inbreuken elektronische informatiesystemen

Amsterdam
17 september 2013

Geachte Minister Opstelten,

1. Graag reageert stichting Bits of Freedom op het wetsvoorstel voor een meldplicht voor inbreuken op elektronische informatiesystemen.

2. Bits of Freedom is zeer verheugd dat het ministerie dit wetsvoorstel heeft gepubliceerd. We onderschrijven het doel dat de wet probeert te bereiken, namelijk het vergroten van de cyber security bij organisaties in de vitale sectoren. De vele inbreuken in de afgelopen jaren onderstrepen de noodzaak van deze meldplicht.

3. Toch zijn er de nodige verbeteringen in het wetsvoorstel noodzakelijk. Het doel van de meldplicht wordt onvoldoende gerealiseerd. Dat komt omdat de wetgeving onvoldoende effectief is en de reikwijdte te beperkt. Daarnaast geeft het parlement de regie om kaders vast te stellen teveel uit handen. Tot slot is er onvoldoende transparantie over de uitvoering en opvolging van de meldplicht.

4. Hieronder lichten wij bovenstaande opmerkingen nader toe.

De regeling is onvoldoende effectief

5. Het is de bedoeling van het wetsvoorstel om maatschappelijke ontwrichting te voorkomen en een veiligheidscultuur te creëren. Een meldplicht is dan een goed middel om snel helderheid te krijgen over mogelijke maatschappelijke risico's. Ook kan er dankzij de meldplicht adequate hulp geboden worden om verdere maatschappelijke verstoring tegen te gaan.

6. Om de meldplicht bij te laten dragen aan de vergroting van cyber security in vitale sectoren is het noodzakelijk dat aan de meldplicht wordt voldaan. Het wetsvoorstel dient daarom te waarborgen dat deze meldplicht wordt nageleefd. Deze waarborgen ontbreken in dit wetsvoorstel.

7. Er staat geen boete op het niet nakomen van de meldplicht. Bovendien is er geen instantie aangewezen die kan controleren of er aan de meldplicht wordt voldaan. Er wordt uitgegaan van de goede wil van organisaties die onder het bereik van de wet vallen om de meldplicht na te leven. Zo is deze meldplicht in de praktijk een meldverzoek. Dat is onwenselijk.

> Onderzoek wijst uit dat bedrijven die hun processen goed op orde hebben wel zullen rapporteren en de bedrijven die hun beveiliging niet goed op orde hebben niet melden.[1] Daarmee wordt in de praktijk vervolgens alleen aan de meldplicht voldaan door de 'good guys', terwijl het de bedoeling is dat ook de 'bad guys', die het met de beveiliging van hun systemen niet zo nauw nemen, de meldplicht nakomen.

8. Daarom moet er een mogelijkheid bestaan om te controleren of er aan de plicht wordt voldaan en het nakomen van deze plicht desnoods af te dwingen.

9. Ten eerste moet er een sanctie op het niet-melden worden geïntroduceerd. De Memorie van Toelichting (MvT) stelt ten onrechte dat een sanctie de drempel om meldingen te doen kan verhogen.[2] De prikkel van een sanctie draagt bij aan het (versneld) realiseren van de 'just culture' binnen de vitale sectoren.

10. Ten tweede moet een toezichthoudende organisatie worden aangewezen die de naleving van de meldplicht controleert. Het NCSC is vanwege de noodzakelijke specifieke kennis hiervoor de meest geschikte organisatie. Het is de vraag hoe het NCSC achter het bestaan van een inbreuk moet komen, als zij niet over een effectief middel beschikken om te controleren of aan de meldplicht is voldaan. Daarbij vraagt Bits of Freedom zich af of het NCSC momenteel over de capaciteit beschikt om deze taak op zich te nemen, ook wanneer er geen sprake is van een controleverplichting door het NCSC.

> Het NCSC heeft in het verleden laten zien grote capaciteitsproblemen te hebben, zoals gebleken is bij de aanpak van het Pobelkabotnet.[3]

11. Het is eveneens onduidelijk in welke gevallen het NCSC hulp zal bieden in plaats van alleen de melding in ontvangst te nemen. De taakstelling en opvolging van een melding door het NCSC is daarmee onvoldoende gepreciseerd.

---

1 Jane Winn, Are 'Better' Security Breach Notification Laws Possible? *Berkeley Technology Law Journal Vol 24 2009*
2 MvT p 2
3 Kamerstukken II 2012/13, 26 643, nr. 272, p. 2

12. De suggestie dat het NCSC eventueel een sectorale toezichthouder in kan schakelen,[4] is onvoldoende waarborg voor naleving van de meldplicht. Zo zal het eventuele aangescherpte toezicht te laat plaatsvinden.

> Bits of Freedom adviseert om een sanctie op te nemen voor het niet nakomen van de meldplicht. Daarnaast moet het NCSC worden aangewezen als toezichthouder op het naleven van de meldplicht. Ook moet de taakstelling van het NCSC nader gespecificeerd worden en dient het NCSC de capaciteit te krijgen die nodig is om deze meldplicht effectief te ondersteunen.

De reikwijdte van de meldplicht is te beperkt

13. Ook de meldplicht zelf moet worden uitgebreid. Alleen daadwerkelijke inbreuken op de veiligheid en de integriteit van een systeem moeten onder dit voorstel worden gemeld.[5] DDoS-aanvallen vallen hier volgens de Memorie van Toelichting niet onder. Bits of Freedom acht dit onjuist.

14. Het wetsvoorstel geeft geen eenduidige definitie van beveiliging. Een veelgebruikte definitie van informatiebeveiliging richt zich op de beschikbaarheid, vertrouwelijkheid en integriteit van deze systemen. Er is dus ook sprake van een inbreuk op de beveiliging bij een verlies van de beschikbaarheid van een dienst.

15. Het is dan ook niet gek dat een DDoS-aanval onder de wetsbepaling valt, ook al wordt die vervolgens in de toelichting hiervan uitgesloten. Wanneer er sprake is van een DDoS-aanval die een systeem plat legt, is er immers sprake van een daadwerkelijke inbreuk. De dienst die via het systeem wordt geleverd, is dan namelijk niet bereikbaar. Daarmee wordt eveneens voldaan aan de twee cumulatieve voorwaarden die de toelichting stelt, namelijk een daadwerkelijke inbreuk op de veiligheid, die vervolgens de beschikbaarheid van de dienst kan onderbreken.

16. Er zijn zwaarwegende redenen om DDoS-aanvallen onder de meldplicht te laten vallen. Een DDoS-aanval kan namelijk een 'stepping stone' zijn voor andere aanvallen of als afleidingsmanoeuvre dienen. Om deze redenen is een snelle melding van een DDoS-aanval juist cruciaal voor het beschermen van de continuïteit en beschikbaarheid van vitale infrastructuren.

17. De regel zou dus moeten zijn: een DDoS-aanval wordt gemeld als er sprake is van een "belangrijke mate van maatschappelijke ontwrichting". Het niet hoeven melden van een DDoS-aanval zou een uitzondering moeten zijn, die

4 MvT p 5
5 MvT p 3

intern deugdelijk gemotiveerd moet worden. Deze deugdelijke motivering moet later gecontroleerd kunnen worden door het NCSC.

> Bits of Freedom adviseert om de melding van DDoS-aanvallen op te nemen in de meldplicht.

De wetgever geeft de regie uit handen

18. Belangrijke aspecten van deze wet zullen bij Algemene Maatregel van Bestuur (AMvB) geregeld worden. Voor de invulling hiervan zal overleg met de organisaties in de vitale sectoren plaatsvinden. Onder de nader in te vullen aspecten valt in ieder geval welke organisaties aan de meldplicht moeten voldoen, een specifieke regeling voor in welke gevallen gemeld moet worden en wat er precies gemeld moet worden.

> Een goed voorbeeld hiervan is de verstoring van de beschikbaarheid of betrouwbaarheid van een dienst. De verstoring hiervan moet in "belangrijke mate" zijn. Wat "een verstoring in belangrijke mate" van een dienst is, moet nog blijken uit overleg met organisaties uit de vitale sectoren.

19. Het parlement dient het beleid vast te stellen en te controleren. Door de invulling van deze voorwaarden grotendeels aan overleg met de sector over te laten, geeft het parlement de regie uit handen. Daarnaast gaat het parlement akkoord met de mogelijkheid dat de uitwerking in lagere regelgeving anders uitpakt dan met deze wet wordt beoogd.

20. Dit acht Bits of Freedom onwenselijk. Een duidelijkere omschrijving van de voorwaarden waaronder de meldplicht van toepassing is, zou dit probleem oplossen zonder dat dit ten koste gaat van de flexibiliteit van de wet.

> Bits of Freedom adviseert om de voorwaarden waaronder de meldplicht moet worden nageleefd duidelijker te definiëren, evenals op welke organisaties de meldplicht van toepassing is.

Transparantie leidt tot grotere cyber security

21. Een melding hoeft volgens de Memorie van Toelichting in beginsel niet met het publiek gedeeld te worden gemaakt als er geen schadelijke gevolgen zijn. Er wordt gesteld dat het belang van de organisatie zwaarder kan wegen dan openbaar maken. Ook wordt gesteld dat de maatschappelijke onrust groter kan worden door openbaarmaking van de melding.[6] Bits of Freedom is van mening dat transparantie juist wenselijker is.

22. Transparantie zorgt voor vertrouwen in de organisatie en leidt tot

6 MvT p 8

bewustwording bij organisaties. Het imago van een organisatie wordt meer beschadigd door geheimzinnigheid dan door openheid. Maar zelfs als dit imago wel beschadigd zou worden, dan nog dient het imago van organisaties ondergeschikt te zijn aan cyber security en niet andersom.

23. Openbaarheid komt het onderzoek naar cyber dreigingen ten goede. Dit kan de cyber security vergroten. Ook kan openbaarheid de bewustwording bij andere organisaties en bij de consument vergroten.

24. Proactieve transparantie over het aantal meldingen, de inhoud en opvolging daarvan en in welke sectoren deze inbreuken plaatsvinden, is daarom vitaal voor het bereiken van de doelstelling van het wetsvoorstel. Dat geldt niet alleen voor inbreuken waarin daadwerkelijk (maatschappelijke) schade geleden is, maar voor alle gedane (of niet gedane) meldingen over inbreuken.

> Bits of Freedom adviseert gegevens over het aantal inbreuken per sector, de aard en de impact daarvan, en de opvolging naar aanleiding van deze meldingen periodiek - bijvoorbeeld per kwartaal - openbaar te maken.
>
> Bits of Freedom wil benadrukken dat deze gegevens geopenbaard kunnen worden zonder dat deze herleidbaar zijn tot een specifieke organisatie.

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd. Uiteraard ben ik graag bereid om het bovenstaande nader toe te lichten, mocht daaraan behoefte bestaan.

Hoogachtend,

Ton Siedsma

De Nederlandsche Bank
Eurosysteem

AFM
Autoriteit Financiële Markten

Ministerie van Veiligheid en Justitie
T.a.v. de minister van Veiligheid en Justitie
Postbus 20301
2500 EH DEN HAAG

Datum	17 september 2013
Ons kenmerk	SBI-SHMe-13090533
Pagina	1 van 4
Betreft	gezamenlijke consultatiereactie AFM en DNB op wetsvoorstel melding inbreuken elektronische informatiesystemen

Geachte heer Opstelten,

Op 22 juli jl. heeft u het wetsvoorstel melding inbreuken elektronische informatiesystemen ter openbare internetconsultatie aangeboden. Graag maken De Nederlandsche Bank en de Autoriteit Financiële Markten van deze gelegenheid gebruik om het volgende onder uw aandacht te brengen.

Het consultatievoorstel voorziet in een meldplicht aan de minister van Veiligheid en Justitie in geval van een inbreuk op de veiligheid of een verlies van integriteit van een informatiesysteem waardoor de beschikbaarheid of betrouwbaarheid van een product of dienst in belangrijke mate wordt of kan worden onderbroken. Het voorstel raakt alle sectoren met producten of diensten die van een zodanig belang zijn voor de Nederlandse samenleving dat onderbreking van de beschikbaarheid of betrouwbaarheid daarvan kan leiden tot ernstige maatschappelijke gevolgen, zoals de energiesector, telecommunicatiesector, luchtvaartsector en de financiële sector. Volledigheidshalve vermelden wij dat onze opmerkingen uitsluitend betrekking hebben op de financiële sector.

DNB en AFM constateren dat de regelgeving voortvarend is ontworpen en ter consultatie is voorgelegd. Gezien het brede cross-sectorale bereik van de regels is het naar ons oordeel ook logisch dat is gekozen voor een kaderwet op hoofdlijnen, waarbij ruimte wordt gelaten voor een verdere uitwerking per sector. Niettemin menen DNB en AFM dat het consultatievoorstel specifieker zou moeten ingaan op een aantal zaken, met name op de taak- en rolverdeling tussen het Nationaal Cyber Security Centrum (NCSC) en de sectorale toezichthouder(s).

Wettelijke verankering taak- en rolverdeling
Het consultatievoorstel voorziet niet in een wettelijke verankering van de taak- en rolverdeling tussen het NCSC enerzijds en de sectorale toezichthouder(s) anderzijds. Het consultatievoorstel roept hierbij bovendien een gemengd beeld op. Enerzijds valt te lezen dat de hulp door het NCSC onder meer behelst het coördineren van de inzet van andere (overheids)organisaties (concept MvT, p. 1), anderzijds wordt vermeld dat de voorgestelde meldplicht bestaande crisisbeheersingsstructuren onverlet laat (id. p. 4).

Zoals uit de brief van de minister van Veiligheid en Justitie van 6 juli 2012 blijkt, welke brief in de geconsulteerde memorie van toelichting wordt genoemd, bestaat er ten aanzien van ondernemingen uit de sector financiën reeds een meldplicht, alsmede een handhavingsinstrumentarium voor de betreffende sectorale toezichthouder.

De Nederlandsche Bank
Westeinde 1
Postbus 98
1000 AB Amsterdam

Autoriteit Financiële Markten
Vijzelgracht 50
Postbus 11723
1001 GS Amsterdam

Voorts is van belang dat DNB en AFM samen met medewerkers van het ministerie van Financiën het tripartiete crisisorgaan (TCO) vormen dat reeds opereert in situaties waarin het consultatievoorstel voorziet[1]. De afwezigheid van een duidelijke taak- en rolverdeling kan in de praktijk tot onwenselijke situaties leiden. Juist in een crisissituatie zal snel en efficiënt optreden veel schade kunnen voorkomen. Daarbij is van belang dat de betrokken belangen snel worden onderkend en tegen elkaar worden afgewogen. Met name is in dit verband van belang dat overleg plaatsvindt tussen NCSC en TCO over de informatie die NCSC ontvangt in het kader van de meldplicht en de aan het NCSC toegekende bevoegdheid informatie door te geven aan derden en/of openbaar te maken. In het TCO, waarin DNB, AFM en de minister van Financiën op bestuurlijk niveau zijn vertegenwoordigd, kunnen de verschillende belangen (financiële stelsel, betrokken financiële onderneming(en), maatschappelijke belangen) worden gewogen.

DNB en AFM adviseren u de taak- en rolverdeling tussen het NCSC en de sectorale toezichthouders zodanig wettelijk te verankeren dat zij de afweging blijven maken voor zover het sectorale gevallen betreft, met ondersteuning van het NCSC. Bij sector overstijgende problemen kan geëscaleerd worden naar het TCO en op ministerieel niveau.

Reikwijdte regeling
Het consultatievoorstel ziet op 'inbreuk op de veiligheid' en 'verlies van integriteit'. Onduidelijk is wat onder deze voor het wetsvoorstel essentiële begrippen moet worden verstaan. AFM en DNB verzoeken de begrippen veiligheid en verlies van integriteit van een elektronisch informatiesysteem te verduidelijken. De meldplicht in dit wetsvoorstel ziet alleen op een daadwerkelijke inbreuk op de veiligheid en op een daadwerkelijk verlies van integriteit van een elektronisch informatiesysteem en niet op ernstige verstoringen waarbij geen sprake is van een dergelijke ICT-inbreuk, zoals DDoS aanvallen. Recente aanvallen als deze in de financiële sector (en in andere sectoren) hebben ons inziens juist duidelijk gemaakt dat adequate melding en het delen van kennis en informatie door diegenen die dienen te handelen noodzakelijk is om de continuïteit van het betalings- en effectenverkeer optimaal te waarborgen. Wij adviseren derhalve om ook het melden van ernstige verstoringen zonder bedoelde inbreuk, maar met impact op de continuïteit van diensten en producten, onder de reikwijdte van de voorgestelde regeling te brengen, nadat wordt voorzien in geadviseerde regeling van samenwerking tussen het NCSC en sectorale toezichthouders.

Ontbreken van een sanctie
In de memorie van toelichting op het consultatievoorstel is benadrukt dat het NCSC geen sancties kan opleggen. Tegelijkertijd volgt uit het voorstel en de toelichting dat het melden aan het NCSC niet vrijwillig is. De vraag rijst hoe dit in de praktijk zal functioneren. Het is denkbaar dat – gezien de verschillende meldplichten, op grond van het consultatievoorstel en de Wet op het financieel toezicht (Wft) – een financiële onderneming in een crisissituatie vergeet om (ook) aan het NCSC te melden. AFM en DNB achten het niet hun taak de betreffende onderneming daarop te wijzen of het NCSC namens een financiële onderneming in een crisissituatie zelf te betrekken. Het is naar het oordeel van DNB en AFM raadzaam om in het voorstel en de toelichting vast te leggen

[1] Zie Memorandum of Understanding van DNB, AFM en het ministerie van Financiën, bijlage bij de brief van de minister van Financiën aan de Tweede Kamer d.d. 27 april 2011 (TK, 27 863, nr. 39).

dat niet van de sectorale toezichthouders wordt verwacht dat zij toe zouden zien op naleving van de meldplicht.

Naast de meldplicht noemt de wet de mogelijkheid dat het NCSC de aanbieder bijstaat bij het treffen van maatregelen (artikel 4, onderdeel b). Zoals hierboven is opgemerkt, adviseren DNB en AFM dat het NCSC geen aanbevelingen geeft aan aanbieders uit de sector financiën, dan nadat met de sectorale aanbieders is afgestemd. In aanvulling hierop merken DNB en AFM op dat uit artikel 4 van het consultatievoorstel geen verplichting lijkt voort te vloeien voor aanbieders om een door het NCSC gegeven advies op te volgen, maar dit zou in de memorie van toelichting bevestigd kunnen worden.

Vertrouwelijke gegevens
Uit artikel 6 van het consultatievoorstel lijkt te volgen dat informatie uit meldingen gebruikt kan worden voor het geven van informatie en advies aan andere aanbieders, een CERT, of het publiek. Aan het publiek kunnen geen gegevens worden verstrekt die herleid kunnen worden tot afzonderlijke aanbieders, producten of diensten, tenzij het maatschappelijk belang dat vergt (art. 6, lid 2). Met de verwijzing naar het maatschappelijk belang dreigt een cirkelredenering te ontstaan. Immers, het doel achter de meldplicht en het geven van advies is het voorkomen van maatschappelijke onrust. Het maatschappelijk belang lijkt hierbij per definitie aan de orde te zijn.

Verder menen AFM en DNB dat de beperking met betrekking tot de herleidbaarheid tot individuele aanbieders – die nu slechts van toepassing is op informatieverstrekking aan het publiek - ook van toepassing zou moeten zijn op de informatievertrekking naar andere aanbieders. Het zal hier immers gaan om informatie die concurrentiegevoelig van aard is.

AFM en DNB zijn zelf gebonden aan een strikte geheimhoudingsplicht, voor zover het gaat om vertrouwelijke toezichtinformatie (zie o.a. artikel 1:89 van de Wet op het financieel toezicht). Deze plicht komt voort uit Europese richtlijnen en is bedoeld om vrije informatieverstrekking door onder toezicht staande onderneming te bevorderen. Het zou de informatieverstrekking door aanbieders uit de sector financiën ten goede komen, indien het wetsvoorstel voor de minister van Veiligheid en Justitie een geheimhoudingsplicht zou introduceren, die vergelijkbaar is met de verplichting die rust op de betreffende sectorale toezichthouders.

Internationale impact
Het consultatievoorstel noch de memorie van toelichting gaan uitgebreid in op de internationale dimensie van de voorgestelde regels. Banken en handelsplatformen kennen een groot internationaal karakter en beperken hun activiteiten niet tot landsgrenzen. Het zal zo zijn dat in geval van incidenten ook internationale samenwerking en coördinatie wenselijk is. Het verdient aanbeveling om meer dan nu onder het voorgestelde artikel 6, in te gaan op de extraterritoriale werking van het voorstel.

Wij hopen u hiermee voldoende te hebben geïnformeerd en zijn graag bereid tot het geven van een nadere toelichting.

Hoogachtend,

Autoriteit Financiële Markten

Drs. H.W.O.L.M. Korte
Bestuurslid

De Nederlandsche Bank

Mr. F. Elderson
Directeur

Nederlandse
Vereniging van Banken

Ministerie van Veiligheid en Justitie
Postbus 20301
2500 EH DEN HAAG

Datum 16 september 2013
Referentie BR1986

Betreft: Reactie op wetsvoorstel melding inbreuken elektronische informatiesystemen

Geachte lezer,

Bij deze willen we u bedanken voor de mogelijkheid te reageren op dit wetsvoorstel.
Onderstaand treft u onze reactie.

Algemeen
Het wetsvoorstel beschrijft op hoofdlijnen de huidige werkwijze van de banken met het NCSC. Banken delen, op basis van reciprociteit informatie over incidenten met het NCSC. Op dit moment zien de NVB en de banken het NCSC als een ondersteunende partij. En die ondersteuning door het NCSC vereist input vanuit de sector(en). De kennisdeling op basis van die reciprociteit is de kracht van de huidige vorm van samenwerking.
De NVB en de banken zijn ook betrokken bij de ICT Response Board. Ook daar zullen banken – waar relevant en nodig – informatie delen.
De recente DDoS aanvallen zijn een goed voorbeeld hoe de samenwerking werkt. In het verslag van de Ministers van Financiën en van Veiligheid en Justitie staat daarover o.a.: "Naar aanleiding van de geconstateerde verstoringen is er terstond intensief contact gelegd tussen de banken en de betrokken instanties, onder meer met de ministeries van Veiligheid en Justitie, Financiën en De Nederlandsche Bank (DNB)."

Doelstelling/uitgangspunt wetsvoorstel
De NVB en de banken vinden dat het wetsvoorstel averechts zou kunnen gaan werken. In plaats van een werkwijze, die is gebaseerd op vertrouwen en op reciprociteit, wordt nu een wettelijk kader geschapen waarbinnen de informatie moet worden geleverd aan het NCSC.
Het NCSC krijgt in het wetsvoorstel een meer toezichthoudende rol. Het risico is dan reëel dat de verhoudingen tussen de sector(en) en het NCSC verandert. Mogelijk leidt dit tot een situatie die veel minder "voelt" dan een publiek-private partnership.
De banken nemen er verder kennis van dat DDoS aanvallen in het wetsvoorstel buiten scope blijven.

Concluderend stellen de NVB en de banken dan ook, dat dit wetsvoorstel de wederzijdse samenwerking, gebaseerd op reciprociteit, negatief beïnvloedt.

De NVB vindt dat een alternatief voor het wetsvoorstel bijvoorbeeld in de vorm van een "manifest van samenwerking" effectiever zal werken in de praktijk..

NVB en de banken vinden het wel reëel, dat er eisen worden gesteld aan het melden van security incidenten voor specifieke sectoren. Deze meldingen zullen dan – voor de sectoren waar dat mogelijk is – moeten worden gemeld aan de eigen toezichthouder. Voor de banken geldt al dat de WFT[1] eist dat een bank de toezichthouder informeert over incidenten die een ernstig gevaar vormen voor de integere uitoefening van het bedrijf in het kader van de eisen aan beheerste en integere bedrijfsvoering.

Vertrouwelijkheid van informatie
Voor de banken en de NVB is, de vertrouwelijkheid van gedeelde informatie een groot punt van zorg, zowel in het huidige wetsvoorstel, als ook al in de huidige situatie.
Voor de financiële sector geldt, dat vertrouwelijke mededelingen van banken aan DNB onder de geheimhoudingsplicht vallen van de WFT. Deze mededelingen van DNB aan de Minister vallen ook buiten de WOB (WFT, artikel 1.47 Lid 2).
De banken denken dat er de ruimte voor discussie is doordat art. 10 lid 1 sub c van de WOB spreekt over bedrijfs- en fabricagegegevens. Deze formulering is voor verschillende uitleg vatbaar en leidt op zijn minst tot procedures bij de rechter waar verweer tegen gevoerd moet worden. Dat is niet bevorderlijk voor een goed samenwerkingsklimaat tussen het NCSC, de NVB en de banken.
Incidentgegevens zullen niet altijd kwalificeren als bedrijfs- of fabricage gegevens. Gegevens met betrekking tot de wijze van aanvallen zullen er bij voorbeeld wellicht niet onder vallen. Ook is de vraag hoe de vertrouwelijkheid moet worden gewaarborgd als sprake is van een keten van meerdere partijen, waar de melder een schakel in vormt. Informatie over andere ketenonderdelen valt vermoedelijk evenmin onder een eventuele uitzondering voor de melder. De banken willen graag dat deze wetgeving expliciet duidelijk maakt welke vertrouwelijke informatie niet op basis van de WOB kan worden opgevraagd.

Een andere vraag in het kader van vertrouwelijkheid van gegevens is de vraag, wat er mag worden gedaan door het NCSC met de aangeleverde informatie.
Artikel 6 biedt verder ook nog het NCSC de mogelijkheid om de gegevens van de aanbieder nationaal en internationaal te gebruiken voor het geven van advies. Dit betekent dat andere partijen mogelijk de beschikking krijgen over zeer gevoelige en vertrouwelijke gegevens van de aanbieder. Dit is – zonder instemming – van de aanbieder niet wenselijk, met name vanuit de genoemde optiek van vertrouwelijkheid van informatie.

Dit is de kern van ons commentaar. Onderstaand volgt het verdere inhoudelijke commentaar op het wetsvoorstel.

[1] Wet Financieel Toezicht

Algemene opmerkingen bij het wetsvoorstel
Indien u dit wetsvoorstel wilt doorzetten, geven we onderstaande inhoudelijke reactie op het voorstel. Als u besluit de richting van een *Manifest van Samenwerking* in te slaan, dan dringen we er ook op aan rekening te houden met onderstaande aanbevelingen.

De meeste van de genoemde punten zouden ook aandachtspunten kunnen zijn die aandacht krijgen in de Algemene Maatregel van Bestuur (AMvB) per sector.

- *Onduidelijkheid wetsvoorstel*
  Het is van groot belang dat de onderliggende AMvB voor de financiële sector in goed overleg met de sector zal worden ingevuld. Het wetsvoorstel is op zich erg vaag.
  Wij adviseren in ieder geval een eigen AMvB voor de financiële sector. Het wetsvoorstel spreekt van 'een ICT-inbreuk die in belangrijke mate leidt of kan leiden tot een inbreuk op de veiligheid of een verlies van integriteit'. Belangrijke mate dient o.i. te worden gekoppeld aan de vitale functies van de banken: betalings- en effectenverkeer. Het is wenselijk zo concreet mogelijk te benoemen wanneer "in belangrijke mate" sprake is van een inbreuk op deze veiligheid en hoe moet worden omgegaan met de term "kan leiden". De invulling zal niet moeten leiden tot te veel meldingen die in tweede instantie blijken "mee te vallen".
- *Relatie met uitbreiding WBP betreffende data lekken*
  NVB en de Banken zien in feite twee wetten met een grote overlap, weliswaar met andere doelen. Er zijn behoorlijk wat inbreuken denkbaar op elektronische informatiesystemen die ook datalekken van persoonsgegevens tot gevolg hebben. Hoe waarborgen deze wetsvoorstellen dat sectoren niet met dubbele informatieverplichtingen komen te zitten?
- *Banken hebben al meldplicht over incidenten richting DNB;*
  Niet alleen banken, maar ook andere kritieke infrastructuren staat onder toezicht van door de overheid aangestelde toezichthouders. Hierbij hebben zij vaak al een meldplicht als het gaat om incidenten die aan bepaalde criteria voldoen. Dat is voldoende voor het uitoefenen van een zorgvuldig en betaalbaar toezicht. Uw opmerking over de beperkte toename van de administratieve lasten (zie ook bij de **inhoudelijke reactie** over administratieve lasten) is niet realistisch en in zijn algemeenheid veel te laag;
- *Beschikbaar stellen informatie*
  De NVB en de banken vinden het ongewenst dat een andere instantie dan de bank zelf (en in uitzonderlijke gevallen DNB) bepaalt of en zo ja welke gegevens beschikbaar worden gesteld aan derden en/of aan het publiek.
  Artikel 6 van het wetsvoorstel geeft de minister en feitelijk dus het NCSC de ruimte om naar eigen inzicht informatie aan andere bedrijven en zelfs het publiek door te geven. Aanbieders mogen niet terughoudend zijn met het leveren van inhoudelijke informatie. Banken en/of de NVB (afhankelijk van de situatie) dienen en zullen deze verantwoordelijkheid nemen.
  In de memorie van toelichting geeft de wetgever aan dat dit artikel de vertrouwelijkheid van informatie waarborgt. NVB en de banken dringen er op aan dat er minimaal een aanpassing dient te komen in de regelgeving over het openbaar maken van gegevens. Bijvoorbeeld zou de wet (of de AMvB) kunnen vastleggen dat als een instelling en het NCSC geen overeenstemming kunnen bereiken over publicatie van gegevens dit moet worden geëscaleerd naar de minister en de Raad van Bestuur van de betreffende instelling(en).
- *Onverwijld melden*
  Het wetsvoorstel spreekt over het "onverwijld" melden van incidenten. Dit zal niet altijd mogelijk zijn. Ten eerste is niet altijd direct bekend, dat een incident grootschalige gevolgen kan of gaat hebben. Ten tweede is op dat moment vaak slechts beperkt informatie beschikbaar. Tot slot (en daar is nu ervaring opgedaan bij de DDoS incidenten) betreft het vaak informatie uit een keten, beginnend bij de private sector die wordt getroffen, maar met links naar andere sectoren en naar de overheid. Het is niet altijd duidelijk waar informatie vandaan moet komen. En die informatie is ook niet altijd direct beschikbaar bij de aanbieder.
  Wij adviseren in de wet duidelijk onderscheid te maken tussen de termen onverwijld (is tijdig) melden en de volledigheid van de melding (gegeven de fase waarin de melding wordt gedaan)..

- *Welke informatie moet worden gedeeld?*
  In artikel 4 staat bij onverwijld melden ook, dat het NCSC onverwijld "alle overige gegevens die nodig zijn" kan opvragen. Dit is een vrijbrief om (bijna) alles op te vragen. Het is niet wenselijk dit toe te staan. NVB en banken gaan ervan uit dat overige op te vragen informatie ten hoogste wordt vastgesteld in onderling overleg;
- *Wie meldt?*
  Het wetsvoorstel gaat over het meldplicht door de aanbieder. Er dient een heldere scheidslijn te komen tussen aanbieder, afnemer en verantwoordelijkheden. Nu lijkt de verantwoordelijkheid te liggen bij de aanbieder, terwijl een andere partij in de keten nalatig kan zijn;
- *Verplicht hulp aan sectoren*
  Banken in Nederland beschikken over professionele IT en information security organisaties. Het is niet de rol van de overheid te bepalen waar en wanneer banken behoefte hebben aan hulp in geval banken met een incident worden geconfronteerd.
  De huidige samenwerking laat organisaties vrij om hulp te bieden of te vragen en dat is naar onze mening de enige manier waarop zo'n samenwerking succesvol kan zijn;
- *Rol NCSC*
  De rol van het NCSC ligt op de in het wetsvoorstel genoemde punten niet vast. Welke formele rol heeft het NCSC bij de ondersteuning van bedrijven? Wat is precies de rol van het NCSC in het maken van risico inschattingen?
- *Just culture*
  De banken ondersteunen – en zijn ook voortrekkers geweest – van een veiligheidscultuur waarin het leren van incidenten vooropstaat. Dit wordt in het wetsvoorstel "*just culture*" genoemd. Het hele wetsvoorstel is in feite strijdig met deze "just culture" gedachte.
- *Meldplichtige partijen*
  Hoe worden in deze wet partijen als Google, Paypal, Marktplaats, etc.. meegenomen? Vallen deze partijen ook onder deze wet?

Inhoudelijke reactie bij generieke deel Memorie van Toelichting

Memorie van Toelichting; punt 2. Algemeen

Wij onderschrijven de doelstelling hier genoemd, om de meldplicht zo licht als mogelijk te houden. Doelstelling van de samenwerking in het NCSC is primair kennisdeling en wederzijdse hulp.
De opmerking die daarbij wel dient te worden gemaakt, is dat de uitwisseling, zoals die nu plaats vindt, gebeurt onder het zogenoemde *"Traffic Light Protocol" (TLP).* De zender bepaalt daarbij de mate van vertrouwelijkheid van de informatie en bepaalt daarmee ook, in hoeverre de informatie buiten de sector kan en mag worden gedeeld. Uiteraard zal het TLP binnen redelijkheid moeten worden gebruikt. Dat is ook de huidige praktijk.

Memorie van Toelichting; punt 2. Meldplichtige partijen

Wij adviseren hierbij aan te sluiten op de producten en diensten die ook al vanuit de optiek vitaal worden meegenomen. Dit is ook het uitgangspunt bij het Alerteringssyteem Terrorismebestrijding. De NVB verwacht dat de "grenzen" van de huidige producten en diensten die vitaal zijn, opnieuw worden bekeken, ook voor het ATb. We gaan ervan uit, dat de genoemde aanwijzing in overleg met de sector zal plaatsvinden.

Memorie van Toelichting; punt 2. Vertrouwelijkheid

In deze paragraaf wordt gewezen op het belang van vertrouwelijkheid. Artikel 6 van de wetgeving gaat hierop in.
Daarmee geeft het wetsvoorstel aan, dat vertrouwelijkheid belangrijk is. De NVB en de banken zijn, zoals al eerder in deze reactie is aangegeven, bezorgd over de opvraagbaarheid van gedetailleerde, vertrouwelijke informatie. De NVB en de banken zien graag meer duidelijkheid over informatie die wel en die niet opvraagbaar is.

Memorie van Toelichting; punt 2. Sectorale meldplichten; verhouding tot wetsvoorstel meldplicht datalekken en verhouding tot EU-richtlijnen

In de memorie van Toelichting wordt aandacht besteed aan de administratieve lasten door verschillende Nederlandse wetgeving, als ook op Europese wetgeving rond data inbreuken en security inbreuken.
Op dit moment is e.e.a niet concreet te maken. We verwachten – en rekenen op – grote zorgvuldigheid ten aanzien van de administratieve lasten, maar ook ten opzichte van een Europees level playing field. Het is niet wenselijk dat in Nederland veel zwaardere eisen gelden, die leiden tot hogere lasten voor de Nederlandse financiële sector (en andere sectoren), vergeleken met het buitenland.
Memorie van Toelichting 4: Administratieve lasten
NVB en de banken ondersteunen het uitgangspunt van minimale extra administratieve lasten.
Wij herkennen ons niet in de gemaakte rekensom. Op het moment dat door het NCSC gevraagde informatie afwijkt van al eerder geleverde informatie, zullen – zeker bij serieuze inbreuken, waarbij veel informatie moet worden verzameld en gedeeld – de kosten per incident aanzienlijk zijn.
Wij adviseren deze informatie niet te concretiseren in deze regelgeving.

Per artikel. Memorie van Toelichting en wetsvoorstel
Artikel 1 en 2
Banken en NVB gaan ervan uit, dat "aanwijzing met de betrokken bewindspersoon" voor de financiële sector inhoudt, dat de sector via het Ministerie van Financiën wordt betrokken bij deze aanwijzing.
Artikel 3
Hierboven is al uitgebreid ingegaan op de constateringen dat de termen "in belangrijke mate", "kan leiden" en "onverwijld" onvoldoende concreet zijn. Dit moet nader worden ingevuld.
De Memorie van Toelichting spreekt – wat de laatste term betreft – over "zo onverwijld als mogelijk". Dat laatste lijkt een betere term.
Artikel 3 en 4
De wetgeving op dit punt is duidelijk. De Memorie van Toelichting dient te kunnen melden, dat de additionele informatie die het NCSC vraagt, tot stand komt in overleg met de sector, in ons geval de NVB en de banken.
Verder zouden de NVB en de banken hier graag een nuancering willen zien over aan te leveren informatie en de waarborg van vertrouwelijkheid, ook in het kader van de WOB.
Artikel 5
Waarvan acte. Wij onderschrijven het belang dat de AMvB goed duidelijk moet maken in welke gevallen deze afspraken gelden en op welke wijze wordt bepaald welke extra informatie wordt – en kan worden – geleverd.
Artikel 6
Hier is in deze reactie al uitgebreid op ingegaan. Belangrijk vinden de NVB en de banken dan ook dat verzoeken u in deze paragraaf altijd in afstemming met de aanbieder en/of de sector te doen. De aanbieder/sector is immers de partij, die het meest weet wat er speelt.

Nederlandse
Vereniging van Banken

We hopen onze punten van zorg op deze manier voldoende te hebben aangeduid en toegelicht. Uiteraard kunt u voor vragen met mij contact opnemen.

Met vriendelijke groet,

Wim Mijs
Directeur

NEDERLAND ICT

Ministerie van Veiligheid en Justitie
De heer I.W. Opstelten
Postbus 20301
2500 EH DEN HAAG

Woerden, 17 september 2013

Betreft : ontwerpwetsvoorstel melding inbreuken elektronische informatiesystemen
Kenmerk : 35853/

Geachte heer Opstelten,

Graag dank ik u voor uw uitnodiging om te reageren op de consultatie van het ontwerpwetsvoorstel melding inbreuken elektronische informatiesystemen (hierna: het ontwerpwetsvoorstel). Met dit wetsvoorstel wordt een meldplicht voor een inbreuk op de veiligheid of een verlies van integriteit van elektronische informatiesystemen (ICT -inbreuken) geïntroduceerd. Nederland ICT heeft dit ontwerp enerzijds beoordeeld vanuit haar betrokkenheid bij de cybersecurity aanpak in Nederland anderzijds vanuit de doelgroep telecomaanbieders die bij Nederland ICT zijn aangesloten.

Investeren in digitale veiligheid en het beschikbaar houden van ICT-voorzieningen is essentieel voor de netwerkeconomie. Nederland ICT beschouwt transparantie over cyberincidenten als een randvoorwaarde voor het creëren van vertrouwen rond de inzet en gebruik van ICT. Het delen van informatie en leren van incidenten is daar onderdeel van. Tegelijk vraagt Nederland ICT zich af of met een additionele meldplicht wel het doel van de wet wordt bereikt. Doel is immers om de gevolgen bij een incident zo beperkt mogelijk te houden en de overheid optimaal in staat te stellen hulp te bieden waar nodig. Een meldplicht sec legt eenzijdig de focus op het melden en voorschriften hoe de melding eruit moet zien in plaats van het beperken van de gevolgen van cyberincidenten.

Wetsvoorstel stimuleert toezicht in plaats van hulp
ICT Nederland ondersteunt de doelstelling van de wet, zijnde het bieden van hulp door het NCSC. De wet heeft niet tot doel additioneel toezicht in het leven te roepen. Een kernvraag is wie bepaalt dat hulp nodig is, op welk moment en op welke manier assistentie wordt verleend. Dit is in het ontwerp niet geregeld. De hoeveelheid informatie die moet worden aangeleverd roept de vraag op of de overheid niet toch een toezichtsfunctie inricht, als zodanig (onbedoeld) verpakt in het bieden van hulp. Nederland ICT is bezorgd dat de wet in de praktijk anders zal uitpakken ook al wordt in het ontwerpwetsvoorstel niet voorzien in sanctionering en handhaving.

Het verdient aanbeveling dat in de MvT nader wordt omschreven dat de wet geen toezichthoudend karakter heeft

Postbus 401
3440 AK Woerden
Pompmolenlaan 7
3447 GK Woerden

T 0348 49 36 36
F 0348 48 22 88
info@nederlandict.nl
www.nederlandict.nl

ING Bank
Rek.nr. 66 25 90 546
KvK 30174840

NEDERLAND ICT

Bestaande en nieuwe meldplichten onduidelijk maken wet overbodig

Sinds de motie Hennis-Plasschaert in oktober 2011 door de Tweede Kamer werd aanvaard zijn voor het digitale domein meerdere meldplichten in het leven geroepen. De telecomsector kent thans diverse meldplichten. Het ontwerpwetsvoorstel kent een aantal bepalingen waarvan de formulering niet aansluit op verordening 611/2013. Deze verordening heeft rechtstreekse werking en treedt daarmee in de plaats van nationale regelgeving. Daarnaast is onvoldoende duidelijk hoe het ontwerpwetsvoorstel zich verhoudt tot het wetsvoorstel gebruik meldplicht datalekken[1]. Deze nieuwe meldplicht heeft een algemene strekking. In Europa worden nieuwe meldplichten ingericht door middel van een databeschermingsverordening en een richtlijn voor netwerk en informatiebeveiliging (Cyber Security Directive).

In algemene zin gelden thans de volgende meldplichten:

1. meldplicht bij een inbreuk op persoonsgegevens op grond van verordening 611/2013 (in werking getreden op 25 augustus 2013);
2. meldplicht bij ACM bij een inbreuk op beveiliging van persoonsgegevens op grond van artikel 11.3a Tw[2];
3. meldplicht bij het Agentschap Telecom voor (mogelijke) verstoring van continuïteit bij het Agentschap Telecom op grond van artikel 11a.2 Tw[3] en het Besluit continuïteit openbare elektronische communicatienetwerken[4];
4. meldplicht bij verstoring van vitale openbare telecommunicatie-infrastructuur en -diensten bij het Agentschap Telecom op grond van artikel 14.6 lid 2 Tw en de plicht aanwijzingen van de minister van Economische Zaken op te volgen in het geval van buitengewone omstandigheden als bedoeld in hoofdstuk 14 Tw.

In voorkomend geval zijn dus drie verschillende instanties betrokken. Aan deze instanties zal informatie moeten worden gegeven over de aard, omvang en opvolging van het incident. De verhouding tot de bestaande sectorale meldplichten wordt in de MvT niet in voldoende mate toegelicht. Niet duidelijk is of beoogd wordt de aan te leveren informatie te stroomlijnen met de informatie die reeds in het kader van bestaande sectorale meldplichten en de toekomstige brede meldplicht dient te worden aangeleverd. Dat zou zonder meer het geval moeten zijn.

Voorkomen dient te worden dat bedrijven meer bezig zijn met het informeren van toezichthouders dan het oplossen van het incident. Nederland ICT vreest een juridische lappendekken van meldplichten, doublures en onnodige administratieve lasten. De meldplicht dient inhoudelijk zoveel mogelijk met andere meldplichten te worden gestroomlijnd. De wet dient daarvoor een duidelijke grondslag te bieden.

[1] Wetsvoorstel 33 662, nr.2

[2] Aanpassing van de Telecommunicatiewet per 5 juni 2012

[3] Aanpassing van de Telecommunicatiewet per 5 juni 2012

[4] Stb 2012, 514, in werking per 1 januari 2013

Daarnaast worden de volgende meldplichten verwacht:

1. meldplicht voor verlies persoonsgegevens, nu nog bij ACM maar volgens het wetsvoorstel gebruik meldplicht datalekken straks bij het CBP;
2. meldplicht bij ACM bij inbreuken op gekwalificeerde certificaten (wijziging Besluit elektronische handtekeningen, loopt vooruit op Verordening betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt[5]);
3. meldplicht bij ACM/NCSC/CBP op grond van artikel 15 lid 2 ontwerp-Verordening betreffende elektronische identificatie en vertrouwensdiensten;
4. meldplicht inbreuken vitale informatiesystemen op basis van het onderhavige ontwerpwetsvoorstel bij het NCSC;
5. Meldplicht ontwerp-Richtlijn netwerk en informatiebeveiliging (Cyber Security Directive);
6. Meldplicht op grond van ontwerp-Verordening gegevensbescherming.

Nederland loopt in Europa voorop met het introduceren van meldplichten voor inbreuken op vitale informatiesystemen en de beveiliging van persoonsgegevens. Hoe voorkomt u dat binnen afzienbare tijd de meldplicht moet worden herzien in verband met de dan aangenomen Europese richtlijn netwerk en informatiebeveiliging? Hetzelfde geldt voor de Verordening gegevensbescherming die naar verwachting in 2015 in werking treedt en de nieuwe brede meldplicht datalekken en de Wet bescherming persoonsgegevens grotendeels zal vervangen. Ook in praktische zin voegt het wetsvoorstel weinig toe aangezien bedrijven thans ook zonder een wettelijke grondslag het NCSC om ondersteuning kunnen vragen.

In het licht van de Europese ontwikkelingen is het onderhavige wetsvoorstel overbodig, mede gelet op de termijn waarop het in werking zal kunnen treden. Het is wenselijk dat aansluiting wordt gezocht bij de Europese voorstellen in plaats van het creëren van een additionele nationale meldplicht.

De rol van het NCSC is onduidelijk

Het wetsvoorstel is onduidelijk over de rolverdeling tussen het NCSC en bedrijven als actie op een incident moet worden ondernomen. Wat mag een bedrijf van het NCSC verwachten? Moet het NCSC communicatie afstemmen met de onderneming? Dat is ook relevant gelet op het feit dat multinationals veelal ICT-incidenten op basis van financiële regelgeving eerst bij de beurstoezichthouders moeten melden.

Nader uitgewerkt dient te worden wat een bedrijf van het NCSC mag verwachten

Effectiviteit twijfelachtig

Een belangrijke kwestie is het aantal meldingen dat het NCSC zal ontvangen. In het ontwerpwetsvoorstel wordt een goede poging gedaan om de meldplicht af te bakenen tot alleen die incidenten die ernstig maatschappelijke gevolgen kunnen hebben, maar de afbakening is niet eenduidig. De ervaring met de huidige meldplichten leert dat bedrijven zekerheidshalve alle incidenten melden om te voorkomen dat het achterwege blijven van een melding wordt gezien als het 'opzettelijk niet naleven'. Het Agentschap Telecom heeft op basis van de meldplicht van

[5] Voorstel van 4 juni 2012, COM (2012) 238 final

artikel 11.3a Tw binnen één jaar (5 juni 2012 t/m 4 juni 2013) 237 meldingen ontvangen. Voor de meldplicht op basis van artikel 11a.2 Tw betrof het 46 incidenten.[6] Niet alleen kan door de hoeveelheid meldingen en de capaciteit bij het NCSC de effectiviteit in het gedrang komen, ook is de vraag of deze hoeveelheid meldingen bijdraagt aan het uiteindelijke doel: hulp verlenen. Het NCSC zal onmogelijk alle gevallen kunnen beoordelen en ondersteuning kunnen bieden. Zie verder de opmerkingen onder artikel 2- ernstige maatschappelijke gevolgen.

Wet moet rekening houden met uitbesteding van informatiesystemen
Vaak zijn ICT-bedrijven betrokken bij de ondersteuning en het beheer van informatiesystemen van andere bedrijven die diensten aan het publiek aanbieden (o.a. in geval van uitbesteding). De opdrachtgever zal over de meldplicht afspraken moeten maken met het ICT-bedrijf. Dit zal contractueel moeten worden geregeld, en bedrijven zullen dit tijdig, in de koude fase, dienen overeen te komen. Daartoe dient te zijner tijd voldoende gelegenheid te worden gegeven bij het bepalen van het tijdstip van inwerkingtreding van de wet.

Een termijn van zes maanden voor inwerkingtreding is noodzakelijk in verband met noodzakelijke contractuele aanpassingen in de bedrijfsketen

Nationaal loket noodzakelijk – bestaande meldplichten uitzonderen
Er dient één nationaal loket te komen voor alle meldplichten waarbij meldingen door middel van een eenduidig formulier kunnen worden gedaan. Telecomaanbieders dienen wegens bestaande meldplichten zouden voorlopig te uitgezonderd tot het moment dat er één loket is en een eenduidig administratief proces is vastgesteld.

Er dient één nationaal meldplichtloket met eenduidige processen te komen, met een voorlopige uitzondering van de telecomaanbieders

Handhaafbaarheid en rechtsonzekerheid: strijdigheid met AvdW
Het wetsvoorstel is onvoldoende duidelijk over de consequenties van niet-naleving van de meldplicht. Het wetsvoorstel heeft evenwel geen vrijblijvend karakter. Dat neemt niet weg dat het ontbreken van directe handhavingsmogelijkheden niet in overeenstemming is met Aanwijzing 11 van de Aanwijzingen voor de regelgeving. Hierin is bepaald dat niet tot het treffen van een regeling wordt besloten dan nadat is nagegaan of handhaving in voldoende mate te realiseren valt. Het standpunt verwoord op pagina 5 van de MvT onder het kopje 'naleving', inhoudende dat wanneer mocht blijken dat de meldplicht onvoldoende vrijwillig wordt nageleefd alsnog kan worden besloten tot het inrichten van een stelsel van toezicht en handhaving, is daarmee niet in overeenstemming. Dit staat tevens op gespannen voet met het rechtzekerheidsbeginsel. Een stelsel van toezicht en handhaving moet worden ingericht voordat de wettelijke regeling in werking treedt.

Conform de Aanwijzingen voor de regelgeving dient eerst te worden nagegaan of handhaving in voldoende mate valt te realiseren

[6] Presentatie Ministerie van Economische Zaken in het OPT d.d. 4 juni 2013

NEDERLAND ICT

Artikelsgewijze opmerkingen

› *Artikel 2 aan te wijzen aanbieders* – In het ontwerp wordt voorgesteld om de afbakening van de aanbieders en vitale producten/ diensten die onder de meldplicht vallen, te bepalen in een AMvB. De schaalgrootte van het bedrijf en de marktverhoudingen spelen een belangrijke rol bij de vraag of een product of dienst een vitaal karakter heeft. Nederland ICT vindt dat hierbij dient te worden uitgegaan van afbakening conform de vastgestelde 31 vitale producten en diensten in Nederland (programma bescherming vitale infrastructuren). Aldus wordt optimaal aangesloten bij bestaande structuren.

› *Artikel 2 ernstige maatschappelijke gevolgen* - Waar in de aanhef bij de wet en artikel 2 wordt gesproken over "ernstige maatschappelijke gevolgen" gaat het in artikel 6 lid 1 over "schadelijke maatschappelijke gevolgen". Nederland ICT stelt voor om ook in artikel 6 lid 1 te spreken van 'ernstige maatschappelijke gevolgen'. Tegelijk stelt Nederland ICT voor om 'ernstige maatschappelijke gevolgen' in de MvT nader toe te lichten. Dit is nu zeer open geformuleerd waarbij bedrijven niet kunnen inschatten wat wel en wat niet gemeld hoeft te worden. Aansluiting kan worden gezocht bij de ENISA Technical Guidelines on Reporting Incidents[7]. In dit verband is van belang dat het NCSC open staat voor overleg of een incident mogelijk meldenswaardig is. Onnodige meldingen moeten worden voorkomen, maar te strikte interpretatie van de meldplicht ook. Het NCSC is geëquipeerd om bedrijven bij te staan voorafgaand aan het doen van een melding.

› *Artikel 3 onverwijlde melding* - Het artikel spreekt van 'onverwijld' als termijn voor de melding. Ook artikel 34a Wbp en artikel 11.3a Tw bepalen dat de aanbieder de toezichthouder onverwijld in kennis dient te stellen van inbreuken. Het begrip 'onverwijld' is echter niet eenduidig en wordt in de regelgeving op onderscheiden wijze ingevuld. In de ontwerp-Verordening gegevensbescherming wordt voor de meldplicht van artikel 31 lid 1 uitgegaan van aanlevering 'zonder onredelijke vertraging' en indien haalbaar, niet later dan 24 uur. Dit sluit aan bij de gangbare praktijk voor aanlevering van gegevens aan de overheid. Nederland ICT vindt het van belang dat zoveel mogelijk wordt aangesloten op komende Europese regelgeving.

› Artikel 3 *in belangrijke mate* – Bepaald is dat melding dient te worden gedaan als de beschikbaarheid of betrouwbaarheid van een dienst 'in belangrijke mate' wordt onderbroken. Voor de criteria voor het bepalen van de ernst van de inbreuk dient te worden uitgegaan van de criteria die zijn ontwikkeld door de ICT Response Board (IRB) als onderdeel van het NCSC.

› *Artikel 4 informatieplicht* - Nederland ICT vindt dat het NCSC zich terughoudendheid moet opstellen bij het proactief opvragen van informatie. Een organisatie die getroffen wordt, heeft de handen vol aan de bestrijding van een incident en in die situatie moet de focus zoveel mogelijk liggen op incidentrespons en niet op administratieve handelingen of niet-noodzakelijke informatie-uitwisseling. Ook het verlenen van hulp dient in overleg te gebeuren. Bedrijven hebben een eigen verantwoordelijkheid en de overheid moet niet op de stoel van bedrijven gaan zitten.

[7] http://www.enisa.europa.eu/

- Artikel 6 gegevens*verstrekking aan derden/openbaarmaking* – De aanbieder zal het NCSC vergaand moeten informeren over de aard van het incident om het NCSC in staat te stellen hulp te bieden. Dat betekent dat het NCSC zal kunnen beschikken over bedrijfsvertrouwelijke en anderszins gevoelige informatie. Het eerste lid 1 onder c geeft de kaders voor het informeren van het publiek. Hierin wordt nadrukkelijk wel de veiligheid van de Staat als afwegingsgrond meegenomen maar niet de belangen van de betreffende organisatie. Het tweede lid bepaalt dat openbaarmaking van informatie die herleidbaar is tot afzonderlijke aanbieders, producten of diensten niet plaatsvindt, tenzij het maatschappelijk belang dat vergt. In dit kader is essentieel dat vertrouwelijke omgang met deze informatie wordt gewaarborgd. Artikel 6 beoogt dat te doen, maar gaat daarin niet ver genoeg, omdat (a) het wetsvoorstel weliswaar een materiële noodzakelijkheidstoets bevat, neergelegd in het tweede lid, maar onvoldoende duidelijk is wat onder 'maatschappelijk belang' zal moeten worden verstaan, (b) de bepaling in lid 3 door de zinsnede "onverminderd andere wetten" een open regeling bevat ten aanzien van het gebruik van de gegevens en (c) het wetsvoorstel de aanbieder geen voorafgaande inzagemogelijkheid geeft bij verstrekking van de gegevens aan derden. Nederland ICT acht het van belang dat de wet een uitdrukkelijke grondslag biedt voor het maken van een belangenafweging waarbij ook met de belangen van de betrokken organisatie rekening wordt gehouden, waarbij voorafgaand overleg plaatsvindt.

- De zinsnede 'onverminderd andere wetten' in artikel 6 lid 3 lid roept tevens de vraag op of wordt beoogd dat ook informatie kan of desgevraagd dient te worden verstrekt aan ACM op basis van artikel 7 ACM Instellingswet. Dit is onwenselijk. Het NCSC is immers geen 'bestuursorgaan, dienst, toezichthouder en andere persoon, belast met de opsporing van strafbare feiten, onderscheidenlijk het toezicht op de naleving van wettelijke voorschriften'. De publiekrechtelijke status van het NCSC als onderdeel van het ministerie van V&J dient in dit verband in de MvT nader te worden toegelicht om misverstanden te voorkomen.

Conclusie en aanbeveling

Alles overziende is de onduidelijke verhouding ten opzichte van de overige (sectorale) meldplichten onbevredigend. Het wetsvoorstel staat op gespannen voet met het rechtszekerheidsbeginsel als bedoeld in artikel 18 van de Aanwijzingen voor de regelgeving. Niet duidelijk is wat de consequenties van niet-naleving zijn. Afwijking van de Aanwijzingen voor de regelgeving is alleen toegestaan indien onverkorte toepassing uit het oogpunt van goede regelgeving niet tot aanvaardbare resultaten zou leiden. Gelet op de ontwerp-Richtlijn netwerk en informatiebeveiliging en de ontwerp-Verordening voor gegevensbescherming, de reeds bestaande nationale sectorale wetgeving en de nieuwe wet gebruik meldplicht datalekken is het onderhavige ontwerpwetsvoorstel de facto overbodig.

Nederland ICT stelt voor dat, wanneer toch gekozen wordt voor een nationale meldplicht vitale informatiesystemen, anderhalf jaar na invoering een evaluatie plaatsvindt om de effectiviteit ervan vast te stellen en de wet te herijken aan alsdan geldende nationale en Europese regelgeving. In ieder

NEDERLAND ICT

geval dient de telecomsector van de wet te worden uitgezonderd gelet op de reeds bestaande sectorspecifieke meldplichten en de wet brede meldplicht datalekken.

Met deze reactie hoopt Nederland ICT een constructieve bijdrage te leveren aan het versterken van de cyber security maatregelen in Nederland. Nederland ICT stimuleert samenwerking en de inzet van middelen om inbreuken op vitale informatiesystemen alsmede de gevolgen zoveel mogelijk te beperken.

De inhoud van deze reactie wordt tevens ondersteund door Tele2 en NLKabel.

Met vriendelijke groet,
Nederland ICT

Peter van Schelven
Directeur a.i.

netbeheer nederland
energie in beweging

vereniging van
energienetbeheerders
Nederland

Anna van Buerenplein 43
2595 DA Den Haag
Postbus 90606
2509 LP Den Haag
Telefoon 070 - 2055 000
secretariaat@netbeheernederland.nl
www.netbeheernederland.nl

Ministerie van Veiligheid en Justitie
Directie Wetgeving en Juridische Zaken

Postbus 20301
2500 EH DEN HAAG

Uw kenmerk	412089
Ons kenmerk	BR-13-899
Behandeld door	
Telefoon	
E-mail	
Datum	16 september 2013
Onderwerp	Reactie Netbeheer Nederland – consultatie wetsvoorstel meldplicht ICT-inbreuken

Het ministerie van Veiligheid en Justitie heeft op 22 juli jl. het wetsvoorstel melding inbreuken elektronische informatiesystemen voor consultatie gepubliceerd. Netbeheer Nederland maakt graag gebruik van de geboden gelegenheid om namens de gezamenlijke netbeheerders haar zienswijze ten aanzien van dit wetsvoorstel aan u kenbaar te maken.

Algemeen

De vereniging Netbeheer Nederland is de belangenbehartiger van de wettelijk aangewezen landelijke en regionale elektriciteit- en gasnetbeheerders. Netbeheer Nederland is het aanspreekpunt voor netbeheeraangelegenheden. De (energie)netbeheerders hebben twee hoofdtaken: zij faciliteren het functioneren van de markt en beheren de fysieke netinfrastructuur. Onder invloed van met name Europese en nationale klimaatdoelstellingen speelt – naast een veilig, betrouwbaar en betaalbaar transport van energie – het faciliteren van de transitie naar een duurzame energievoorziening een steeds belangrijkere rol in het werkveld van Netbeheer Nederland. Deze ontwikkeling stelt onder andere eisen aan de energie-infrastructuur.

Onderhavig wetsvoorstel introduceert een meldplicht voor ICT-inbreuken aan het Nationaal Cyber Security Centrum (NCSC), een onderdeel van het ministerie van Veiligheid en Justitie. De meldplicht geldt alleen voor aanbieders van producten of diensten waarvan de beschikbaarheid of betrouwbaarheid van vitaal belang is voor de Nederlandse samenleving, en alleen als de inbreuk tot gevolg

ABN-AMRO 81.30.01.036
KvK Arnhem 09175117

heeft of kan hebben dat die beschikbaarheid of betrouwbaarheid in belangrijke mate wordt onderbroken. De sectoren elektriciteit en gas, meer in het bijzonder 'energienetwerkbeheerders', worden in de memorie van toelichting van het wetsvoorstel expliciet vermeld als doelgroep. Gelet hierop beschouwt Netbeheer Nederland zich – namens de gezamenlijke elektriciteit- en gasnetbeheerders – als belanghebbende bij het voorliggende wetsvoorstel meldplicht voor ICT-inbreuken. Netbeheer Nederland heeft t.a.v. dit wetsvoorstel de volgende opmerkingen.

Begrippen en reikwijdte meldplicht (artikel 1 t/m 3)
De meldplicht in het wetsvoorstel ziet alleen op een daadwerkelijke inbreuk op de veiligheid en op een daadwerkelijk verlies van integriteit van een elektronisch informatiesysteem. De nog bij Algemene Maatregel van Bestuur (AMvB) aan te wijzen organisaties in de vitale sectoren zijn echter, aldus de memorie van toelichting bij het wetsvoorstel, niet verplicht om elke ICT-inbreuk te melden aan het NCSC. De verplichting tot melden geldt alleen als de inbreuk tot gevolg heeft of kan hebben dat de beschikbaarheid of betrouwbaarheid van de nog bij AMvB aan te wijzen producten of diensten in belangrijke mate wordt of kan worden onderbroken met maatschappelijke ontwrichting als (mogelijk) gevolg. Wat onder 'in belangrijke mate' moet worden verstaan wordt in onderhavig wetsvoorstel echter niet verduidelijkt. Wel wordt in de memorie van toelichting aangegeven dat 'mede op basis van overleg met de betrokken sectoren en departementen' nader zal worden uitgewerkt wat voor de verschillende producten en diensten moet worden verstaan onder *in belangrijke mate*.

Naar de mening van Netbeheer Nederland is op basis van het voorliggende wetsvoorstel niet duidelijk wanneer het voorgenomen overleg met de betreffende sectoren zal plaatsvinden. Van belang is volgens Netbeheer Nederland dat dit overleg in het kader van onderhavig wetgevingstraject tijdig zal moeten plaatsvinden om de exacte reikwijdte van het wetsvoorstel meldplicht ICT-inbreuken nader te bepalen. Met het oog op de rechtszekerheid is het daarbij van belang dat de uitkomsten van het overleg met de betreffende sectoren in de wettekst en/of bijbehorende memorie van toelichting tot uitdrukking komen. In het voorgenomen sectorenoverleg zal naar de opvatting van Netbeheer Nederland – naast de invulling van het begrip maatschappelijke ontwrichting – ook specifiek aandacht moeten worden besteed aan de begrippen *inbreuk op de veiligheid* en *verlies van integriteit* van een elektronisch systeem. Ook een nadere concretisering van deze begrippen is mede bepalend voor de precieze reikwijdte van onderhavig wetsvoorstel. Op dit punt schiet het voorliggende wetsvoorstel, althans in de memorie van toelichting, tot dusverre tekort.

Netbeheer Nederland geeft hierbij aan als belanghebbende graag deel te nemen aan het voorgenomen sectorenoverleg.

Aanvullende informatieplicht (artikel 4)
Volgens de memorie van toelichting is denkbaar dat het NCSC naar aanleiding van een melding nadere gegevens nodig heeft om de aard en ernst van de ICT-inbreuk te kunnen inschatten en de aanbieder adequaat te kunnen helpen. In deze gevallen is in het voorliggende wetsvoorstel (artikel 4) een aanvullende informatieplicht opgenomen, die volgens de memorie van toelichting 'wordt geactiveerd door een concreet verzoek van het NCSC in reactie op een in artikel 3 bedoelde melding'.

Netbeheer Nederland is van mening dat in de memorie van toelichting expliciet zal moeten worden opgenomen dat gebruikmaking van de aanvullende informatieplicht door NCSC (namens de minister van Veiligheid en Justitie) niet verder gaat dan strikt noodzakelijk. Deze toevoeging dient namelijk te voorkomen dat NCSC (namens de minister van Veiligheid en Justitie) op een ongelimiteerde wijze gebruik maakt van de aanvullende informatieplicht. Daarnaast wijst Netbeheer Nederland erop dat de nog op te stellen AMvB de juiste handvatten zal moeten bieden voor het kunnen verrichten van een toereikende melding. Ook dit kan ertoe leiden dat gebruikmaking van de aanvullende informatieplicht meer uitzondering dan regel is ter voorkoming van onnodige administratieve lasten.

Ten slotte, een zorgvuldige en terughoudende opstelling bij het gebruikmaken van de aanvullende informatieplicht sluit ook aan op het zogenoemde proportionaliteitsbeginsel waaraan overheidsoptreden – in het kader van de (bestuursrechtelijke) algemene beginselen van behoorlijk bestuur – is gebonden.

Vertrouwelijkheid gegevens melding (artikel 6)

Wettelijke geheimhoudingsbepalingen

Op grond van artikel 6 van het voorliggende wetsvoorstel heeft de minister van Veiligheid en Justitie de bevoegdheid de in het kader van een melding verstrekte gegevens te gebruiken als basis voor advies en informatie aan 1) andere meldplichtige organisaties, 2) door de minister aangewezen CERT's (computercrisisteams) en 3) aan het publiek. Hoewel uit de memorie van toelichting kan worden opgemaakt dat de minister op dit punt zorgvuldig en terughoudend te werk moet gaan, is naar de mening van Netbeheer Nederland hierin ten onrechte geen expliciete aandacht besteed aan wettelijke geheimhoudingsbepalingen, die voor bepaalde sectoren gelden. De Elektriciteitswet 1998 bevat bijvoorbeeld de volgende geheimhoudingsbepaling (artikel 79, eerste lid):

> "1. *Een netbeheerder die bij de uitvoering van zijn taak de beschikking krijgt over gegevens waarvan hij het vertrouwelijke karakter kent of redelijkerwijs moet vermoeden, is verplicht tot geheimhouding van die gegevens, behoudens voor zover enig wettelijk voorschrift hem tot mededeling verplicht, of uit zijn taak de noodzaak tot mededeling voortvloeit*".

Netbeheer Nederland is van oordeel dat artikel 6 van het voorliggende wetsvoorstel op gespannen voet staat met sectorale geheimhoudingsbepalingen, zoals artikel 79, eerste lid, van de Elektriciteitswet 1998. Derhalve zal het wetsvoorstel eveneens op dit onderdeel nader uitgewerkt moeten worden. Het op initiatief van het ministerie van Veiligheid en Justitie nog te organiseren sectorenoverleg zou hiertoe een constructieve bijdrage kunnen leveren, mits dit onderdeel ook daadwerkelijk wordt geagendeerd (naast de concretisering van de centrale begrippen in dit wetsvoorstel).

EPCIP-richtlijn

Daarnaast wijst Netbeheer Nederland op EU-richtlijn nr. 2008/114 inzake de identificatie van Europese kritieke infrastructuren (EPCIP-richtlijn) in samenhang met EU-verordening nr. 543/2013 (Transparantieverordening). Het is namelijk mogelijk dat delen van energienetwerken op basis van de EPCIP-richtlijn worden aangemerkt als European Critical Infrastructures (ECI's) om in het bijzonder de grensoverschrijdende leveringszekerheid van energie te beschermen tegen door mensen veroorzaakte dreigingen, technologische dreigingen en natuurrampen. De eigenaren/exploitanten zijn uiteindelijk verantwoordelijk voor de bescherming van de betreffende ECI's. In de Transparantie-verordening is voorzien in de mogelijkheid om de identificatie en locatie van de kritische netonderdelen als gevoelige informatie in de zin van EPCIP-richtlijn aan te merken. Dat betekent dat wanneer ECI's zijn aangemerkt, de betreffende (energie)netbeheerder verplicht kan zijn om de naam en locatie daarvan geheim te houden.

Nu de geheimhoudingsplicht van artikel 79, eerste lid, van de Elektriciteitswet 1998 op basis van het voorliggende wetsvoorstel wordt doorbroken, zal naar de opvatting van Netbeheer Nederland in dit wetsvoorstel nauwkeurig moet worden omschreven welke gegevens aan het NCSC moeten worden gemeld. In dit verband moet in het wetsvoorstel ook de geheimhouding van de specifieke informatie omtrent ECI's, die een netbeheerder aan NCSC moet melden, worden geborgd.

Samenloop wetsvoorstel meldplicht datalekken

In de memorie van toelichting van het wetsvoorstel wordt ook ingegaan op de verhouding tot het wetsvoorstel meldplicht datalekken. Hier wordt gesteld dat de situatie zich kan voordoen dat een ICT-inbreuk onder beide meldplichten valt. In dat geval moet de inbreuk, aldus de memorie van toelichting, derhalve zowel bij het NCSC als bij het College bescherming persoonsgegevens (Cbp) worden gemeld. Naar het oordeel van Netbeheer Nederland wordt hieraan terecht toegevoegd dat nodeloze administratieve lasten zullen worden voorkomen door onderlinge afstemming van de wijze waarop moet worden gemeld en de gegevens die dienen te worden verstrekt, en door processen efficiënt in te richten. Niettemin merkt Netbeheer Nederland in dit verband op dat juist de onderlinge afstemming van meldplichten in de memorie van toelichting nadere invulling behoeft. De huidige formulering op dit onderdeel is namelijk ontoereikend en daardoor te vrijblijvend van aard.

AMvB

Volgens het voorliggende wetsvoorstel zal bij de Algemene Maartregel van Bestuur (AMvB) nader worden geregeld voor welke partijen de meldplicht gaat gelden, welke gegevens moet worden gemeld en op welke wijze zal moeten worden gemeld. Netbeheer Nederland vindt het van belang dat zij namens de elektriciteit- en gasnetbeheerders ook bij de inhoudelijke vormgeving van deze AMvB wordt betrokken.

Ten slotte, middels deze brief heeft Netbeheer Nederland haar zienswijze ten aanzien van het wetsvoorstel meldplicht ICT-inbreuken aan uw ministerie kenbaar gemaakt. Mocht uw ministerie in het verdere wetgevingstraject behoefte hebben aan een nadere toelichting, dan is Netbeheer Nederland daartoe graag bereid. U kunt hiervoor contact opnemen met de heer Durk Groenveld, jurist

van Netbeheer Nederland (zie briefhoofd voor contactgegevens).

Met vriendelijke groet,

Laurens Knegt
directeur

Schiphol Group

0 BD

Ministerie van Veiligheid & Justitie
Directie Wetgeving & Juridische Zaken
Sector staat- en bestuursrecht

Telefoonnummer	Briefnummer	Bijlage	
020-6012789		1	
Faxnummer	Behandeld door	Uw schrijven d.d.	Schiphol,
		22-07-2013	5 september 2013

Betreft: Verzoek commentaar [uw kenmerk 412081]

Hierbij stuur ik u, r. het commentaar op het wetsvoorstel melding inbreuken elektronische informatiesystemen.
Een copy zal tevens middels e-mail aan u worden verstrekt.

Met vriendelijke groet,

Schiphol Group

Hans Aldenkamp
Information Security Advisor

Schiphol Group Postbus 7501 1118 ZG Schiphol Telefoon (020) 601 91 11 Fax (020) 604 14 75
Schiphol Nederland BV K v K Amsterdam nr 34166584
ABN AMRO Bank NV nr 54.56.10.478 ABN AMRO Bank NV nr 48.67.49.304 ING Bank nr 69.76.60.729

Op- en aanmerkingen concept Wetsvoorstel melden inbreuken elektronische informatiesystemen
Ingebracht door Schiphol Nederland BV, i.o.v. se vanuit brief Min V&J (Kenmerk 412081)

Voorstel van wet

Wij Willem-~~Alexander~~Alexander, bij de gratie Gods, Koning der Nederlanden, Prins van Oranje-Nassau, enz. enz. enz.
Allen, die deze zullen zien of horen lezen, saluut! doen te weten:
Alzo Wij in overweging genomen hebben, dat het wenselijk is een verplichting in het leven te roepen voor organisaties die deel uitmaken van de vitale infrastructuur van Nederland om een inbreuk op de veiligheid of een verlies van integriteit van hun elektronische informatiesystemen te melden teneinde ernstige maatschappelijke gevolgen daarvan te voorkomen of beperken;
Zo is het, dat Wij, de Afdeling advisering van de Raad van State gehoord, en met gemeen overleg der Staten-Generaal, hebben goedgevonden en verstaan, gelijk Wij goedvinden en verstaan bij deze:

Artikel 1

In deze wet en de daarop gebaseerde bepalingen wordt verstaan onder:
- aanbieder: degene die een product of dienst exploiteert, beheert of beschikbaar stelt;
- informatiesysteem: geheel of gedeeltelijk met elektronische middelen bestuurd systeem waarvan een product of dienst afhankelijk is;
- Onze Minister: Onze Minister van Veiligheid en Justitie;
- product of dienst: product of dienst als bedoeld in artikel 2.

Artikel 2

Deze wet is van toepassing op de bij algemene maatregel van bestuur aan te wijzen aanbieders van de daarbij aan te wijzen 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.

Artikel 3

1. De aanbieder geeft Onze Minister onverwijld kennis van een inbreuk op de veiligheid of een verlies van integriteit van zijn informatiesysteem waardoor de beschikbaarheid of betrouwbaarheid van een product of dienst in belangrijke mate wordt of kan worden onderbroken.
2. De kennisgeving omvat in ieder geval:
a. de aard en omvang van de inbreuk of het verlies;
b. het tijdstip van de aanvang van de inbreuk of het verlies;
c. de mogelijke gevolgen van de inbreuk of het verlies;
d. een prognose van de hersteltijd;
e. zo mogelijk de door de aanbieder genomen of te nemen maatregelen om de gevolgen van de inbreuk of het verlies te beperken of herhaling hiervan te voorkomen;
f. de contactgegevens van de in Nederland gevestigde functionaris die verantwoordelijk is voor het doen van de kennisgeving.

Opmerking [HA1]: Consultatie bij voorkeur via reguliere overleggen aangesloten bij het NCSC. In ons geval Airport-ISAC.
CONCREET:
Wie wijst aan welke producten of diensten onder de werkingssfeer vaan deze wet gaan vallen? Intern leidt dit al tot discussie over kreten als "vitaal voor de Nederlandse samenleving" of "ontwrichtend".

Opmerking [HA2]: Integriteit en beschikbaarheid zijn 2 afzonderlijke dingen. Een systeem kan qua integriteit (data-juistheid) zijn aangetast, maar kan nog 100% beschikbaar zijn. Meestal wordt gesproken over betrouwbaarheidseisen bestaande uit Beschikbaarheid, Integriteit, en Vertrouwelijkheid (BIV)

Opmerking [HA3]: Hier ligt een directe relatie met het begrip 'kan leiden tot' in laatste zin van artikel 2. Dus een verwachting of mogelijke impact en dus per definitie subjectief. Er is meer behoefte aan objectiviteit in deze.

Artikel 4

Desgevraagd verstrekt de aanbieder die een kennisgeving als bedoeld in artikel 3 heeft gedaan, Onze Minister onverwijld alle overige gegevens die nodig zijn om:
a. de risico's voor de beschikbaarheid of betrouwbaarheid van het product of de dienst in te schatten;
b. de aanbieder bij te staan bij het treffen van maatregelen om de beschikbaarheid en betrouwbaarheid van het product of de dienst te waarborgen of te herstellen.

Opmerking [HA4]: Dit vraagt om een verdere detaillering! Er zou eerder gesproken kunnen worden over "hoofzakelijke" gegevens. Als voorbeeld: "Wij sluiten persoonsgegevens en klantgegevens uit".
AANVULLING: Wat wordt de bewaartermijn??

Artikel 5

Bij of krachtens algemene maatregel van bestuur worden nadere regels gesteld over de artikelen 3 en 4, waaronder in ieder geval nadere regels over:
a. de gegevens die ter uitvoering van artikel 3 worden verstrekt;
b. de wijze waarop een kennisgeving als bedoeld in artikel 3 wordt gedaan en waarop gegevens als bedoeld in artikel 4 worden verstrekt.

Opmerking [HA5]: Gegevens worden in principe vertrouwelijk aangeleverd. Dit betekent zeker niet via publieke mail. Dus enige afspraken over encryptie is zeker van toepassing.

Artikel 6

1. Ter voorkoming of beperking van schadelijke maatschappelijke gevolgen in of buiten Nederland van een inbreuk of een verlies als bedoeld in artikel 3, eerste lid, kan Onze Minister de gegevens, bedoeld in de artikelen 3 en 4, gebruiken voor het geven van informatie en advies aan:
a. andere aanbieders;
b. een bij regeling van Onze Minister aangewezen computercrisisteam in of buiten Nederland;
c. het publiek, mits de veiligheid van de Staat daarmee niet geschaad kan worden.
2. Tenzij het maatschappelijke belang dat vergt, worden aan het publiek geen gegevens verstrekt die herleid kunnen worden tot afzonderlijke aanbieders, producten of diensten.
3. Onverminderd andere wetten worden de gegevens uitsluitend gebruikt voor de in artikel 4 omschreven doelen of ter uitvoering van het eerste lid.
4. Bij of krachtens algemene maatregel van bestuur kunnen nadere regels worden gesteld over het eerste lid.

Opmerking [HA6]: Door wie wordt dit bepaald? De minister of het NCSC..??

Artikel 7

De artikelen van deze wet treden in werking op een bij koninklijk besluit te bepalen tijdstip dat voor de verschillende artikelen of onderdelen daarvan verschillend kan zijn.

Artikel 8

Deze wet wordt aangehaald als: Wet melding inbreuken elektronische informatiesystemen.

Lasten en bevelen dat deze in het Staatsblad zal worden geplaatst en dat alle ministeries, autoriteiten, colleges en ambtenaren wie zulks aangaat, aan de nauwkeurige uitvoering de hand zullen houden.

Vewin
Vereniging van waterbedrijven in Nederland

Minister van Veiligheid en Justitie
de heer mr. I.W. Opstelten
Postbus 20301
2500 EH Den Haag

onderwerp Reactie wetsvoorstel melding inbreuken elektronische informatiesystemen
uw kenmerk 412095
ons kenmerk 95167/SG
voor informatie

datum 17 september 2013

Geachte heer Opstelten,

Graag maakt Vewin gebruik van de mogelijkheid te reageren op de consultatie van het concept wetsvoorstel melding inbreuken elektronische informatiesystemen.

Bijgevoegd treft u de position paper van Vewin (bijlage 1), evenals tekstvoorstellen tot aanvulling van het wetsvoorstel en de Memorie van Toelichting (bijlage 2).

Onze belangrijkste wensen zijn:

1. ICT-inbreuken via de sectorale toezichthouder (ILT) bij het NCSC melden
2. Geen interventiebevoegdheid voor het NCSC richting drinkwaterbedrijven
3. Meldingen van ICT-inbreuken en alle verstrekte gegevens uitzonderen van de Wob

Hoogachtend,

drs. Th.J.J. Schmitz
directeur

Vewin
Bezuidenhoutseweg 12
2594 AV Den Haag
T (070) 3490 350
info@vewin.nl
www.vewin.nl
Postbus 90611 • 2509 LP Den Haag

Vewin
Vereniging van waterbedrijven in Nederland

Bijlage 1
Position Paper

Wet melding inbreuken elektronische informatiesystemen

Aansluiting bij bestaande meldplichten
Met het wetsvoorstel melding inbreuken elektronische informatiesystemen krijgen drinkwaterbedrijven een dubbele meldplicht: aan het NCSC en aan de sectorale toezichthouder, de Inspectie voor Leefomgeving en Transport (ILT) van het ministerie van IenM. Dit is niet in lijn met de uitgangspunten zoals op 6 juni 2012 door de Minister van VenJ aan de Tweede Kamer is gecommuniceerd: "Zoveel als mogelijk zal worden aangesloten bij bestaande meldplichten waardoor organisaties slechts op één plek hoeven te melden en administratieve lasten beperkt worden." Een rechtstreekse melding aan het NCSC is vanuit sectoraal toezicht onwenselijk. Melden en toezicht zijn onlosmakelijk met elkaar verbonden en moeten in één hand (blijven) liggen. Op basis van de Drinkwaterwet (DWW) zijn (potentiële) drinkwaterverstoringen meldplichting bij de ILT. Hieronder vallen ook ICT-inbreuken met een (potentiële) drinkwaterverstoring als gevolg. In overleg tussen het drinkwaterbedrijf en de ILT worden de (mogelijke) gevolgen van de inbreuk beoordeeld en daarmee de noodzaak van melding aan het NCSC. Indien nodig, meldt de ILT de inbreuk bij het NCSC.

➢ **ICT-inbreuken worden via de ILT bij het NCSC gemeld**

Adviezen op afstand
De functie van het NCSC is het bieden van hulp en coördinatie om een ICT-inbreuk te dichten en maatschappelijke ontwrichting zoveel als mogelijk te voorkomen. De adviezen en ondersteuning van het NCSC zijn niet-afdwingbaar. Het NCSC heeft, zonder tussenkomst van bevoegd gezag (IenM), géén interventiebevoegdheden jegens de drinkwaterbedrijven.

➢ **Het NCSC heeft geen interventiebevoegdheid richting drinkwaterbedrijven**

Betere verankering van de vertrouwelijkheid van meldingen en alle verstrekte gegevens
De DWW stelt (art. 37, lid 4) dat de in het leveringsplan opgenomen gegevens, die betrekking hebben op het voorkomen van een verstoring, de voorbereiding op een verstoring dan wel het optreden in geval van een verstoring, informatie is als bedoeld in artikel 10 van de Wob.
Volgens de toelichting bij het wetsvoorstel betreft de bij de melding verstrekte informatie in het algemeen bedrijfs- en fabricagegegevens als bedoeld in de uitzonderingsgrond van art. 10, eerste lid, sub c, van de Wob. In het wetsvoorstel zelf is dit niet geregeld. Vewin pleit voor een bepaling in de wet waarbij identiek aan de DWW een aanname van vertrouwelijke informatie in de zin van de Wob wordt geregeld. Bescherming van kwetsbare informatie moet wettelijk ingebouwd worden.

➢ **Meldingen van ICT-inbreuken en alle verstrekte gegevens uitzonderen van de Wob**

Den Haag, 17 september 2013
Voor informatie: Sabine Gielens, 070 349 08 83, gielens@vewin.nl

Vewin
Bezuidenhoutseweg 12
2594 AV Den Haag
T (070) 3490 850
info@vewin.nl
www.vewin.nl
Postbus 90611 • 2509 LP Den Haag

Vewin
Vereniging van waterbedrijven in Nederland

Bijlage 2 Voorstellen tot aanvulling van het wetsvoorstel en de MvT (vet gearceerd)

'Voorstel van wet

Artikel 3

1. De aanbieder geeft, **met inachtneming van het bepaalde in lid 3**, Onze Minister onverwijld kennis van een inbreuk op de veiligheid of een verlies van integriteit van zijn informatiesysteem waardoor de beschikbaarheid of betrouwbaarheid van een product of dienst in belangrijke mate wordt of kan worden onderbroken.
2. De kennisgeving omvat in ieder geval:
a. de aard en omvang van de inbreuk of het verlies;
b. het tijdstip van de aanvang van de inbreuk of het verlies;
c. de mogelijke gevolgen van de inbreuk of het verlies;
d. een prognose van de hersteltijd;
e. zo mogelijk de door de aanbieder genomen of te nemen maatregelen om de gevolgen van de inbreuk of het verlies te beperken of herhaling hiervan te voorkomen;
f. de contactgegevens van de in Nederland gevestigde functionaris die verantwoordelijk is voor het doen van de kennisgeving.
3. De kennisgeving als bedoeld in lid 1, alsmede de gegevensverstrekking als bedoeld in lid 2, geschiedt door tussenkomst van Onze Minister wie het aangaat, de betrokken toezichthouder of een andere bij regeling van Onze Minister in overeenstemming met Onze Minister wie het aangaat aangewezen instantie aan wie de vitale aanbieder een inbreuk op de veiligheid of een verlies van integriteit van zijn informatiesysteem dient te melden.

Artikel 4

1. Desgevraagd verstrekt de aanbieder die een kennisgeving als bedoeld in artikel 3 heeft gedaan, Onze Minister onverwijld alle overige gegevens die nodig zijn om:
a. de risico's voor de beschikbaarheid of betrouwbaarheid van het product of de dienst in te schatten;
b. de aanbieder bij te staan bij het treffen van maatregelen om de beschikbaarheid en betrouwbaarheid van het product of de dienst te waarborgen of te herstellen.
2. De kennisgeving als bedoeld in artikel 3 en de verstrekte gegevens in het vorige lid van dit artikel zijn informatie als bedoeld in artikel 10, lid 1, van de Wet openbaarheid van bestuur.

Artikel 6

1. Ter voorkoming of beperking van schadelijke maatschappelijke gevolgen in of buiten Nederland van een inbreuk of een verlies als bedoeld in artikel 3, eerste lid, kan Onze Minister de gegevens, bedoeld in de artikelen 3 en 4, gebruiken voor het geven van informatie en advies aan:
a. andere aanbieders;
b. een bij regeling van Onze Minister aangewezen computercrisisteam in of buiten Nederland;
c. het publiek, mits de veiligheid van de Staat daarmee niet geschaad kan worden. Tenzij het maatschappelijke belang dat vergt, worden aan het publiek geen gegevens verstrekt die herleid kunnen worden tot afzonderlijke aanbieders, producten of diensten.
2. Het verstrekken van informatie als bedoeld in lid 1 vindt plaats in afstemming met de betrokken aanbieder en diens toezichthouder.
3. Onverminderd andere wetten worden de gegevens uitsluitend gebruikt voor de in artikel 4 omschreven doelen of ter uitvoering van het eerste lid.
4. Bij of krachtens algemene maatregel van bestuur kunnen nadere regels worden gesteld over het eerste lid.

Vewin
Bezuidenhoutseweg 12
2594 AV Den Haag
T (070) 3490 850
info@vewin.nl
www.vewin.nl
Postbus 90611 • 2509 LP Den Haag

Vewin
Vereniging van waterbedrijven in Nederland

Memorie van Toelichting

Taak van het Nationaal Cyber Security Centrum (blz. 2)
Het verlenen van hulp aan getroffen vitale organisaties en het waarschuwen van andere vitale organisaties voor gebleken kwetsbaarheden, met als doel om maatschappelijke ontwrichting te voorkomen of in elk geval zo veel mogelijk te beperken, staat in het geval van het NCSC dus centraal. Hierdoor alsook door het ontbreken van de mogelijkheid van sanctionering **en het ontbreken van een interventiebevoegdheid**, onderscheiden de taak van het NCSC en de meldplicht die het NCSC in staat stelt die taak te vervullen, zich van die van bijvoorbeeld de sectorale toezichthouders en de in enkele sectoren reeds bestaande meldplichten met betrekking tot ICT-inbreuken bij die toezichthouders.

Artikel 6
Met de term computercrisisteam (eerste lid, onder b) wordt een CERT bedoeld. Het woord is ontleend aan artikel 7 van de concept-NIB-richtlijn. Informatieverstrekking kan alleen plaatsvinden aan die (buitenlandse of Nederlandse) CERT's die bij ministeriële regeling, na toetsing of gegevensuitwisseling daarmee gerechtvaardigd en verantwoord is, daartoe zijn aangewezen. **De ministeriële regeling waarbij buitenlandse CERT's worden aangewezen resp. de AMvB die nadere regels kan stellen, zullen een garantie van geheimhouding als voorwaarde voor gegevensverstrekking stellen. Tevens zullen er in de ministeriële regeling uitsluitend buitenlandse en Nederlandse CERT's worden opgenomen die in eigen land een met artikel 4 lid 2 (verwijzing naar de Wob) van dit besluit vergelijkbare regeling hebben getroffen.**

Vewin
Bezuidenhoutseweg 12
2594 AV Den Haag
T (070) 3490 850
info@vewin.nl
www.vewin.nl
Postbus 90611 • 2509 LP Den Haag

0 BD

VNO NCW

MKB Nederland

Zijne Excellentie
Minister mr. I.W. Opstelten
Ministerie van Veiligheid en Justitie
Turfmarkt 147
2511 DP DEN HAAG

Briefnummer
13/11.327/Ma/Ven

Onderwerp
Consultatie melding inbreuken elektronische informatiesystemen

Den Haag
16 september 2013

Telefoonnummer

Excellentie,

Graag willen VNO-NCW en MKB-Nederland gebruik maken van de geboden mogelijkheid om te reageren op de consultatie over het concept wetsvoorstel melding inbreuken elektronische informatiesystemen. Het wetsvoorstel geeft aanleiding tot een aantal serieuze zorgen, die wij in deze brief nader zullen toelichten.

Algemeen

ICT is van fundamenteel belang voor onze economie en maatschappij. In steeds grotere mate is onze samenleving afhankelijk geworden van ICT. Vrijwel alle processen worden beheerd door complexe ICT-systemen. Als deze uitvallen kan dit leiden tot grote economische schade of zelfs maatschappelijke ontwrichting. Nederland is de afgelopen jaren opgeschrikt door een aantal kleinere en grotere security breaches bij bedrijven en overheden. Teneinde een zo goed mogelijke verdediging tegen deze breaches op te kunnen bouwen en in stand te houden is het van groot belang dat kennis over deze breaches wordt gedeeld.

VNO-NCW en MKB-Nederland zijn in dit verband voorstander van een systeem van *just culture*: een dusdanige cultuur die aanmoedigt om cyberincidenten vrijwillig te melden, met als enig doel het verbeteren van de veiligheid van het gehele systeem. Een dergelijke cultuur, die bestaat in de luchtvaart, gaat uit van vertrouwen en wederzijdse afhankelijkheid. Een wettelijke meldplicht, zoals die nu wordt geïntroduceerd in het wetsvoorstel, staat hiermee feitelijk op gespannen voet en kan zelfs averechts werken op de opbouw van de *just culture*, zoals die zich nu binnen het NCSC en de daar binnen ingerichte sectorale overlegstructuren ontwikkelt.

Malietoren / Bezuidenhoutseweg 12 / Postbus 93002 / 2509 AA Den Haag
www.vno-ncw.nl / 070-349 03 49 / www.mkb.nl / 015-219 12 12

Informeel wordt hier tussen bedrijven onderling en met de overheid veel kennis gedeeld om risico's en breaches beter te kunnen inschatten en daarnaar te handelen.

VNO-NCW en MKB-Nederland roepen u dan ook op om de introductie van deze wettelijke meldplicht te heroverwegen.

Onbepaaldheid meldplicht

Als er toch wordt gekozen voor de invoering van een wettelijke meldplicht voor security breaches, is het van groot belang deze goed in te kaderen. Hoewel de intentie van het wetsvoorstel lijkt te zijn de meldplicht te beperken tot incidenten met een grote impact, roepen de gekozen formuleringen in het wetsvoorstel vragen op.
VNO-NCW en MKB-Nederland vinden het wetsvoorstel onvoldoende concreet over de invulling van de meldplicht, zowel wat betreft de vraag voor welke aanbieders en welke producten en diensten de meldplicht zal gelden als wat betreft de inhoud en omvang van de melding en de in verband daarmee aan te leveren gegevens. Dit maakt het zeer moeilijk in te schatten wat de meldplicht precies gaat betekenen, in termen van administratieve lasten en risico's.
Vooral de inzet om alle incidenten onder de meldplicht te brengen die potentieel maatschappij- ontwrichtend zijn, en er na de inbreuk onverwijld dient te worden gemeld, is in dit verband zorgelijk. De facto komen hierdoor vrijwel alle breaches onder de werkingssfeer van de meldplicht. Dit roept tevens vragen op over de capaciteit van het NCSC om bij een dergelijke grote stroom aan meldingen daadwerkelijk hulp te bieden.

Vertrouwelijkheid informatie

Als gevolg van deze meldplicht lopen aanbieders in potentie het risico dat zij het NCSC zeer vergaand moeten informeren over incidenten. Dat betekent dat het NCSC zal kunnen beschikken over bedrijfsvertrouwelijke en anderszins gevoelige informatie. Het is cruciaal dat vertrouwelijke omgang met deze informatie is gewaarborgd, niet in de laatste plaats omdat onzorgvuldige omgang met deze informatie juist zou kunnen leiden tot maatschappelijke ontwrichting of de veiligheid van de Staat in gevaar zou kunnen brengen.
Artikel 6 biedt de gevraagde garanties niet om een aantal redenen:
a. informatie aan het publiek wordt slechts verstrekt als de veiligheid van de Staat daarmee niet wordt geschaad. Bedrijven zijn van oordeel dat eenzelfde voorwaarde dient te gelden als de minister weet of kan weten dat een of meer bedrijven worden geschaad;

b. de zinsnede 'onverminderd andere wetten' betekent dat onder meer de Wet openbaarheid van bestuur van toepassing is. Dat is slechts aanvaardbaar als in het onderhavige wetsvoorstel wordt opgenomen dat alle in het licht van dit wetsvoorstel verstrekte informatie niet kan worden opgevraagd op basis van de Wet openbaarheid van bestuur;
c. wij kunnen ons wel voorstellen dat bepaalde informatie in het algemeen belang wordt gedeeld met andere aanbieders of aangewezen computercrisisteams. De beslissing hiertoe dient ons inziens echter primair te liggen bij het bedrijf dat de informatie heeft aangeleverd, dan wel bij de sectorale toezichthouder. Mocht dit anders worden beoordeeld, dan willen wij wel de verzekering dat de bedrijven die het aangaat voor de verstrekking van die gegevens daarvan op de hoogte worden gesteld en een redelijke termijn krijgen om zich daarover uit te spreken en zich daartegen bij de rechter te verzetten. Daarnaast dient de ministeriële regeling waarbij buitenlandse *certs* worden aangewezen een garantie van geheimhouding als voorwaarde voor gegevensverstrekking te bevatten.

Administratieve lasten en dubbele meldplichten
Ingevolge het wetsvoorstel moeten bedrijven rechtstreeks (en niet via de sectorale toezichthouder) melding doen bij het NCSC. Veel sectoren waarop de onderhavige meldplicht van toepassing gaat worden kennen echter al een meldplicht bij de sectorale toezichthouder die in veel gevallen hetzelfde beoogt als in dit wetsvoorstel is opgenomen. De telecomsector spant in dit verband de kroon met drie (deels al geldende) meldplichten. VNO-NCW en MKB-Nederland vrezen voor (drie-)dubbele meldplichten en een grote stijging van de administratieve lasten. Wij doen een beroep op u om een getrapte melding mogelijk te maken via de sectorale toezichthouder, zodat de lasten voor de bedrijven worden beperkt.
Daarenboven wijzen wij op het feit dat de Europese Commissie begin dit jaar een voorstel heeft gedaan voor een richtlijn voor Netwerk- en Informatiebeveiliging, waarin een meldplicht voor security breaches voor vitale sectoren is opgenomen. Voor de vaak internationaal opererende bedrijven is een level playing field van groot belang en het is niet wenselijk dat in Nederland zwaardere eisen gaan gelden op dit punt. Daar komt bij dat internationale bedrijven vaak werken met wereldwijde systemen, hetgeen kan leiden tot een grote hoeveelheid meldingen en een grote administratieve en operationele last tijdens een ernstig incident. Het verdient naar onze mening dan ook aanbeveling te wachten met invoering van deze wet en aan te sluiten bij de aanstaande Europese meldplicht.

Overige opmerkingen

- In artikel 2 van het wetsvoorstel wordt gesproken over ernstige maatschappelijke gevolgen, terwijl het in artikel 6 gaat over schadelijke maatschappelijke gevolgen. VNO-NCW en MKB-Nederland pleiten ervoor de terminologie op elkaar aan te sluiten en in beide gevallen te spreken over ernstige maatschappelijke gevolgen.

- Artikel 3 stelt dat aanbieders onverwijld na ontdekking van de inbreuk dienen te melden. Dit zal vaak niet mogelijk zijn. De aanbieder heeft tijd nodig om zelf te analyseren of er sprake is van een incident met mogelijk maatschappelijke ontwrichting tot gevolg. Door de gebruikte formulering worden te veel incidenten onder de scope van het wetsvoorstel gebracht.

- Artikel 4 ziet op het verstrekken van additionele informatie na de melding, waarna het NCSC een risico inschatting gaat maken. Dit artikel dient terughoudend te worden toegepast. Bedrijven en sectoren zijn vaak zelf goed in staat om problemen op te lossen. Indien dit niet het geval is, zullen zij zelf met de vraag om hulp komen. Met het aanleveren van de gevraagde informatie kan bovendien kostbare tijd verloren gaan tijdens het oplossen van een incident.
Ook het verlenen van hulp dient naar de mening van VNO-NCW in nauw overleg met het getroffen bedrijf en/of de sector te gebeuren. Voorkomen moet worden dat het NCSC 'de regie overneemt' en op de stoel van de bedrijven gaat zitten.

- Volgens de memorie van toelichting behelst de rol van het NCSC het geven van adviezen en het bieden van handelingsperspectief. VNO-NCW en MKB-Nederland pleiten ervoor uitdrukkelijk in de Memorie van Toelichting op te nemen dat het NCSC, zonder tussenkomst van het bevoegde gezag, geen interventiebevoegdheden heeft.

- Zoals hierboven aangegeven zijn VNO-NCW en MKB-Nederland voorstander van de ontwikkeling van een *just culture*, waarin op basis van vrijwilligheid incidenten worden gedeeld met het doel het gehele systeem te versterken. Het verdient aanbeveling om deze wettelijke meldplicht tijdelijk in te stellen, totdat de *just culture* zich heeft kunnen manifesteren. Een evaluatie van het wetsvoorstel op effectiviteit en noodzakelijkheid zou maximaal anderhalf jaar na invoering dienen plaats te vinden.

- Beursgenoteerde bedrijven in de VS zijn verplicht ieder kwartaal aan de Securities and Exchange Commission (SEC) te melden of er ernstige incidenten zijn geweest. Het is van belang dat de meldingen aan het NCSC en de SEC op één lijn staan, mede omdat de Wet Openbaarheid Bestuur kan leiden tot publicatie van de incidenten of dat het NCSC deze zelf bekend maakt.

VNO NCW

MKB Nederland

- VNO-NCW en MKB-Nederland gaan ervan uit dat de AMvB('s) in nauwe samenwerking met de diverse sectoren worden opgesteld. Van belang is dat in de AMvB('s) een heldere beschrijving worden opgenomen wanneer een incident in een bepaalde sector onder de meldplicht valt.

- De inschatting in de MvT van de administratieve lasten (57 euro per melding) wordt als absoluut onrealistisch ervaren.

Wij hopen met deze reactie een constructieve bijdrage te hebben geleverd en dringen erop aan bovengenoemde punten mee te nemen bij de verdere gedachtevorming over het wetsvoorstel. VNO-NCW en MKB-Nederland worden graag betrokken bij verdere uitwerking en het opstellen van de AMvB('s).

Hoogachtend,

drs. C. Oudshoorn
Directeur Beleid