concept 16 juli 2013 t.b.v. consultatie

Wet houdende regels over het melden van een inbreuk op de veiligheid of een verlies van integriteit van elektronische informatiesystemen die van vitaal belang zijn voor de Nederlandse samenleving (Wet melding inbreuken elektronische informatiesystemen)

MEMORIE VAN TOELICHTING

ALGEMEEN

1. Inleiding

Dit wetsvoorstel introduceert een meldplicht voor een inbreuk op de veiligheid of een verlies van integriteit van elektronische informatiesystemen (hierna ook: ICT-inbreuken). 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 heeft of kan hebben dat de beschikbaarheid of betrouwbaarheid in belangrijke mate wordt onderbroken. De meldplicht geldt alleen voor bij algemene maatregel van bestuur aan te wijzen aanbieders van daarbij aan te wijzen producten of diensten. De melding moet worden gedaan aan de Minister van Veiligheid en Justitie. De melding wordt behandeld door het Nationaal Cyber Security Centrum (NCSC), een onderdeel van het ministerie. De melding stelt het NCSC in staat om hulp te verlenen aan de getroffen aanbieder en om andere vitale aanbieders te waarschuwen, met als uiteindelijke doel om het risico van maatschappelijke ontwrichting in te schatten en die ontwrichting te voorkomen of in elk geval zo veel mogelijk te beperken.

Met dit wetsvoorstel wordt gevolg gegeven aan het verzoek van de Tweede Kamer om te komen tot de wettelijke vastlegging van een meldplicht bij het NCSC voor organisaties die betrokken zijn bij voor de samenleving vitale informatiesystemen ('security breach notification') (motie-Hennis-Plasschaert, Kamerstukken II 2011/12, 26 643, nr. 202). Aanleiding voor dat verzoek waren de gebeurtenissen bij het bedrijf DigiNotar in het najaar van 2011. Deze ICT-inbreuk heeft het toegenomen belang en de onderlinge verwevenheid van ICT-systemen bij de overheid en (overige) vitale sectoren nadrukkelijk zichtbaar gemaakt.

Dit wetsvoorstel is aangekondigd in een brief aan de Tweede Kamer van 6 juli 2012 (Kamerstukken II 2012/13, 26 643, nr. 247). Zoals in die brief is beschreven, zijn bij de invulling van de meldplicht de volgende uitgangspunten gehanteerd: aansluiten bij bestaande wet- en regelgeving, aansluiten bij Europese initiatieven, publiek-private samenwerking, te bieden hulp ter voorkoming van maatschappelijke ontwrichting staat centraal, en eigen verantwoordelijkheid van vitale organisaties. Voorts beoogt de meldplicht bij te dragen aan het creëren van een veiligheidscultuur, de zogeheten 'just culture', waarin het leren van incidenten vooropstaat.

Dit wetsvoorstel sluit ook aan bij de ambitie van de Europese Commissie om EU-breed te komen tot een meldplicht voor overheden en vitale marktpartijen die bijdraagt aan het verhogen van de digitale veiligheid.

2. Inhoud en betekenis

Meldplicht

Doel van de in dit wetsvoorstel vervatte meldplicht voor aanbieders van voor de Nederlandse samenleving vitale producten en diensten aan het NCSC is tweeledig. Een melding van een ernstige ICT-inbreuk vanuit de vitale sectoren aan het NCSC is enerzijds bedoeld om tijdig te kunnen inschatten hoe groot de impact en daarmee de potentiële maatschappelijke ontwrichting is. Anderzijds stelt de melding het NCSC in staat om hulp aan de getroffen organisatie te verlenen en om te anticiperen op de mogelijk bredere effecten van een dergelijke inbreuk, door andere vitale organisaties te waarschuwen en te adviseren. De hulp door het NCSC aan de getroffen organisatie behelst het bieden van handelingsperspectief door het geven van advies en informatie en het coördineren van de inzet van andere (overheids)organisaties of daar waar noodzakelijk het bieden van technische ondersteuning om de gevolgen van een inbreuk te beperken.

Belangrijk bij de in dit wetsvoorstel vervatte meldplicht is ook dat deze een cultuur tracht te realiseren waarin het gezamenlijk bijdragen aan veiligheid centraal staat. In de luchtvaartsector

bestaat bijvoorbeeld ruime ervaring met deze praktijk onder de noemer van het werken aan een 'just culture'.

Bij het doen van de meldingen is van belang dat deze in vertrouwen gedaan worden om kwetsbaarheden te beperken dan wel in de toekomst te vermijden. De meldplicht past daarbij in het bredere kader van de ingezette publiek-private samenwerking met betrekking tot het realiseren van cybersecurity binnen de overheid en de vitale sectoren. Om het NCSC een ondersteunende rol te laten vervullen bij het voorkomen en beperken van onderbrekingen van de beschikbaarheid en betrouwbaarheid van voor de samenleving vitale diensten en producten én te zorgen voor een veiligheidscultuur waarbij meldingen gedaan worden om daar lering uit te trekken, is het van belang om de drempel om meldingen te doen zo laag mogelijk te maken. In verband hiermee is de voorgestelde meldplicht niet voorzien van de mogelijkheid van sanctionering en is de meldplicht primair gericht op het bieden van hulp. Het NCSC kan daarbij functioneren als informatieknooppunt, ofwel de spin in het web, om partijen te informeren en te adviseren over de te ondernemen acties. Het NCSC kan daarbij putten uit een omvangrijk nationaal en internationaal netwerk van o.a. publieke en private Computer Emergency Response Teams waarbinnen veel kennis beschikbaar is over de wijze van omgaan met en het leveren van response bij ICT-inbreuken.

Taak van het Nationaal Cyber Security Centrum

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 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.

Het NCSC vervult van oudsher voor de (rijks)overheid de functie van Computer Emergency Response Team (CERT). Een CERT is een team van ICT-experts dat snel en adequaat kan reageren op een beveiligingsincident met computers of netwerken met als doel om schade te beperken en snel herstel van de dienstverlening te bevorderen. Als CERT geeft het NCSC gevraagd en ongevraagd advies over informatiebeveiliging en wisselt het kennis uit met andere CERT's in en buiten Nederland.

Daarnaast fungeert het NCSC als informatieknooppunt voor ICT-inbreuken binnen de overheid en de vitale sectoren. Voortvloeiend uit deze taak heeft het NCSC een rol in het op basis van expertise adviseren en ondersteunen van door inbreuken getroffen partijen binnen de (rijks)overheid en de vitale sectoren. Daarbij staat het beperken of voorkomen van maatschappelijke ontwrichting voorop. Vanuit zijn (inter)nationale kennis- en netwerkfunctie kan het NCSC voor partijen binnen de doelgroep kennis ontsluiten en deze aanbieden om inbreuken op de juiste wijze van een gepast antwoord te voorzien.

Hierbij levert het NCSC handelingsperspectief om de inbreuk, met inachtneming van de eigen verantwoordelijkheid van de betrokken organisaties voor hun informatiebeveiliging, op te lossen. Tevens kan het NCSC, vanuit zijn rol als platform voor samenwerking tussen publieke en private partijen, op eenvoudige wijze kennis en kunde beschikbaar maken en daarmee bijdragen aan een adequate reactie op ICT-inbreuken.

Melding

Met het oog op de bovenstaande taken van het NCSC is het van belang dat de melding aan het NCSC bestaat uit voldoende informatie om daadwerkelijk invulling te geven aan deze taken en een inschatting te kunnen maken van de risico's van een inbreuk en de in verband daarmee benodigde maatregelen. Daarbij is het van belang dat de melding, hoewel deze qua aard per vitale sector verschilt, in elk geval bestaat uit een aantal elementen. Ten eerste dient de melding inzicht te geven in de aard en omvang van de ICT-inbreuk. Op basis van deze informatie kan onder meer gericht in het nationale en internationale netwerk gezocht worden naar relevante informatie en kennis die voor de getroffen partij van belang is. Een specificatie van het soort getroffen systemen is in dit verband bijvoorbeeld van belang. Ten tweede dient bij de melding aangegeven te worden wat het tijdstip van aanvang van de betrokken ICT-inbreuk is. Ten derde dient de melding in te

gaan op de reeds getroffen maatregelen, zodat mede op basis daarvan geadviseerd kan worden over de eventuele nog te treffen aanvullende maatregelen. Ook is het van belang dat de melding ingaat op de te verwachten hersteltijd, én dat de melding contactgegevens van de betrokken partij bevat, zodat desgewenst in nader contact kan worden getreden in het kader van de hulpverlening.

Meldplichtige partijen

Dit wetsvoorstel bevat een meldplicht voor aanbieders van vitale producten of diensten binnen diverse sectoren. Het betreft hierbij de sectoren: elektriciteit, gas, drinkwater, telecom, keren en beheren oppervlaktewater, financiën, overheid en transport (mainports Rotterdam en Schiphol). Te denken valt daarbij aan aanbieders zoals energienetwerkbeheerders, drinkwaterbedrijven, telecombedrijven, beheerders van hoofdwaterkeringen, banken, het Havenbedrijf Rotterdam, de NV Luchthaven Schiphol en Luchtverkeersleiding Nederland. Het gaat daarbij dus om onderdelen van de vitale infrastructuur waarbij een inbreuk direct of indirect (cascade-effect) tot maatschappelijke ontwrichting kan leiden. De aanbieders en hun concrete producten en diensten waarvoor de meldplicht gaat gelden, zullen worden aangewezen bij algemene maatregel van bestuur.

Voor certificaatdienstverleners, waartoe in het verleden bijvoorbeeld Diginotar behoorde, geldt dat de melding van ICT-inbreuken langs andere weg vorm wordt gegeven. Daarvoor is met name gekozen vanwege de onzekerheid over het moment van inwerkingintreding en de uiteindelijke inhoud en reikwijdte van het voorstel voor een verordening van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt (voorstel van 4 juni 2012, COM(2012) 238 final). De conceptverordening bevat onder meer een - rechtstreeks werkende - plicht tot melding van inbreuken op de veiligheid van elektronische vertrouwensdiensten (artikel 15, tweede lid). Met het oog daarop wordt vooruitlopend op de verordening volstaan met de introductie van een meldplicht voor gekwalificeerde certificaten door middel van een aanpassing van het Besluit elektronische handtekeningen. Hierdoor komt nadrukkelijk te gelden dat veiligheidsinbreuken in de systemen van dienstverleners van gekwalificeerde certificaten gemeld moeten worden bij zowel de toezichthouder als het NCSC. Naast gekwalificeerde certificaten worden ook ongekwalificeerde certificaten uitgegeven. Zoals eerder door de Minister van Binnenlandse Zaken en Koninkrijksrelaties is aangegeven betreft dit een internationaal stelsel, waarbij de Nederlandse inbreng in Europees verband erop gericht is het stelsel waar mogelijk te verbeteren. De Ministers van Economische Zaken, Binnenlandse Zaken en Koninkrijksrelaties en Veiligheid en Justitie staan in nauw contact met certificaatdienstverleners om aanvullende afspraken te maken over het melden van inbreuken op deze ongekwalificeerde certificaten.

Te melden ICT-inbreuken

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. Het wetsvoorstel ziet niet op verstoringen waarbij geen sprake is van een dergelijke ICT-inbreuk, zoals DDoS-aanvallen (Distributed Denial of Service). Bij een DDoS-aanval wordt de bereikbaarheid van een online-dienst aangetast zonder aantasting van de systemen die in dat verband worden gebruikt. Veelal zal het bij deze 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. Een en ander laat overigens onverlet dat partijen de mogelijkheid hebben om ernstige verstoringen van de bereikbaarheid op basis van vrijwilligheid aan het NCSC te melden.

De aan te wijzen organisaties in de vitale sectoren zijn niet verplicht om elke ICT-inbreuk aan het NCSC te melden. De verplichting tot melden geldt alleen als de inbreuk tot gevolg heeft of kan hebben dat de beschikbaarheid of betrouwbaarheid van het aangewezen product of de aangewezen dienst in belangrijke mate wordt of kan worden onderbroken. Mede op basis van overleg met de betrokken sectoren en departementen zal nader worden uitgewerkt wat voor de verschillende betrokken producten en diensten moet worden verstaan onder "in belangrijke mate". Daarbij zal mede bepalend zijn onder welke omstandigheden sprake is of kan zijn van maatschappelijke ontwrichting.

Vertrouwelijkheid

Om de getroffen aanbieder te kunnen helpen en de schadelijke gevolgen van de ICT-inbreuk te helpen voorkomen of beperken, zal het NCSC vaak moeten beschikken over bedrijfsvertrouwelijke gegevens die niet in verkeerde handen mogen vallen. Technische gegevens over de inrichting van elektronische informatiesystemen kunnen bijvoorbeeld misbruikt worden door degenen die de systemen willen aanvallen. Van belang is dat organisaties waarvoor de meldplicht gaat gelden, niet terughoudend zijn met het verschaffen van informatie. Met het oog hierop dient de vertrouwelijke omgang met informatie goed te worden geregeld. Daartoe regelt het voorgestelde artikel 6 met welk doel en aan wie informatie en advies mag worden verstrekt die gebaseerd is op de aan het NCSC op grond van de in dit wetsvoorstel vervatte meldplicht verstrekte gegevens. Zie verder de artikelsgewijze toelichting. De met betrekking tot de melding verstrekte informatie betreft in het algemeen bedrijfs- en fabricagegegevens als bedoeld in artikel 10, eerste lid, onder c, van de Wet openbaarheid van bestuur.

Verhouding tot sectorale meldplichten

Voor enkele sectoren geldt thans voor ICT-inbreuken al een verplichting tot melding aan de sectorale toezichthouder. Een voorbeeld hiervan is de plicht voor aanbieders van openbare elektronische communicatienetwerken en -diensten om een inbreuk op de veiligheid en een verlies van integriteit te melden aan de Minister van Economische Zaken bij het Agentschap Telecom op grond van artikel 11a.2 van de Telecommunicatiewet, als door die inbreuk of dat verlies de continuïteit van het netwerk of de dienst in belangrijke mate werd onderbroken. Zie voor een overzicht van overige sectorale meldplichten de bijlage bij bovengenoemde brief aan de Tweede Kamer van 6 juli 2012. Zoals gegeven het karakter van de meldplicht aan het NCSC al is aangegeven, verschilt de aard en strekking van dergelijke meldplichten aan de toezichthouder van de in dit wetsvoorstel opgenomen verplichting tot melden bij het NCSC. Ook als een aanbieder van een vitaal product of vitale dienst een ICT-inbreuk op basis van andere wetgeving reeds moet melden bij een ander overheidsorgaan, is het cruciaal dat het bedrijf de inbreuk óók onverwijld en rechtstreeks aan het NCSC meldt, om vertraging in het daar waar nodig bieden van hulp zo veel mogelijk te beperken en om het delen van informatie over de kwetsbaarheid met andere mogelijk getroffenen te bespoedigen. Een toename van de administratieve lasten voor genoemde aanbieders, die zowel op basis van huidige wetgeving als op grond van dit wetsvoorstel tot melding verplicht zullen zijn, zal zo veel mogelijk worden voorkomen door de wijze waarop moet worden gemeld en de gegevens die dienen te worden verstrekt voor de te onderscheiden meldplichten waar mogelijk op elkaar af te stemmen en processen efficiënt in te richten. De voorgestelde meldplicht sluit aan op het bestaande stelsel van sectorale meldplichten en treedt niet in de thans geldende sectorale bevoegdheden. Daarmee laat de voorgestelde meldplicht ook de bestaande crisisbeheersingsstructuren onverlet.

Verhouding tot wetsvoorstel meldplicht datalekken

Bij het parlement is een wetsvoorstel aanhangig tot wijziging van de Wet bescherming persoonsgegevens (Wbp) en de Telecommunicatiewet in verband met de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens (gebruik meldplicht datalekken, Kamerstukken II 2012/13, 33 662). De in dat wetsvoorstel bedoelde melding moet worden gedaan aan het College bescherming persoonsgegevens (Cbp). Die melding ziet op inbreuken op de in de Wbp voorgeschreven beveiliging van persoonsgegevens tegen verlies en onrechtmatige verwerking. Een sterk vergelijkbare meldplicht voor inbreuken op de beveiliging van persoonsgegevens is reeds opgenomen in artikel 11.3a van de Telecommunicatiewet. Bij een inbreuk op de veiligheid of een verlies van integriteit waarop het onderhavige wetsvoorstel ziet, is er weliswaar sprake van een inbreuk op de beveiliging van een informatiesysteem van een organisatie, maar daarbij hoeven niet noodzakelijkerwijs ook persoonsgegevens in het geding te zijn. Daarbij valt te denken aan geautomatiseerde procescontrolesystemen ten behoeve van het aansturen van fysieke processen. Niettemin kan het zich voordoen dat een ICT-inbreuk onder beide meldplichten valt. In dat geval moet de inbreuk derhalve zowel bij het NCSC als bij het Cbp worden gemeld. Ook hiervoor geldt 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.

Verhouding tot EU-richtlijnen

Een van de belangrijkste recente internationale ontwikkelingen op het terrein van cybersecurity is de in februari gepubliceerde Europese Cyber Security Strategie (JOIN(2013) 1 final, Kamerstukken II 2012/13, 22 112, nr. 1588) alsmede het (ook in deze strategie genoemde) ontwerp van een Netwerk- en Informatiebeveiligingsrichtlijn (hierna te noemen: NIB-richtlijn, COM(2013) 48, Kamerstukken II 2012/13, 22 112, nr. 1588, en Kamerstukken II 2012/13, 33 602, nr. 1). De Europese onderhandelingen over het ontwerp van deze NIB-richtlijn zijn inmiddels begonnen. De ontwerp-richtlijn zet in op het toegenomen belang van samenwerking binnen de Europese Unie op het terrein van informatiebeveiliging en ziet op het opbouwen van nationale capaciteiten, de coördinatie bij grensoverschrijdende inbreuken, en publiek-private samenwerking.

Zoals in het algemeen overleg over het behandelvoorbehoud met betrekking tot deze ontwerprichtlijn op 24 april 2013 reeds aan de Tweede Kamer is aangegeven (Kamerstukken II 2012/13, 22 112, nr. 1629, blz. 5), is het van belang dat de uiteindelijke NIB-richtlijn goed aansluit op het te zijner tijd in Nederland functionerende stelsel. De ontwerprichtlijn doet dat nu nog onvoldoende, zoals wat betreft het begrip 'incident', de bevoegdheden van de 'bevoegde autoriteit' en de lijst met 'marktdeelnemers' (vitale aanbieders). Ik zal het parlement twee keer per jaar schriftelijk informeren over de voortgang in de EU-Telecomraad, waarin de onderhandelingen over de NIB-richtlijn plaatsvinden (Kamerstukken II 2012/13, 22 112, nr. 1629, blz. 6, en Kamerstukken I 2012/13, 33 602, nr. A, blz. 15). Daarbij zal in het bijzonder worden ingegaan op de ontwikkelingen van de Europese beraadslagingen, de positie van Nederland en eventuele wijzigingen van standpunten zoals reeds vastgelegd in het BNC-fiche.
Ik verwacht dat de NIB-richtlijn op zijn vroegst in 2015 zal worden vastgesteld, waarna anderhalf jaar beschikbaar zal zijn voor de implementatie.

Naleving

Zoals gezegd is de in dit wetsvoorstel vervatte meldplicht niet voorzien van de mogelijkheid van sanctionering. Het NCSC gaat geen toezicht houden op de naleving van de meldplicht en krijgt ook geen handhavingsbevoegdheden. De voorgestelde meldplicht voor ICT-inbreuken sluit aan bij de huidige praktijk van vrijwillige gegevensuitwisseling in het kader van publiek-private samenwerking. In die praktijk worden thans op vertrouwelijke basis gegevens aan het NCSC verstrekt, zonder dat het NCSC beschikt over formele bevoegdheden tot toezicht en handhaving. Met name ook vanwege de rol als CERT is het NCSC verantwoordelijk voor de waarschuwing, advisering en (tweedelijns)ondersteuning van getroffen organisaties binnen de (rijks)overheid en de vitale sectoren bij ICT-inbreuken, met als oogmerk om maatschappelijke ontwrichting door uitval of verlies van de beschikbaarheid of betrouwbaarheid van voor de samenleving vitale diensten of producten zo veel mogelijk te beperken en voorkomen. Die rol verdraagt zich slecht met de functie van toezichthouder en handhaver. Mede vanwege de aansluiting bij de bestaande publiek-private samenwerking wordt verwacht dat de voorgestelde meldplicht goed wordt nageleefd. De doelgroep is beperkt tot de rijksoverheid en de vitale aanbieders in de randvoorwaardelijke sectoren. Het nut en de noodzaak van het delen van vertrouwelijke gegevens met betrekking tot ICT-inbreuken die ernstige gevolgen hebben of kunnen krijgen, wordt hier breed gedragen. Voornoemde partijen zijn zich bewust van hun verantwoordelijkheid. Met de voorgestelde inrichting van de meldplicht die in samenwerking met de betrokken aanbieders nader gestalte wordt gegeven, worden gunstige voorwaarden geschapen voor spontane naleving. Tegenover de bescheiden kosten van melding voor de betrokken organisaties staan hoge baten in de vorm van schadebeperking en probleemoplossing. Gegevens die ter uitvoering van de meldplicht worden verstrekt, worden vertrouwelijk behandeld, zodat voor schade aan reputatie of concurrentiepositie niet gevreesd hoeft te worden.
Als blijkt dat de meldplicht in een concreet geval opzettelijk niet is nageleefd, kan het NCSC de instanties die belast zijn met het toezicht op de naleving door de betrokken aanbieder van de op hem van toepassing zijnde sectorale wetgeving hierover desgevraagd informeren. In zo'n geval verstrekt het NCSC nadrukkelijk geen gegevens die het uit hoofde van de meldplicht heeft ontvangen. Aan de hand van een dergelijk signaal kan de sectorale toezichthouder beoordelen of niet-naleving van de meldplicht voor hem aanleiding vormt om het sectorale toezicht aan te scherpen.
Mocht blijken dat de meldplicht onvoldoende wordt nageleefd, dan kan alsnog worden besloten tot het inrichten van een stelsel van toezicht en handhaving.

Interventiemogelijkheden

In bovengenoemde brief aan de Tweede Kamer van 6 juli 2012 is, naast de security breach notification, ook ingegaan op het belang van een adequaat stelsel van interventiemogelijkheden. Dit wetsvoorstel regelt, mede met het oog op bovengenoemde motie Hennis-Plasschaert, alleen de meldplicht bij het NCSC van inbreuken op informatiesystemen voor aanbieders van voor de samenleving vitale producten of diensten. Mede gelet op de omstandigheid dat er voor het NCSC geen toezichthoudende rol is weggelegd is ervoor gekozen dit wetsvoorstel niet tevens aanpassingen van de huidige wetgeving op het punt van interventiebevoegdheden voor de sectorale toezichthouders of de betrokken vakministeries te laten behelzen. Wijzigingen van of aanvullingen op de in de huidige regelgeving al opgenomen interventiebevoegdheden zullen, zoals aangegeven in de eerdergenoemde brief d.d. 6 juli, waar nodig een plaats krijgen in ontwerp-wetgeving van de voor de betrokken sectoren verantwoordelijke ministers. Daarbij vervult de Minister van Veiligheid en Justitie een coördinerende rol.

3. Totstandkoming van dit wetsvoorstel

Consultatie
PM

4. Administratieve lasten

De in dit wetsvoorstel geregelde meldplicht heeft geen gevolgen voor de administratieve lasten van burgers, maar zal wel leiden tot een bescheiden stijging van de administratieve lasten voor de organisaties die onder het toepassingsbereik vallen. Een definitieve raming kan pas worden gemaakt als vaststaat voor welke aanbieders en voor welke producten en diensten de meldplicht zal gelden (aan te wijzen bij algemene maatregel van bestuur (amvb)), welke gegevens verstrekt moeten worden en op welke wijze dat moet gebeuren (nader te regelen bij of krachtens amvb). In de nota van toelichting bij de amvb (en in de toelichting van de krachtens die amvb eventueel vast te stellen ministeriële regeling) zal hierop nader worden ingegaan. Bovendien ben ik voornemens om samen met de betrokken sectoren en departementen nader uit te werken, zo mogelijk per sector, bijvoorbeeld bij of krachtens algemene maatregel van bestuur of in beleidsregels, welke inbreuken ernstig genoeg zijn om onder de meldplicht te vallen (nadere uitwerking van "in belangrijke mate" in artikel 3, eerste lid). Ook die nadere uitwerking bepaalt voor een deel de omvang van de administratieve lasten.

Intussen mag wellicht een eerste indicatie van de te verwachten administratieve lasten worden ontleend aan de hierboven al besproken meldplicht voor de aanbieder van een openbaar elektronisch communicatienetwerk of een openbare elektronische communicatiedienst (artikel 11a.2 Telecommunicatiewet). De totale administratieve lasten van die meldplicht zijn geraamd op circa € 277 000 per jaar, uitgaande van 10 meldingen per aanbieder per jaar en van 486 aanbieders (Kamerstukken II 2010/11, 32 549, nr. 3, blz. 26). Naar verwachting zal in elk geval het aantal aanbieders waarvoor de in dit wetsvoorstel geregelde meldplicht voor ICT-inbreuken zal gelden, aanzienlijk kleiner zijn (alleen vitale aanbieders).

Zoals gezegd zullen voor elkaar overlappende meldplichten de wijze waarop moet worden gemeld en de gegevens die dienen te worden verstrekt, zo veel mogelijk onderling worden afgestemd.

ARTIKELSGEWIJS

Artikel 1

Aanbieder: De omschrijving is (afgezien van het element 'bouwen') afgeleid van de definitie van 'aanbieden' in artikel 1.1, onder i, van de Telecommunicatiewet. Een aanbieder kan zowel een rechtspersoon als een natuurlijke persoon zijn.

Informatiesysteem: Het zal vaak gaan om systemen die van internet afhankelijk zijn, maar dat is geen vereiste.

Product of dienst: De meldplicht geldt alleen voor de producten en diensten die bij de in artikel 2 bedoelde algemene maatregel van bestuur zijn aangewezen. De termen 'product' en 'dienst' duiden in de wettekst op een *aangewezen* product of dienst.

Artikel 2

Dit artikel regelt de reikwijdte van de wet en geeft een grondslag voor aanwijzing bij algemene maatregel van bestuur van de aanbieders en de producten en diensten waarvoor de in artikel 3 opgenomen meldplicht geldt.
Het moet gaan om voor de Nederlandse samenleving vitale producten of diensten. Een aanbieder kan ook buiten Nederland gevestigd zijn; het gaat erom dat hij producten of diensten aanbiedt die vitaal zijn voor de Nederlandse samenleving.
De voordracht voor de algemene maatregel van bestuur zal worden gedaan in overeenstemming met de andere betrokken bewindspersonen.

Artikel 3

De meldplicht geldt alleen in geval van een daadwerkelijke inbreuk op de veiligheid of een daadwerkelijk verlies van integriteit van een elektronisch informatiesysteem, en dus, zoals in het algemeen deel van deze memorie is toegelicht, niet tevens bij (andere) verstoringen, zoals DDoS-aanvallen.

De meldplicht geldt daarnaast alleen als door de ICT-inbreuk de beschikbaarheid of betrouwbaarheid van het aangewezen product of de aangewezen dienst in belangrijke mate wordt of kan worden onderbroken. Mede op basis van overleg met de betrokken sectoren en departementen zal nader worden uitgewerkt (bijvoorbeeld bij of krachtens de in artikel 5 bedoelde algemene maatregel van bestuur of in beleidsregels) wat voor de verschillende betrokken producten en diensten moet worden verstaan onder "in belangrijke mate". Daarbij zal mede bepalend zijn onder welke omstandigheden sprake is of kan zijn van maatschappelijke ontwrichting. Hierbij gaat het bijvoorbeeld om criteria zoals langdurige uitval van een vitaal proces of vitale dienst waardoor zowel de aanbieder als andere partijen geconfronteerd worden met de gevolgen van de uitval. Tevens valt daarbij te denken aan de ernst van de inbreuk, waardoor deze mogelijk ook voor andere partijen binnen de rijksoverheid en de vitale sectoren schadelijk is.

De meldplicht geldt dus ook als de ICT-inbreuk nog niet daadwerkelijk heeft geleid tot een belangrijke onderbreking van de beschikbaarheid of betrouwbaarheid van een vitaal product of vitale dienst, maar dat gevolg wel zal kunnen hebben. Dit is immers evenzeer informatie die van groot belang is met het oog op het voorkomen van schadelijke maatschappelijke gevolgen. Bovendien kan ook van dergelijke inbreuken veel worden geleerd.

Van belang is het dat de melding van een ICT-inbreuk waarvoor de meldplicht geldt zo onverwijld als mogelijk wordt gedaan, teneinde het NCSC zo snel als mogelijk in de gelegenheid te brengen de risico's voor de beschikbaarheid of betrouwbaarheid van een vitaal product of vitale dienst te kunnen bepalen en hulp te verlenen bij het treffen van maatregelen om de beschikbaarheid of betrouwbaarheid te waarborgen of herstellen. Daarbij dient in aanmerking genomen te worden dat soms enige tijd zal verstrijken tussen de feitelijke inbreuk en de constatering (van de ernst) daarvan door de aanbieder.

De omschrijving van de bij de melding te verstrekken gegevens is zo veel mogelijk identiek aan de omschrijving in artikel 7, tweede lid, van het Besluit continuïteit openbare elektronische communicatienetwerken en -diensten en aan de omschrijving die voor verleners van gekwalificeerde certificaten naar verwachting zal worden opgenomen in artikel 2, eerste lid, van het Besluit elektronische handtekeningen.

Artikel 4

Denkbaar is dat het NCSC naar aanleiding van een melding nadere gegevens nodig heeft om de aard en de ernst van de ICT-inbreuk te kunnen inschatten en de aanbieder adequaat te kunnen helpen, bijvoorbeeld als de aanbieder bij het doen van de melding nog geen volledige zekerheid kan bieden over de gevolgen van de inbreuk of over de te nemen maatregelen. Dit artikel bevat voor dergelijke gevallen een aanvullende informatieplicht, die wordt geactiveerd door een concreet verzoek van het NCSC in reactie op een in artikel 3 bedoelde melding.

Artikel 5

De hier bedoelde nadere regels dienen onder meer om te concretiseren welke gegevens voor de verschillende aangewezen producten en diensten ingevolge de meldplicht verstrekt moeten worden en de wijze waarop de gegevens verstrekt moeten worden. De nadere regels kunnen bijvoorbeeld ook gebruikt worden om te verduidelijken wat voor de verschillende aangewezen producten en diensten bij de toepassing van artikel 3, eerste lid, moet worden verstaan onder "in belangrijke mate".

Artikel 6

De meldplicht heeft primair tot doel om het NCSC in staat te stellen om de risico's van de ICT-inbreuk te kunnen inschatten en de door de inbreuk getroffen aanbieder bij te staan (zie artikel 4). Het achterliggende belang daarvan is het voorkomen of beperken van maatschappelijke ontwrichting in Nederland. De verstrekte gegevens mogen vervolgens ook worden gebruikt als basis voor advies en informatie aan andere aangewezen aanbieders als bedoeld in artikel 2, aan door de minister aangewezen CERT's en aan het publiek. De melding kan bijvoorbeeld aanleiding geven tot het, eveneens met het oog op het beperken of voorkomen van maatschappelijke ontwrichting, waarschuwen van andere partijen binnen de betrokken vitale sector of andere vitale sectoren, door informatie te verstrekken over de herkomst van gerichte aanvallen of over technische kwetsbaarheden in informatiesystemen die op meerdere plaatsen worden gebruikt. Daarbij spreekt het voor zichzelf dat de informatieverstrekking aan andere aanbieders vanuit bovenbedoeld oogpunt niet verder gaat dan strikt noodzakelijk is om die aanbieders in staat te stellen om te bepalen of zij wellicht met een zelfde soort inbreuk of de mogelijkheid daarvan te maken hebben en om de maatregelen te nemen die in geval van een (mogelijke) inbreuk benodigd zijn om de beschikbaarheid of betrouwbaarheid van hun voor de samenleving vitale producten of diensten te waarborgen.

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.

Tenzij de staatsveiligheid in het geding is, mogen de verstrekte gegevens ook worden gebruikt als basis voor publieksvoorlichting. Daarbij zal het veelal niet nodig zijn om gegevens te verstrekken die herleid kunnen worden tot afzonderlijke aanbieders of afzonderlijke producten en diensten, bijvoorbeeld als het publiek moet worden gewaarschuwd voor de risico's van een door internetcriminelen gehanteerde werkwijze. Maar soms zal de voorlichting alleen effectief kunnen zijn als de aanbieder of het product of de dienst concreet wordt aangeduid, bijvoorbeeld als het nodig is om het publiek te waarschuwen dat een bepaald product of een bepaalde dienst tot nader order beter niet gebruikt kan worden. De beslissing om dergelijke voorlichting te geven, vergt een belangenafweging. Zo zal het belang van het publiek om op de hoogte te zijn niet altijd opwegen tegen het belang van de betrokken aanbieder. Denkbaar is ook dat de bekendmaking de maatschappelijke schade juist vergroot in plaats van voorkomt of beperkt. Het NCSC zal zo mogelijk de betrokken toezichthouder betrekken bij deze belangenafweging.

Het derde lid verbiedt ander gebruik dan nodig is voor de twee in artikel 4 omschreven doelen (risico-inschatting en hulp aan de getroffen aanbieder) dan wel de uitvoering van het eerste lid. De formulering "Onverminderd andere wetten" ziet bijvoorbeeld op artikel 8:28 Algemene wet bestuursrecht (inlichtingen verstrekken aan de bestuursrechter door partijen in een beroepsprocedure), artikel 126nc e.v. Wetboek van Strafvordering (vorderen van gegevens door officier van justitie) en op de Wet op de inlichtingen- en veiligheidsdiensten 2002. Wat de Wet openbaarheid van bestuur betreft zij opgemerkt dat de met betrekking tot de melding verstrekte informatie in het algemeen bedrijfs- en fabricagegegevens betreft als bedoeld in artikel 10, eerste lid, onder c, van die wet.

Het kan wenselijk blijken om nadere regels te stellen over het eerste lid van artikel 6, bijvoorbeeld over de aanwijzing van CERT's op grond van het eerste lid, onder b. In die mogelijkheid voorziet het vierde lid.

Artikel 7

Hoewel het in de bedoeling ligt om deze wet als één geheel in werking te laten treden, is de mogelijkheid van gedifferentieerde inwerkingtreding opengehouden. De bepaling is niet bedoeld om de meldplicht voor afzonderlijke aanbieders, producten of diensten op verschillende tijdstippen in werking te kunnen laten treden. Mocht een dergelijke differentiatie nodig zijn, dan kan zij eventueel worden vormgegeven in de algemene maatregel van bestuur, bedoeld in artikel 2.

De Minister van Veiligheid en Justitie,