Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2011–2012

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 220

BRIEF VAN DE MINISTER VAN VEILIGHEID EN JUSTITIE

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 23 december 2011

Digitale informatie-uitwisseling is essentieel geworden voor het functioneren van de Nederlandse samenleving, zowel voor het economische verkeer als voor het functioneren van de overheid. Inbreuken op de veiligheid van het internet raken ons direct, waarbij het grensoverschrijdende aspect noopt tot een integrale en internationale aanpak. De gebeurtenissen rondom DigiNotar, de recente incidenten zoals weergegeven in de berichtgeving in het kader van Lektober en de ontdekking van het Duqu-virus, onderschrijven de «sense of urgency» die dit kabinet heeft bij een voortvarende uitvoering van de Nationale Cyber Security Strategie (NCSS). Met de NCSS heeft de overheid samen met belangrijke partijen uit het bedrijfsleven en wetenschap de lijnen uitgezet voor de integrale aanpak van cyber security waarbinnen publiek-private, civiel-militaire en internationale samenwerking op innovatieve wijze vorm krijgt. Er zijn snel stappen gezet, maar er zal ook nog uitwerking plaats moeten vinden.

In het AO Nationale Veiligheid van 1 juni 2011 (kamerstuk 28 684, nr. 323) heb ik uw Kamer een dreigingsbeeld cyber security en een juridisch kader cyber security met een inventarisatie van de juridische knelpunten daarbinnen toegezegd. Tevens verzocht uw Kamer meer informatie over de wetgeving in Oostenrijk met betrekking tot cybercrime, met name over de rechtsmacht. In het plenair debat Diginotar van 13 oktober 2011 (Handelingen II, 2011/2012, nr. 12 debat over Diginotar en ICT-problemen bij de overheid) heeft uw Kamer verzocht om nadere informatie over het Nationaal Cyber Security Centrum (NCSC) dat 1 januari 2012 van start zal gaan. Daarnaast heeft uw Kamer in dit debat met de motie Hennis-Plasschaert c.s.[1] de regering verzocht over te gaan tot een wettelijke meldplicht, een zogenaamde «security breach notification».

Doel van deze brief is uw Kamer mede namens de Ministers van Economische Zaken Landbouw en Innovatie, Binnenlandse Zaken en Koninkrijksrelaties, Defensie en Buitenlandse Zaken te informeren over bovenstaande punten. Deze punten zijn de afgelopen maanden binnen de context van de NCSS uitgevoerd.

[1] Zie Kamerstukken 2010/11, 26 643, nr. 202.

kst-26643-220
ISSN 0921 - 7371
's-Gravenhage 2011

U wordt geïnformeerd over:
- Het Cyber Security Beeld Nederland (CSBN); in deze brief treft u de analyse aan van het CSBN, de reactie van de CSR en de kabinetsreactie. Het volledige CSBN en de volledige reactie van de CSR wordt met deze brief meegezonden[1].
- Het Juridisch Kader Cyber Security; in deze brief wordt nader ingegaan op het voor Cyber Security relevante juridisch kader. Een uitvoerige beschrijving van het juridisch kader cyber security treft u aan in het meegezonden document Juridisch Kader Cyber Security.
- De inrichting van het Nationaal Cyber Security Centrum (NCSC); in deze brief treft u de hoofdlijnen aan waarlangs het NCSC zal worden ingericht. In de bijlage bij deze brief treft u de verdere uitwerking van het inrichtingsvoorstel NCSC.

Ten aanzien van implicaties van ontwikkelingen in het cyberdomein voor het buitenlands veiligheids- en defensiebeleid, als ook internationaalrechtelijke aspecten, loopt er momenteel een adviesaanvraag bij de Adviesraad Internationale Vraagstukken en de Commissie van Advies inzake Volkenrechtelijke Vraagstukken. De regeringsreactie op het advies die voor het eerste kwartaal van 2012 is voorzien, zal nader ingaan op de internationale veiligheidsdimensie van cyberdreigingen. Cyberdreigingen hebben immers ook belangrijke buitenlandspolitieke en militaire consequenties. In het AO Nationale Veiligheid van 1 juni 2011 heeft uw Kamer mij verzocht om het artikel in de Wall Street Journal te bekijken over het feit dat de VS elke cyberaanval zien als een oorlogshandeling en aan te geven hoe Nederland hiermee omgaat. Over dit punt zal uw Kamer worden geïnformeerd in de beleidsreactie op het advies van de Adviesraad Internationale Vraagstukken en de Commissie van Advies inzake Volkenrechtelijke Vraagstukken.

Het Cyber Security Beeld Nederland

Het Cyber Security Beeld Nederland (CSBN) is opgesteld door Govcert.nl en bouwt voort op en sluit aan bij de Nationale Risicobeoordeling en het Nationaal Trendrapport Cybercrime en Digitale Veiligheid 2010 dat in november 2010 is gepubliceerd (2010–2011, 28 684, nr. 292). Het CSBN geeft inzicht in de problematiek van cyber security en maakt daarbij onderscheid tussen verschillende vormen van dreigingen op het terrein van cyber security. Voor de ontwikkeling van het CSBN zijn inzichten gebundeld waarover AIVD, MIVD, KLPD, NCTV en Govcert.nl op basis van hun taak beschikken. Deze zijn daarna aangevuld met de kennis die met hen is gedeeld door de private partijen waarmee zij samenwerken. Vervolgens is het CSBN op 10 november 2011 voorgelegd aan de CSR. De CSR heeft op basis van het CSBN het kabinet geadviseerd. De reactie van de CSR is bijgesloten[1].

Het CSBN is gericht op de dreigingen in het ICT-domein voor de Nederlandse situatie, waarbij ontwikkelingen in het buitenland worden meegenomen. De nadruk ligt daarbij op moedwillig handelen. In het CSBN wordt onder andere ingegaan op dreigersgroepen, doelwitten, actuele dreigingen en kwetsbaarheden welke (succesvolle) aanvallen kunnen faciliteren.

Onderzoek naar de omvang van digitale criminaliteit en digitale aanvallen is ook internationaal nog in ontwikkeling. Het is van belang om meer zicht te krijgen op risico's en incidenten in het digitale domein. Deze notie wordt internationaal gedeeld. Hoewel er binnen de vertrouwde publiek-private netwerken dreigingsinformatie wordt gedeeld, zijn de getroffen organisaties en bedrijven in Nederland, maar ook in andere landen, nog terughoudend met het delen van informatie over incidenten. Om een

[1] Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer.

breder en meer kwantitatief beeld van de problematiek te krijgen zal het NCSC meer en op structurele basis aansluiting zoeken bij private partijen. Vanuit de bestaande publiek-private kennis- en informatie-uitwisseling en aangevuld met de in de motie Hennis-Plasschaert c.s. voorgestelde invoering van een meldplicht, de zogenaamde «security breach notification» (2011–2012, 26 643, nr. 202), zal het zicht op de aard en omvang van digitale aanvallen worden vergroot.

Analyse en reactie op het Cyber Security Beeld Nederland

Actoren
Het CSBN schetst een breed scala aan groepen die om uiteenlopende motieven gebruik maken van technieken en kwetsbaarheden om cyberaanvallen in Nederland uit te voeren. De grootste potentiële cyberdreigingen gaan uit van statelijke actoren en van criminelen en in mindere mate van hacktivisten, scriptkiddies en terroristen. Criminelen veroorzaken het merendeel van alle cyberincidenten, waardoor deze het meest tastbaar zijn voor de samenleving. Statelijke actoren kunnen echter de kennis en middelen mobiliseren om de meest geavanceerde en grootschalige aanvallen uit te voeren.

Dreigingen en kwetsbaarheden
Digitale spionage, digitale sabotage en digitale criminaliteit zijn de grootste digitale dreigingen waar Nederland nu mee wordt geconfronteerd. In 2011 is een toename van deze incidenten geconstateerd.

Digitale spionage en sabotage
Het CSBN laat zien dat er sprake is van een toenemende dreiging van digitale spionage. Zowel overheden als private organisaties zijn regelmatig doelwit van digitale spionage geweest, ook in Nederland. Deze cyberaanvallen zijn gericht op het verkrijgen van vertrouwelijke informatie van economische of politieke waarde, of op direct geldelijk gewin.

De toenemende waarschijnlijkheid van digitale sabotage is zorgelijk. Vooralsnog zijn er geen aanwijzingen dat Nederland een gericht doelwit lijkt, echter Nederland is kwetsbaar vanwege de grote afhankelijkheid van ICT-systemen. Een belangrijke ontwikkeling en waarschuwing op dit gebied was de Stuxnet aanval in 2010 en recenter het hieraan gerelateerde Duqu-virus. Stuxnet was de eerste bekende gerichte aanval op industriële controlesystemen (ICS), ook wel aangeduid als SCADA-systemen (Supervisory Control And Data Acquistion). Dergelijke aanvallen vormen een potentieel ernstige bedreiging voor de nationale – en mogelijk ook internationale – veiligheid wanneer zij de vitale infrastructuur (zoals energie, water, financiën) treffen. Bij dergelijke complexe aanvallen is het risico van maatschappelijke ontwrichting reëel.

Digitale criminaliteit
Digitale criminaliteit behelst het merendeel van alle cyberincidenten en is het meest voelbaar voor de samenleving. Duidelijk zichtbaar is dat zowel de overheid, het bedrijfsleven als de individuele burgers een reëel risico lopen om slachtoffer te worden van digitale criminaliteit. De dreiging is het hoogst waar het gaat om bedrijven en burgers. Deze hoge en zich snel ontwikkelende dreiging brengt hoge kosten met zich mee en groeit nog steeds. Digitale criminaliteit is voor de dader zeer aantrekkelijk. Het kan namelijk met een beperkte investering snel winstgevend zijn, terwijl de pakkans laag is. Hightech cybercriminelen lopen voorop in het verbeteren van aanvalsmethoden om hun aanvallen minder zichtbaar en gerichter te maken. Cybercriminelen zijn goed georganiseerd en hebben specialisaties die zij als dienstverlening aanbieden. Zij voeren hun aanvallen uit in tijdelijke samenwerkingsverbanden die zij op internetfora aangaan.

Nieuwe ontwikkelingen
Nieuwe ontwikkelingen die de aandacht vragen zijnde informatiebeveiliging bij het uitbesteden van diensten in «the cloud» en het toenemende gebruik van mobiele apparatuur.
Bij het uitbesteden van diensten in «the cloud» is het moeilijker te overzien of de veiligheid van de data voldoende geborgd is. Daarnaast is het toenemende gebruik van mobiele apparatuur, door de hoge penetratiegraad van deze apparatuur, een groeiend risico. De verwachting is dat serieuze aanvallen gericht op mobiele apparatuur de komende jaren zullen toenemen.

Reactie CSR
De CSR geeft gevraagd en ongevraagd advies aan de regering over relevante ontwikkelingen op het gebied van cyber security. In de CSR hebben publieke, private en wetenschappelijke partijen zitting. In het kader van deze taak heeft de CSR een reactie opgesteld over het CSBN. De CSR herkent zich goed in het CSBN en onderschrijft de daarin genoemde meest relevante dreigingen. Ten aanzien van het CSBN geeft de CSR een tweetal punten die aandacht behoeven voor een verdere versterking van het CSBN. Ten eerste gaat het daarbij om verdere kwalitatieve ontwikkeling van het CSBN. Ten tweede gaat het om een nadere kwantificering van de dreigingen. Samenwerking met de private sector is daarbij nodig om een zo compleet als mogelijk beeld op te bouwen. De CSR heeft aangegeven dat het CSBN in nauwe publiek-private samenwerking tot stand dient te komen en hieraan haar medewerking zal verlenen. Verder geeft de CSR aan het komende jaar de volgende prioriteiten te stellen, namelijk: i) vergroten van het bewustzijn van cyber dreigingen bij publiek, overheid en bedrijfsleven, ii) aandacht voor een pro-actieve benadering, naast preventieve maatregelen, iii) beschikken over een actuele en betrouwbare dreigings- en risicoanalyse, iv) opbouwen van een adequate, door meerdere actoren gedragen response capaciteit en v) versterken en aansturen van onderzoek en kennisopbouw.

Kabinetsreactie
De ingezette actielijnen uit de NCSS sluiten goed aan bij de problematiek die in het CSBN is geschetst. Zo is op het terrein van digitale spionage en sabotage door het kabinet een maatregelenpakket ontwikkeld. Voor bedrijven is er een handleiding Kwetsbaarhedenanalyse beschikbaar gesteld waarmee zij hun weerbaarheid kunnen vergroten. Bij brief (2010–2011, 30 821, nr. 13) is uw Kamer hierover ingelicht.

Op het terrein van digitale criminaliteit neemt het Kabinet gepaste actie door onder meer het team high tech crime te versterken. Bij brief (2010–2011, 29 628, nr. 256) is uw Kamer hierover geïnformeerd. In het kader van de Onderzoeksagenda Cyber Security wordt door publieke partijen, private partijen en wetenschap onder andere gefocust op nieuwe ontwikkelingen en de risico's die daarmee verbonden zijn.

De militaire toepassingsmogelijkheden in het digitale domein nemen snel toe en verscheidene krijgsmachten beschikken over operationele cybercapaciteiten of zijn deze aan het ontwikkelen. De krijgsmacht moet in staat zijn cyberoperaties uit te voeren ter ondersteuning van het reguliere militaire optreden en beschikken over een uitstekende inlichtingenpositie in het digitale domein. Zoals gemeld in de brief «Defensie na de krediet crises» (2010–2011, 32 733, nr. 1) en in de defensiebegroting voor 2012 (2011–2012, 33 000 X, nr. 2) zal Defensie daarom investeren om haar capaciteiten aanzienlijk te versterken en verder te ontwikkelen.

Het is noodzakelijk dat Defensie de kennis en capaciteiten ontwikkelt om offensieve handelingen te verrichten in het digitale domein. De krijgsmacht moet ook in het digitale domein in staat zijn een tegenstander het handelen onmogelijk te maken. De krijgsmacht moet daarbij ten opzichte van elke tegenstander over escalatiedominatie beschikken om onder alle omstandigheden doeltreffend te kunnen zijn. Tevens zal door de ontwikkeling van offensieve capaciteiten het defensief vermogen worden versterkt. Hiertoe zal in 2012 onder meer een defensie cyber doctrine worden opgesteld. Om de inzetbaarheid van de krijgsmacht te waarborgen, wordt verder de digitale weerbaarheid versterkt, vooral door een uitbreiding van de taken van het Defensie *Computer Emergency Response Team* (DefCERT). DefCERT zal begin volgend jaar een convenant sluiten met het NCSC om de samenwerking te versterken. Dit betreft zowel informatie-uitwisseling als (personele) ondersteuning bij calamiteiten. Ook de inlichtingen- en kennispositie van Defensie wordt de komende jaren aanzienlijk versterkt, voornamelijk door het vergroten van de capaciteit bij de MIVD. Ook zal de samenwerking met de AIVD worden geïntensiveerd.

In januari 2012 wordt onder leiding van de Commandant der Strijdkrachten de Taskforce Cyber opgericht die verantwoordelijk is voor de ontwikkeling van de cybervermogens. Vervolgens ligt de prioriteit voor Defensie bij de oprichting van een Defensie Cyber Commando en een Defensie Cyber Expertise Centrum die ook moeten zorgen voor een versterking van de nationale en internationale samenwerking.

Internationale informatie-uitwisseling en samenwerking zijn essentieel voor een goed dreigingsbeeld en adequate aanpak van incidenten. Nederland zoekt daarom aansluiting met cyber security centra in verschillende landen, voortbouwend op bestaande samenwerkingsverbanden zoals de CERT-netwerken. Ook in het herziene NAVO-cyberbeleid, opgesteld in het kader van het nieuw Strategisch Concept waarin cyberdreigingen expliciet zijn opgenomen, zijn informatiedeling en verbeterde response belangrijke doelstellingen waarvoor Nederland heeft gepleit. Daarnaast investeert Nederland in EU-samenwerking. Het kabinet zet dan ook onverminderd in op de in de NCSS ingezette integrale aanpak.

Het kabinet onderschrijft de reactie van de CSR, en zal de adviezen van de CSR onverkort uitvoeren. In 2012 zal het kabinet daarom inzetten op kwantitatieve en kwalitatieve verbetering van het CSBN. Het NCSC zal meer en op structurele basis aansluiting zoeken bij private partijen voor een nadere kwantificering van dreigingen voor het CSBN. Het kabinet maakt graag gebruik van het aanbod van de CSR om haar medewerking te verlenen bij het nader kwantificeren van de genoemde dreigingen.
De kwalitatieve verbetering van het CSBN is een continu proces. Het CSBN zal verder worden uitgebouwd naar een volwaardige dreigings- en risicoanalyse. Medio 2012 zal het tweede CSBN aan uw Kamer worden verzonden. De prioriteiten van de CSR sluiten aan op de punten waarop het kabinet zich in het kader van de NCSS in 2012 zal focussen, namelijk: i) vergroten van het bewustzijn van cyber dreigingen bij publiek, overheid en bedrijfsleven, ii) aandacht voor een pro-actieve benadering, naast preventieve maatregelen, iii) beschikken over een actuele en betrouwbare dreigings- en risicoanalyse, iv) opbouwen van een adequate, door meerdere actoren gedragen response capaciteit en v) versterken en aansturen van onderzoek en kennisopbouw. In het voorjaar van 2012 wordt uw kamer nader geïnformeerd over de voortgang van de implementatie van de NCSS.

Juridisch kader cyber security

In het hierboven genoemde AO Nationale Veiligheid van 1 juni 2011 is stilgestaan bij de juridische context waarbinnen de NCSS wordt uitgevoerd. In het bijgevoegde juridisch kader is ervoor gekozen om de verschillende fasen van het bevorderen van cyber security als uitgangspunt te nemen: preventie, toezicht, meldplichten, interventie, opsporing en repressie. Hieraan gaat het relevante grondwettelijk en verdragsrechtelijk kader vooraf. Tot slot wordt aandacht gegeven aan de waarborgen die op dit terrein voor individuen van belang zijn.

Het juridisch kader gaat niet enkel in op wet- en regelgeving die specifiek op cyber security is gericht. Het bespreekt ook de wet- en regelgeving aangaande bevoegdheden en andere mogelijkheden die in het kader van cyber security relevant kunnen zijn. Het stuk heeft derhalve een brede scope, maar is niet bedoeld als uitputtend overzicht van wetgeving, maar primair als identificatie van relevante aspecten. Ten behoeve van het opstellen van deze brief zijn diverse betrokken publieke en private partijen geconsulteerd.

Voor het juridisch kader cyber security is het van belang wat onder «cyber security» moet worden verstaan. Aangesloten is bij de definitie zoals gehanteerd in de NCSS d.d. 22 februari 2011.[1] Cyber security wordt hierin omschreven als het vrij zijn van gevaar of schade veroorzaakt door verstoring of uitval van ICT of door misbruik van ICT.

Het gevaar of de schade door misbruik, verstoring of uitval kan bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van de ICT, schending van de vertrouwelijkheid van in ICT opgeslagen informatie en aantasting van de integriteit van die informatie. Cyber security ziet derhalve toe op zowel opzettelijke als onopzettelijke incidenten en verstoringen van ICT-netwerken.

Cyber security is een breed terrein dat vele raakvlakken kent met andere beleidsterreinen, waaronder het privacybeleid, het telecombeleid en het buitenlands veiligheids- en defensiebeleid. Deze terreinen zijn slechts meegenomen in dit juridisch kader, daar waar directe aanknopingspunten lijken te bestaan. Voor het privacybeleid, waaronder de meldplicht datalekken (persoonsgegevens) verwijs ik u naar de brief aan uw kamer getiteld:

Verwerking en bescherming persoonsgegevens (TK 2010–2011, 32 761, nr. 1) en de toezeggingen gedaan tijdens het AO van 15 september 2011.

Zoals reeds aangegeven loopt er ten aanzien van de implicaties van de ontwikkelingen in het cyberdomein voor het buitenlands veiligheids- en defensiebeleid momenteel een adviesaanvraag bij de Adviesraad Internationale Vraagstukken en de Commissie van Advies inzake Volkenrechtelijke Vraagstukken met daarin onder andere aandacht voor internationaalrechtelijke aspecten. Uw Kamer wordt hierover op korte termijn geïnformeerd.
Ik wil in relatie tot de motie Franken (EK 31 051 17 mei 2011) benadrukken dat dit kabinet zeer hecht aan de bescherming van de persoonlijke levenssfeer en dit bij de formulering van nieuwe wet- en regelgeving, ook op cyber security terrein, zeer ter harte neemt.

Grondrechtelijk en verdragsrechtelijk kader
Het grondwettelijk en verdragsrechtelijk kader omschrijft de rechten en plichten van de overheid ten opzichte van burgers. Het grondwettelijk en verdragsrechtelijk kader is met name relevant als de wetgever besluit om

[1] Zie Kamerstukken 26 643, nr. 174.

aanvullende wet- en regelgeving met betrekking tot cyber security vast te stellen. In deze gevallen dient de wetgever te beoordelen of de wet- en regelgeving die is voorgesteld, past binnen dit kader.

Voor huidige wet- en regelgeving met betrekking tot cyber security geldt, dat deze reeds bij totstandkoming aan het grondwettelijk en verdragsrechtelijk kader is getoetst. In beginsel wordt wet- en regelgeving en overheidsoptreden na inwerkingtreding niet door de rechter aan het grondwettelijk kader getoetst: artikel 120 Gw sluit een dergelijke toetsing uit. Wel kan de rechter beoordelen of wet- en regelgeving en overheidsoptreden in lijn is met verdragen waarop een algemeen beroep kan worden gedaan, zoals het Europees Verdrag voor de Rechten van de Mens **(«EVRM»)**.

Op grond van artikel 10 Gw en artikel 8 van het EVRM bijvoorbeeld heeft iedereen recht op eerbiediging van zijn of haar persoonlijke levenssfeer. De persoonlijke levenssfeer omvat tal van terreinen, welke zeer uiteenlopend van aard zijn.[1] Hieronder vallen bijvoorbeeld de woning, de briefwisseling en de communicatie via telefoon en andere communicatiemiddelen.

Uitgangspunt van deze bepalingen is dat de overheid uitsluitend beperkingen kan stellen aan de persoonlijke levenssfeer in gevallen die bij of krachtens de wet zijn bepaald. Op grond van artikel 8 EVRM zijn beperkingen voorts alleen toegestaan indien deze noodzakelijk zijn ter bescherming van bepaalde belangen, waaronder de nationale en de openbare veiligheid alsmede het economisch welzijn van een land. Artikel 10 lid 2 Gw vereist voorts, dat de wet regels stelt met betrekking tot het vastleggen en verstrekken van persoonsgegevens.

Het respecteren van het grondwettelijk en verdragsrechtelijk kader is vanzelfsprekend een punt dat buiten discussie staat.
Bij het formuleren van nieuwe wet- en regelgeving is dit de leidraad, waarbij ook de specifieke punten uit de motie Franken[2] m.b.t. de persoonlijke levenssfeer door het kabinet worden onderschreven.

Preventie en toezicht
In deze fase gaat het om het voorkomen van een cyberincident, door onder andere de controle en verbetering van de beveiliging, het verzamelen van informatie over risico's en het uitwisselen van informatie tussen partijen.

Wetgeving van algemene aard
Het Burgerlijk Wetboek is van toepassing daar waar de overheid, als opdrachtgever, een contractuele relatie aangaat met een opdrachtnemer. Deze contractuele relatie is een belangrijk preventief middel om het niveau van informatiebeveiliging te bevorderen door bepalingen die een bepaald niveau van informatiebeveiliging opleggen aan de opdrachtnemer.

Door middel van de Wet Bescherming Persoonsgegevens wordt aan verwerkers van persoonsgegevens de verplichting opgelegd om passende technische en organisatorische maatregelen te treffen om persoonsgegevens te beschermen tegen verlies of enige vorm van onrechtmatige verwerking. Dit betreft een algemene verplichting aan verwerkers van persoonsgegevens. Het College Bescherming Persoonsgegevens is de toezichthouder op de algemene verplichting. In diverse sectoren gelden echter specifieke sectorale verplichtingen waar invulling aan gegeven dient te worden. In de brief aan uw Kamer getiteld: Verwerking en bescherming persoonsgegevens (TK 2010–2011, 32 761, nr. 1) zijn de

[1] Zie Kamerstukken *II*, 1975/76, 13 872, nr. 3, p. 40.
[2] Zie Eerste Kamer, vergaderjaar 2010–2011, 31 051, D.

Staatsecretaris van Veiligheid en Justitie en de Minister van Binnenlandse Zaken en Koninkrijksrelaties reeds uitvoerig ingegaan op de aanpak sanctionering overtredingen Wet Bescherming Persoonsgegevens

Inlichtingen en veiligheidsdiensten
De Wet op de Inlichtingen en Veiligheidsdiensten 2002 (Wiv 2002) omschrijft de taken en regelt de bevoegdheden van de Nederlandse inlichtingen- en veiligheidsdiensten AIVD en MIVD.
Binnen de kaders van hun taakbeschrijving en bevoegdheden zijn AIVD en MIVD bevoegd onderzoek te doen naar digitale aanvallen en naar de dreiging in en vanuit het digitale domein. De Wiv 2002 is opgesteld in een periode waarin wat nu tot het digitale domein wordt gerekend, geen prominente rol speelde binnen het werkterrein van de diensten. Nader onderzocht zal worden of de Wiv 2002 elementen bevat die door voortschrijdende technologische ontwikkelingen achterhaald zijn en de diensten onbedoeld beperken in de goede taakuitvoering in het digitale domein.

De Ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Defensie zullen u hierover, indien noodzakelijk, separaat informeren.

Sectorale verplichtingen
Naast algemene wet- en regelgeving bestaat er op het sectorale niveau relevante wet- en regelgeving met daarbij voor de diverse sectoren van toepassing zijnde verplichtingen.
Deze wet- en regelgeving laat zich veelal kenmerken door de specifieke focus op de sector. Dit neemt echter niet weg dat deze wet- en regelgeving relevant kan zijn in het kader van cyber security. In het juridisch kader worden een aantal verplichtingen uiteengezet zoals die gelden voor: financiële instellingen, nutsvoorzieningen, telecommunicatiediensten, zorginstellingen en het spoorvervoer. De sectorale toezichthouders houden, middels de aan hen toegekende toezichtbevoegdheden, toezicht op de wijze waarop invulling wordt gegeven aan de in wet- en regelgeving vastgelegde zorgplichten zoals die van toepassing zijn op de desbetreffende sector.

De sectorale zorgplichten zijn echter vaak algemeen geformuleerd en zien niet specifiek op het voorkomen van cyber security incidenten. Deze zorgplichten zullen, zeker waar het instellingen van een maatschappelijk vitaal belang betreft, nader worden gespecificeerd. Hiermee zullen toezichthouders beter in staat zijn toezicht te houden op voor cyber security relevante aspecten. De specificatie zal op basis van overleg met de betreffende sectoren en toezichthouders en met ondersteuning van experts uit het op te richten NCSC plaatsvinden.

Meldplichten en maatregelen
In algemene aard kan er strafrechtelijk sprake zijn van een meldplicht indien er sprake is van de schending van een staatsgeheim en bij levensgevaar. Dit zijn echter zeer specifieke gevallen. Ook in contractuele relaties kan een meldplicht bedongen worden of verondersteld worden als goed opdrachtnemer.

Tevens gelden er meerdere sectorale meldplichten met een divers karakter. Beursgenoteerde instellingen dienen bijvoorbeeld koersgevoelige informatie onverwijld openbaar te maken. Daar waar het directe meldplichten betreft zijn momenteel meerdere trajecten in gang gezet. Het is van belang om hierbij te vermelden dat het Kabinet hierbij het uitgangspunt hanteert dat pas wanneer zelfregulering niet werkt er gekeken wordt naar mogelijkheden van wet- en regelgeving.

Ten eerste betreft het een tweetal meldplichten voortvloeiend uit het wijzigingsvoorstel van de Telecommunicatiewet. Dit wetsvoorstel ligt momenteel in de Eerste Kamer.

Het wetsvoorstel voorziet in twee meldplichten bij verschillende toezichthouders bij een gemeenschappelijk meldloket. De eerste meldplicht (artikel 11.3a van de Telecommunicatiewet) gaat om inbreuken die een nadelig effect hebben op de bescherming van persoonsgegevens. De werkingssfeer van dit artikel is beperkt tot aanbieders van elektronische communicatiediensten.
Ten tweede wordt er binnen dit wetsvoorstel ook een meldplicht inzake de continuïteit van elektronische communicatienetwerken en -diensten geïntroduceerd middels het voorgestelde artikel 11a.2. Het gaat hierbij om inbreuken op de veiligheid of verliezen aan integriteit waardoor de continuïteit in belangrijke mate werd verbroken. Deze meldplicht ziet dus, in tegenstelling tot de meldplicht uit artikel 11.3a, niet specifiek op persoonsgegevens.

De bovenstaande meldplichten zijn echter sectorspecifieke meldplichten. Deze meldplichten vinden hun oorsprong in Europese richtlijnen.
In een breder verband is in het regeerakkoord reeds aangekondigd dat het kabinet zal komen met een voorstel tot een meldplicht voor alle diensten van de informatiemaatschappij in gevallen van verlies, diefstal of misbruik van persoonsgegevens, waarbij de datalekken worden gemeld aan de nationale toezichthouder. De Staatssecretaris van Veiligheid en Justitie[1] heeft reeds aangegeven dat er op korte termijn een wetsvoorstel hieromtrent ter consultatie zal worden aangeboden. In dit geval betreft het een meldplicht waarin het element persoonsgegevens centraal staat.

Daarnaast heeft uw Kamer in het debat over DigiNotar d.d. 13 oktober 2011 met de Motie Hennis-Plasschaert c.s.[2] de regering verzocht over te gaan tot een wettelijke meldplicht, een zogenaamde «security breach notification». Het gaat hierbij om inbreuken, voor organisaties betrokken bij voor de samenleving vitale informatiesystemen. In het juridisch kader is nog niet specifiek ingegaan op deze meldplicht, aangezien het geen bestaande wet- en regelgeving betreft. Het laat echter wel zien dat er binnen de huidige juridische kaders niet een direct voor de handliggende wet is waarin deze meldplicht onverwijld kan worden opgenomen. De relevante wetgeving (zie bovenstaande voorbeelden) is immers sectoraal van aard dan wel gericht op persoonsgegevens. De motie Hennis-Plasschaert c.s. geeft aan dat de meldingen juist gericht dienen te zijn op voor de samenleving vitale informatiesystemen.

Uw Kamer zal vóór het zomerreces van 2012 nader geïnformeerd worden over de wijze waarop deze meldplicht zal worden ingericht en op welke wijze de informatie gedeeld kan worden met het NCSC. Het beperken van de administratieve lasten en het borgen van de vertrouwelijkheid van met het NCSC gedeelde informatie zijn hierbij voor het Kabinet belangrijke uitgangspunten.

Interventie en opsporing
De overheid heeft diverse interventiemogelijkheden in de fase dat een cyberincident (dreigt) plaats te vinden. Deze bevoegdheden zijn van strafvorderlijke, bestuursrechtelijke en (in beperkte mate) van civielrechtelijke aard. Daarnaast zijn er bevoegdheden in buitengewone omstandigheden, bijvoorbeeld ter beheersing van een (dreigende) crisis of wanneer deze ontoereikend zijn de Coördinatiewet uitzonderingstoestanden. De praktijk leert overigens dat deze laatste, gezien de stringente voorwaarden, zeer zelden wordt toegepast.

[1] In antwoord op mondelinge vragen tijdens het vragenuur van 25 oktober 2011.
[2] Zie Kamerstukken 2010/11, 26 643, nr. 202.

Overheidsinterventies ten tijde van een (dreigende) cybercrisis, waarbij de nationale veiligheid in het geding is, moeten aan een aantal eisen voldoen willen ze effectief zijn op dit terrein. Allereerst dient de reikwijdte van de maatregelen voldoende te zijn. Cyberincidenten doen zich immers niet slechts voor binnen de ICT-sector zelf, maar zijn sectoroverstijgend. Ten tweede vergt effectief ingrijpen (technische) expertise om de complexe gevolgen daarvan juist in te schatten. Ten derde is het van belang dat snel gehandeld kan worden bij een (dreigende) aanval of verstoring.

Het huidig juridisch kader laat zien dat er op dit moment geen juridische grondslag is voor overheidsoptreden langs bovengeschetste lijn.
De Minister van EL&I heeft weliswaar verregaande bevoegdheden op basis van hoofdstuk 14 en artikel 18.9 van de Telecommunicatiewet, maar deze beperken zich tot aanbieders van elektronische communicatienetwerken en -diensten. Het geheel van voor de vitale belangen van de Nederlandse Staat relevante partijen lijkt derhalve op dit moment niet voldoende bereikt te kunnen worden.

Ten tijde van een dreigende cybercrisis is zoals gezegd ook snel handelen van belang. Wanneer de nationale veiligheid in het geding is, dat is het geval wanneer de vitale belangen van de Nederlandse Staat en/of samenleving zodanig bedreigd worden dat sprake is van (potentiële) maatschappelijke ontwrichting kan de Ministeriele Commissie Crisisbeheersing (MCCB) bijeen geroepen worden. In het geval van cyber crises kan het echter zo zijn dat er geen tijd is om dit ministeriele overleg af te wachten en kan het wenselijk zijn dat tijdelijk bevoegdheden door een andere minister worden overgenomen. Op dit moment is het alleen ten tijde van terroristische dreiging mogelijk een aantal specifieke bestaande bevoegdheden tijdelijk over te dragen aan de Minister van Veiligheid en Justitie, opdat onverwijld maatregelen kunnen worden genomen.

Hoewel in veruit de meeste gevallen reguliere structuren uitstekend in staat zullen zijn het incident af te handelen, lijkt het wenselijk om in bovengenoemde crisissituatie voorts te beschikken over nieuwe aanvullende bevoegdheden waarmee de overheid snel, kundig en dwingend kan optreden.
De ervaringen die zijn opgedaan tijdens recente incidenten, zoals de DigiNotar-crisis, onderstrepen dit.

Evenals bij de in de motie Hennis-Plasschaert voorgestelde invoering van een «security breach notification» lijkt ook ten aanzien van cybercrises binnen de huidige juridische kaders geen direct voor de hand liggende wetgeving aanwezig te zijn, waarmee ook in het geval van crises snel, kundig en niet-vrijblijvend geacteerd kan worden. Het onderzoek naar aanvullende interventiemogelijkheden zal dan ook in samenhang met de uitwerking van de «security breach notification» bezien worden. Over de uitkomsten van dit onderzoek zal ik uw Kamer vóór het zomerreces van 2012 informeren.

Opsporing
In paragraaf 5.3 van het juridisch kader is tevens ingegaan op de strafrechtelijke opsporingsbevoegdheden. Zowel nationaal als internationaal lopen er trajecten waar gekeken wordt naar de noodzakelijkheid om wet- en regelgeving aan te passen die nodig is om ook op internet voldoende mogelijkheden te hebben voor de opsporing. Het vorige Kabinet heeft in 2010 een aantal conceptwetsvoorstellen in advies gebracht. De uitkomst van dit adviestraject heeft er toe geleid dat er meer tijd nodig is om te komen tot daadwerkelijke wetsvoorstellen. Daarnaast worden andere uit de praktijk voorkomende onderwerpen waaronder het

online doorzoeken nader verkend. Voor de zomer van 2012 zal ik uw Kamer hierover nader berichten.

Handhaving en repressie
De voor cyber security relevante mogelijkheden tot handhaving en repressie kunnen zowel bestuursrechtelijk als strafvorderlijk van aard zijn. Interessant hierbij, gezien het vaak grensoverschrijdende karakter van cyberincidenten, is de internationale rechtsmacht kwestie ten aanzien van data. Nederland hanteert hierbij de lijn dat het rechtsmacht heeft over data die zich op servers op Nederlands grondgebied bevindt.

Waarborgen
Wet- en regelgeving kent aan private partijen waarborgen toe om overheidsoptreden in het kader van cyber security te controleren en hiertegen zo nodig rechtsmaatregelen aan te wenden. Het gaat hierbij om rechtsbescherming in het bestuursrecht (bezwaar en beroep), het civiel recht (schadevergoeding) en het strafrecht (o.a. EVRM). De Wet openbaarheid bestuur (de Wob) regelt de openbaarmaking van informatie door de overheid en de wet bescherming persoonsgegevens regelt de verwerking van gegevens die natuurlijke personen direct of indirect kunnen identificeren.

Actueel houden van het juridisch instrumentarium is een continu proces
Dit Kabinet staat voor veilige, betrouwbare ICT en het beschermen van de openheid en vrijheid van het internet.
De toenemende afhankelijkheid van ICT maakt de samenleving steeds kwetsbaarder voor misbruik en (grootschalige) verstoring. Het kabinet is daarom in februari van dit jaar gekomen met de Nationale Cyber Security Strategie.

Het bestaande juridisch kader voor cyber security zoals op hoofdlijnen bij deze brief gevoegd, geeft in basis voldoende handvaten voor de implementatie hiervan. Gezien het grensoverschrijdende karakter van het digitale domein, zal Nederland actief bijdragen aan een adequaat internationaal juridisch kader. Het actueel houden van het juridisch instrumentarium is dan ook een continu proces. Op een aantal punten is geconstateerd dat er mogelijk aanvullende instrumenten nodig zijn om de digitale veiligheid in Nederland te bevorderen. Deze instrumenten hoeven echter niet altijd juridisch van aard te zijn.

Voor een open en vrije digitale samenleving is het van groot belang dat de overheid de persoonlijke levenssfeer respecteert en beschermt.

ICT is een belangrijke drijfveer van economische groei, overheidsmaatregelen gericht op de veiligheid en betrouwbaarheid ervan dienen dan ook geen onnodige administratieve lasten op te leggen die mogelijk een verslechtering van de internationale concurrentiepositie kunnen betekenen. Het uitgangspunt is steeds zelfregulering waar mogelijk, wetgeving daar waar moet.

Rechtsmacht in Oostenrijk
In antwoord op uw vraag naar meer informatie over de veronderstelde grensoverschrijdende rechtsmacht binnen de Oostenrijkse cybercrime wetgeving, kan ik u het volgende melden. Oostenrijk heeft een bestuursrechtelijk gesanctioneerde verbodsbepaling opgenomen in de Telecomwet aangaande *cold calling,* spam en sms. Indien de (verboden) *cold call,* spam of sms niet vanuit Oostenrijk heeft plaatsgevonden of is verzonden, wordt als plaats van de overtreding aangemerkt de plaats waar de verboden *cold call*, spam of sms wordt ontvangen.[1] Hierdoor wordt rechtsmacht voor Oostenrijk gegarandeerd, zijnde het land waar het

[1] Zie § 107 (6) van de Oostenrijkse Telecommunicatiewet.

directe gevolg van de overtreding zich openbaart.

Aangezien het hier een bestuursrechtelijke sanctionering betreft die specifiek ziet op spam en sms biedt deze constructie geen oplossing voor internationale (strafrechtelijke) opsporingsonderzoeken.
Zoals reeds opgemerkt is Nederland gebonden aan bestaande internationaalrechtelijke afspraken, die niet eenzijdig kunnen worden gewijzigd. De Nederlandse inzet is er op gericht de mogelijkheden voor een effectieve aanpak van grensoverschrijdende cybercrime te versterken. Dit ondermeer door het stimuleren van ratificering van de Cybercrime conventie van de Raad van Europa en praktisch door het aangaan van joint investigation teams binnen Europa en internationale bilaterale samenwerking.

Nationaal Cyber Security Centrum (NCSC)

Op 1 januari 2012 gaat het NCSC van start. De ambitie van het NCSC is om de digitale weerbaarheid van de Nederlandse samenleving te vergroten. Dit doet het NCSC door het ontwikkelen van inzicht in onder andere cybertrends, dreigingen, incidenten en kwetsbaarheden. Daarnaast door het bieden van een handelingsperspectief of ondersteuning bieden wanneer zich een dreiging, incident of crisis voordoet. Het NCSC zal haar ambitie langs drie pijlers vormgeven.

- Ontwikkelen en aanbieden van expertise en advies
- Ondersteunen en uitvoeren van response bij dreigingen of incidenten
- Versterking van crisisbeheersing

Het succes van het NCSC hangt af van de inbreng van kennis en kunde van zowel publieke als private partijen. Goede samenwerking en het vertrouwelijk kunnen delen van informatie zijn daarbij belangrijke randvoorwaarden. De overheid investeert onder andere in het NCSC door de inbreng (in januari 2012) van Govcert.nl, de ICT Response Board[1] en een vertegenwoordiging van verschillende relevante overheidspartijen (onder andere AIVD, Politie, OM, Defensie en NFI). Met deze stevige basis nodigt de overheid andere relevante private en publieke partijen uit om zich aan te sluiten bij het NCSC. In 2012 zal worden ingezet op de aansluiting van vitale sectoren bij het NCSC.Op dit vlak is reeds een aantal goede stappen gezet in de vorm van de deelname van private partijen in de publiek-private ICT Response Board. Tevens worden in 2012 de ISAC's verder aangesloten bij het NCSC. Daarbij zullen de volgende sectoren als eerste benaderd worden: energie, ICT/telecom, financieel, drinkwater, keren en beheren oppervlaktewater en transport. Samen met alle partners (in het bijzonder de vitale sectoren) werkt het NCSC aan de versterking van de digitale weerbaarheid van Nederland. Daarbij heeft iedere partij haar eigen verantwoordelijkheid. Het NCSC zal de verschillende partijen daarbij ondersteunen en faciliteren om deze verantwoordelijkheid op passende wijze in te kunnen vullen.

Tot slot

Het CSBN geeft periodiek inzicht in de problematiek van cyber security en maakt daarbij onderscheid tussen verschillende vormen van dreigingen op het terrein van cyber security. Digitale spionage, digitale sabotage en digitale criminaliteit zijn de grootste digitale dreigingen waar Nederland nu mee wordt geconfronteerd. Het kabinet zet onverminderd in op de in de NCSS ingezette integrale aanpak. In 2012 zal het kabinet inzetten op kwantitatieve en kwalitatieve verbetering van het CSBN. Medio 2012 zal het tweede CSBN aan uw Kamer worden verzonden.

[1] Waarin experts van zowel de overheid als van private partijen in deelnemen.

Concreet zal het kabinet zich in het kader van de NCSS in 2012 focussen op: i) vergroten van het bewustzijn van cyber dreigingen bij publiek, overheid en bedrijfsleven, ii) aandacht voor een pro-actieve benadering, naast preventieve maatregelen, iii) beschikken over een actuele en betrouwbare dreigings- en risicoanalyse, iv) opbouwen van een adequate, door meerdere actoren gedragen response capaciteit en v) versterken en aansturen van onderzoek en kennisopbouw. In het voorjaar van 2012 zal uw Kamer nader worden ingelicht over de voortgang.

Uit het juridisch kader cyber security blijkt dat binnen de huidige juridische kaders niet direct een wet voor handen is waarin de, in de motie Hennis-Plasschaert voorgestelde, uitwerking van de wettelijke meldplicht kan worden opgenomen. Over de wijze waarop invulling wordt gegeven aan deze wettelijke meldplicht, zal uw Kamer vóór het zomerreces van 2012 worden geïnformeerd. Uit het juridisch kader cyber security blijkt ook dat het wenselijk lijkt om in geval van een cybercrisis te beschikken over nieuwe aanvullende bevoegdheden waarmee de overheid snel, kundig en niet vrijblijvend kan optreden. De ervaringen tijdens recente incidenten, zoals de DigiNotar-crisis onderstrepen dit. Net als bij de in de motie Hennis-Plasschaert voorgestelde wettelijke meldplicht, valt ten aanzien van cybercrisis te constateren dat er binnen de huidige juridische kaders geen direct voor de hand liggende wetgeving aanwezig is waarmee in geval van een crisis snel, kundig en niet vrijblijvend geacteerd kan worden. Het onderzoek naar aanvullende interventiemogelijkheden zal dan ook in samenhang met de wettelijke meldplicht, de zogenaamde 'security breach notification» bezien worden.

In januari 2012 gaat het NCSC van start. Het NCSC zal langs de volgende drie pijlers worden vormgegeven, namelijk i) ontwikkelen en aanbieden van expertise en advies, ii) ondersteunen en uitvoeren van response bij dreigingen of incidenten en iii) versterking van crisisbeheersing. De overheid investeert in het NCSC door de inbreng van Govcert.nl, de ICT Response Board (waarin experts van zowel de overheid als van private partijen deelnemen) en een vertegenwoordiging van verschillende relevante overheidspartijen (onder andere AIVD, Politie, OM, Defensie en NFI). Met deze stevige basis nodigt de overheid andere relevante private en publieke partijen uit om zich aan te sluiten bij het NCSC. In 2012 zal hier verder op worden ingezet.

Zowel tijdens bilaterale bezoeken als de London Conference on Cyber-space in november j.l., waar politici, bedrijfsleven en maatschappelijke organisaties uit ca. 60 landen spraken over een gezamenlijke agenda voor het digitale domein, heeft Nederland haar aanpak voor het voetlicht gebracht en bleek veel interesse voor samenwerking met Nederland. Hieraan zal in 2012 opvolging worden gegeven.

Het Kabinet zet onverminderd in op het versterken van de veiligheid in het digitale domein. Daarbij staat voor ons de ingezette integrale aanpak samen met private partijen van de NCSS en internationale partners centraal.

De minister van Veiligheid en Justitie,
I. W. Opstelten

Bijlage

Nationaal Cyber Security Centrum

1. Waarom een NCSC

De Nederlandse samenleving wordt steeds afhankelijker van de digitale infrastructuur en is daarmee kwetsbaar voor de verstoringen van vitale functies zoals telecommunicatie, bankieren, waterzuivering en energie. Verstoringen kunnen gerelateerd zijn aan onder andere cybercrime, spionage en gerichte digitale aanvallen zoals Stuxnet[1]. Voorbeelden die recent hebben plaatsgevonden zijn: DigiNotar, de «lekken» in verschillende (overheids)websites en de duqu-malware. Deze verstoringen (moedwillig of onopzettelijk) kunnen gevolgen hebben voor de welvaart en het welzijn van de Nederlandse samenleving.

Op 22 februari is de door het kabinet vastgestelde Nationale Cyber Security Strategie(NCSS) gepresenteerd. Het NCSS benadrukt een integrale aanpak (publiek, privaat en wetenschap) van cyber security. Dit omdat de zorg voor digitale veiligheid in Nederland is belegd bij veel verschillende partijen. Om de onderlinge samenhang op operationeel niveau te verbeteren zet het kabinet in op het oprichten van een Nationaal Cyber Security Centrum (NCSC), waar relevante partijen samenkomen en samenwerken.

2. Opdracht NCSS

In de NCSS heeft het kabinet aangekondigd dat het NCSC per 1 januari 2012 start. Het kabinet heeft de volgende opdracht meegegeven:
Het bijeenbrengen van publieke en private partijen om informatie, kennis en expertise uit te wisselen, zodat inzicht kan worden verkregen in ontwikkelingen, kwetsbaarheden, dreigingen en trends, én ondersteuning kan worden geboden bij incidentafhandeling en crisisbesluitvorming. Het kabinet nodigt publieke en private partijen uit zich aan te sluiten bij het Nationaal Cyber Security Centrum (NCSC). Om dit mogelijk te maken wordt een samenwerkingsmodel ontwikkeld. Het huidige govcert.nl zal worden uitbreid, versterkt en ingebracht in het NCSC.

3. Ambitie

De ambitie van het NCSC is om de digitale weerbaarheid van de Nederlandse samenleving te vergroten. Dit doet het NCSC door het ontwikkelen van inzicht in onder andere trends, dreigingen, incidenten, kwetsbaarheden en risico's binnen het domein van de cyber security. Daarnaast door het bieden van handelingsperspectief wanneer zich een dreiging, incident of crisis voordoet. Het NCSC zal haar ambitie langs drie pijlers vormgeven.

Ontwikkelen en aanbieden van expertise en advies
Het NCSC is een centrum waar expertise over cyber security aanwezig is en wordt ontwikkeld, mede door de inbreng van kennis en kunde door samenwerkingspartners. Deze expertise zal door het NCSC worden gericht op vier thema's:

a. Verhogen van het bewustzijn van eindgebruikers, managers, beleidmakers en bestuurders over de aard, omvang en urgentie van cyberdreigingen. Onder andere door strategische publicaties zoals het Cyber Security Beeld Nederland(CSBN).
b. Bijdragen aan preventie van mogelijke cyberincidenten door het aanbieden van richtlijnen voor digitale veiligheid.
c. Kennis delen door het aanbieden van producten zoals factstheets voor managers en diepgaande Whitepapers voor ICT experts.

[1] Nationale Cyber Security Strategie, zie Kamerstukken 2010/2011, 26 643, nr. 174.

d. Advies geven over mogelijke handelingsperspectieven bij kwetsbaarheden of dreigingen. Advies kan breed gericht zijn of juist aan een specifieke partij (zoals maatwerk adviesdiensten).

Ondersteunen en uitvoeren van response bij dreigingen of incidenten
Door kennis en kunde op te bouwen is het NCSC in staat om adequate ondersteuning te bieden bij een dreiging of incident. Het uitgangspunt voor het NCSC richting de Rijksoverheid is het verzorgen van een tweedelijns response en voor de vitale sectoren een derdelijns response[1]. Concreet biedt het NCSC onder andere:
- waarschuwingen over acute dreigingen;
- ondersteuning op afstand of op locatie ten aanzien van onder andere technische, communicatie en juridische aspecten;
- Praktische diensten zoals schoning van botnets en evaluaties van incidenten.

Versterking van crisisbeheersing
Het NCSC zal een belangrijke rol vervullen bij een ICT-crisis. Ook kan het NCSC een bijdrage leveren aan de versterking van de crisisbeheersing door te ondersteunen bij (grootschalige) cyberoefeningen en scenario's. Kernactiviteiten van het NCSC bij een ICT-crisis zijn:
- Faciliteren van de ICT Response Board (IRB): ten tijde van een crisis wordt een IRB georganiseerd[2]. Het IRB draagt vervolgens een advies tot het nemen van maatregelen voor aan de nationale crisisstructuur. Het IRB is geborgd in het NCSC;
- Operationele coördinatie: Het NCSC verzorgt de coördinatie van het bijeenbrengen van operationele informatie en het duiden daarvan. Daarnaast ondersteunt het NCSC de uitvoering van de maatregelen die uit de nationale crisisbeheersingsstructuur komen.

De crisisgerelateerde procedures worden vastgelegd in het Nationaal Crisisplan ICT (NCP-ICT).

4. Samenwerking: voor en door samenwerkingspartners

Het NCSC vormt een samenwerkingsplatform (fysiek en virtueel) waar de voornaamste publieke en private partners (inclusief wetenschaps- en onderzoeksinstellingen) op het terrein van cyber security worden samengebracht en waar het delen van operationele informatie / kennis op een effectieve en vertrouwde wijze wordt gefaciliteerd.

Meerwaarde ontstaat als informatie, kennis en expertise gericht wordt gedeeld tussen partners of door bundeling effectief kan worden ingezet (bijvoorbeeld tijdens een grote ICT-crisis).

Het NCSC kent onder andere de volgende samenwerkingsvormen:
(1) Liaison: partners zijn betrokken in het NCSC via een of meerdere liaisons (op dagelijkse werkzaam bij het NCSC)
(2) Contactpersoon: Een contactpersoon blijft binnen de eigen (netwerk-)organisatie werkzaam, maar is aanspreekpunt voor deze (netwerk)organisatie namens en richting het NCSC.
(3) Ad hoc samenwerking in bijvoorbeeld themagerichte of onderzoeksprojecten.

De belangrijkste samenwerkingspartners van het NCSC zijn:
– De Rijksoverheid en de vitale sectoren. Zij hebben een bijzondere positie in het realiseren van een veilige en stabiele digitale samenleving en de producten en diensten zijn dan ook primair op deze partners afgestemd;

[1] Toelichting dienstverlening ten aanzien van incident response:
– Eerstelijns incident response: incident response door de eigen interne ICT-organisatie van instanties en bedrijven (bestaande capaciteit en onder de eigen verantwoordelijkheid);
– Tweedelijns incident response: een overkoepelende, branche-gerichte «CERT» (in het geval van de Rijksoverheid is het NCSC die branche-gerichte CERT, of voor de academische sector is dit Surf Cert) die zorgt voor incident response binnen een sector of branche;
– Derdelijns incident response: incident response als aanvulling op de tweedelijns incident response. Bijvoorbeeld het inzetten van het NCSC als aanvulling op de incident response bij vitale sectoren (bijvoorbeeld bijstand voor Surf Cert vanuit het NCSC).

[2] De invulling van een IRB is afhankelijk van het type crisis en bestaat uit publieke en private experts.

– (Inter)nationale organisaties met een publieke taak. Hiermee worden onder andere bedoeld inlichtingen- en veiligheidsdiensten, opsporingsdiensten, forensisch onderzoeksdiensten, defensie etc;
– (Inter)nationale kennis- en onderzoekspartners. Onder andere universiteiten en andere (inter)nationale kennis- en onderzoekscentra;
– de (onderzoeks)partijen genoemd in de Nationale Cyber Security Research Agenda;
– (Inter)nationale private leveranciers. Dit zijn partijen zoals de internet service providers, de IT security specialisten of andere kennisleveranciers of dienstverleners. Private leveranciers worden op een structurele wijze bij het NCSC betrokken om waar nodig snel te kunnen schakelen ten tijde van een ICT-crisis of dreiging;
– (Inter)nationale cyber security gemeenschap. Deze gemeenschap bestaat uit de publieke en private CERT's in zowel binnen als buitenland, internationale Cyber Security centra en netwerken en vormt de internationale backbone van kennis, informatie en response.

5. Ontwikkeling NCSC: groeimodel

Het opbouwen van vertrouwen tussen samenwerkingspartners binnen het NCSC zal worden gerealiseerd via een groeimodel. Over de tijd zal het aantal samenwerkingspartners worden uitgebreid en wordt de relatie met de partners verdiept ten behoeve van de kwaliteit van de dienstverlening.

Wat staat er per januari 2012?
Het NCSC start januari 2012. De contouren van het NCSC staan (o.a. bedrijfsvoering, huisvesting, ICT, benoeming directeur NCSC) en de versterking van de personele capaciteit[1] en middelen is gestart.

De inrichting van het NCSC is beschreven. Het NCSC functioneert waar passend vanuit de nieuwe rollen en taken (inclusief bijbehorende mandaten), waarbij ook de huidige taken van Govcert.nl in het NCSC zijn opgegaan.

Een aantal samenwerkingspartners zoals inlichtingen-, veiligheids- en opsporingsdiensten brengt kennis en kunde in. De ICT Response Board is operationeel.

Wat gebeurt in de loop van 2012?
In 2012 wordt invulling gegeven aan de samenwerking door een koplopergroep van de samenwerkingspartners aan het NCSC te verbinden. Deze koplopergroep bestaat uit de Rijksoverheid en een selectie van de vitale sectoren. Voorzien is dat de 6 randvoorwaardelijke vitale sectoren[2], alsook de financiële sector aangesloten zullen worden bij het NCSC. Deze sectoren zijn van essentieel belang voor het functioneren van onze samenleving en worden – in geval van crisis – als eerste het hardst getroffen[3]. Om de relatie met de vitale sectoren verder te verdiepen neemt het NCSC actief deel in de ISAC's van de vitale sectoren.

Wat gebeurt er vanaf 2013?
Het fundament van het NCSC wordt verder uitgebouwd en versterkt. Het NCSC heeft een strategisch plan voor de jaren 2013–2016, waarin staat beschreven hoe de invulling van het NCSC vorm krijgt. Hierin zijn zowel de *lessons learnt* uit 2012, als de nieuwe ambities voor de komende twee jaren opgenomen. De samenwerking met partners heeft een meer structurele invulling gekregen en is klaar voor de bredere uitrol.
Het aanbod aan producten en diensten wordt kwalitatief verbeterd en uitgebreid. Ook wordt het aantal samenwerkingspartners verbreed. Zo wordt nauwe aansluiting gezocht met de overige vitale sectoren en andere doelgroepen zoals (niet-vitale) multinationals. Ten slotte wordt in

[1] Deze versterking betreft ook personen met specifieke expertise op het terrein van internetbeveiliging.
[2] Electriciteit, gas, drinkwater, telecom/ICT, keren en beheren oppervlaktewater, (weg)transport tijdens crisis.
[3] Daarbij loopt de financiële sector voorop in de invulling van digitale veiligheid in haar sector.

deze fase ook actief aansluiting gezocht met de (inter)nationale kennis en onderzoekspartners.

6. Governance

De uitvoering van activiteiten en de verantwoording over resultaten van het NCSC zullen aan de hand van een jaarstukkencyclus worden ingericht;

– Onder verantwoordelijkheid van het hoofd NCSC worden de jaarstukken opgesteld. Het opstellen van de jaarstukken zal samen met alle actieve partners binnen het NCSC (zowel publiek, privaat en wetenschap) plaatsvinden. Door middel van de jaarstukken zorgen partijen er voor dat de taken waar zij aan gaan bijdragen binnen het NCSC zijn geborgd en dat er heldere resultaatafspraken zijn.
– De jaarstukken zullen door een NCSC-programmagroep, met publiek-private vertegenwoordiging, worden beoordeeld en vastgesteld, onder verantwoordelijkheid van de Nationaal Coordinator Terrorisme en Veiligheid (NCTV). Na vaststelling worden de jaarstukken ter kennisgeving aan de Cyber Security Raad (CSR) voorgelegd.[1] De Tweede Kamer zal middels de jaarlijkse voortgangsrapportage cyber security over de jaarstukken worden geïnformeerd.

Het NCSC wordt aangestuurd door een hoofd die de dagelijkse leiding heeft. Dit hoofd ziet toe op de uitvoering van de taken van het NCSC. Deze taken omvatten het oprichten van een samenwerkingsplatform, incident response, operationele regie tijdens crisis en overeengekomen activiteiten ten behoeve van de expertise- en adviesfunctie. Daarnaast is het hoofd resultaatverantwoordelijk voor de producten en diensten die het NCSC levert.

Door een hoofd NCSC aan te stellen die uitvoering geeft aan de kerntaken van het NCSC en het gebruik van een jaarstukkencyclus, wordt voldoende afstand en onafhankelijkheid tot «beleid» gewaarborgd. Tegelijkertijd is het van belang dat «beleid» goed op de hoogte is van operationele informatie en kennis uit het NCSC die relevant is voor beleidsontwikkeling, zodat advisering richting politiek realistisch is en gebaseerd op de laatste ontwikkelingen.

De beheersmatige verantwoordelijkheid voor het NCSC, zoals algemene ICT-voorzieningen en huisvesting, valt onder de verantwoordelijkheid van het ministerie van Veiligheid en Justitie / NCTV. Doordat het NCSC onderdeel is van het ministerie van Veiligheid en Justitie is de continuïteit van het NCSC geborgd.

7. Delen van informatie in een vertrouwde omgeving

Een van de functies van het NCSC is het zijn van een plek waar informatie gedeeld kan worden tussen publieke en private partijen en tussen publieke partijen onderling. Het centrum vervult een spilfunctie. Het NCSC heeft als uitgangspunt dat het een vertrouwde omgeving kent waar partijen zich, binnen de geldende juridische kaders, vrij en veilig (kunnen) voelen om informatie te delen. De vertrouwelijkheid van deze informatie zal dan ook worden geborgd, conform afspraken die met de partners zullen worden vastgelegd. Over de wijze waarop informatie gedeeld wordt, zullen nadere afspraken gemaakt worden in een convenant. Hierbij valt te denken aan afspraken over de wijze van beveiliging en het karakter van de informatie die gedeeld wordt. Uitgangspunt is dat bestaande wetgeving voor deze deelnemers leidend is. Zo geldt voor bepaalde deelnemers binnen het NCSC, bijvoorbeeld inlichtingen- en opsporingsdiensten, een specifiek juridisch kader omtrent de wijze waarop zij informatie kunnen en mogen delen. Het wederzijdse vertrouwen tussen

[1] Er is geen directe sturingsrelatie tussen het NCSC en de CSR. Wel levert het NCSC producten aan de CSR (bijvoorbeeld het periodiek te verschijnen CSBN).

partijen om informatie te delen kost tijd en zal stapsgewijs worden opgebouwd.

8. Financiën

Het ministerie van VenJ voorziet in haar begroting in de basisfinanciering van de kernactiviteiten van het NCSC. Dit betreft onder andere de kerntaken van het NCSC, zoals informatiedeling en kennisontwikkeling, maar ook de (kantoor)faciliteiten voor de fysieke liaisons/participanten. Hiermee zal een financieel gezonde basis voor het NCSC gelegd worden. Voor aanvullende taken of activiteiten zal gewerkt worden volgens andere financieringsstromen:

- Programma-, project- of taakfinanciering: wanneer het NCSC specifieke programma's, projecten of taken uitvoert die onder de (politieke) verantwoordelijkheid van een andere partij vallen (bijvoorbeeld netwerkmonitoring van het Rijk), dan zal een aparte opdrachtovereenkomst worden afgesloten tussen deze partij en het NCSC (inclusief afspraken over middelen). Subsidies of onderzoeksgelden via bijvoorbeeld de EU kunnen daar ook een onderdeel van zijn.
- Abonnementsfinanciering: dit betekent dat partijen een vergoeding betalen voor specifieke geleverde producten en/of diensten.

Daarmee kunnen de gemaakte kosten worden gedekt. Dit model wordt momenteel door Govcert.nl gehanteerd.

- Financiering met «gesloten beurzen»: het uitgangspunt is dat samenwerkingspartners onder eigen verantwoordelijkheid (en budget) informatie inbrengen en delen binnen het NCSC.