BIJLAGE

Gezamenlijke agenda op het gebied van ICT veiligheidsbeleid.

De gezamenlijke agenda is nooit af. Dit komt deels door het dynamische karakter van de ICT sector, waarin markt- en technologische ontwikkelingen zich in een hoog tempo opvolgen. Deels komt dit door het in elkaar overlopen van lopende activiteiten en de ambitie om met nieuwe activiteiten een antwoord te hebben op de snel veranderende ICT ontwikkelingen.

De agenda is derhalve een mengsel van lopende activiteiten en een vooruitblik naar verdere ambities, die zich nog niet in concrete activiteiten hebben vertaald. Het jaar 2007 was het jaar van de opbouw van de samenwerking en coördinatie en was tevens het jaar, waarin het kabinet heeft geïnventariseerd, waar aanvullende ambities en activiteiten zijn gewenst. Het jaar 2008 wordt het jaar van de inhoudelijke synergie. Justitie, BZK en EZ willen niet alleen onderling gezamenlijk optrekken, maar dat ook graag doen met het bedrijfsleven en andere betrokkenen.

Samenwerking betekent open staan voor een aanpak die ook de partners aanspreekt. Bij ICT veiligheidsbeleid is dat onontbeerlijk, omdat die partners grotendeels zélf de verantwoordelijkheid hebben om de preventieve maatregelen te treffen, die de veiligheid en de weerbaarheid rond ICT kunnen vergroten. De overheid stimuleert, ondersteunt en moet in de respons en bestrijdingsfase naadloos aansluiten bij hetgeen de partners reeds aan preventie hebben gerealiseerd. De ambitie is om in het jaar 2008 beter grip te krijgen, waar die aansluiting verbetering behoeft en dat zal zich in een zich verder ontwikkelende agenda vertalen.

De agenda kent een tweedeling, die aansluit bij de rapportagecycli van:
- Nationale Veiligheid en Bescherming Vitale Infrastructuur, respectievelijk
- Het kabinetsbeleid in pijler V: Veiligheid begint bij voorkomen.

Vervolgens worden de kopjes gebruikt, die aansluiten bij de indeling van maatregelen, zoals internationaal is geaccepteerd (indeling volgens structuur van de Genera Assembly van de Verenigde Naties).

Weerbare samenleving en continuïteit

Publiek-private samenwerking

In de vitale sectoren wordt de publiek-private samenwerking gestimuleerd teneinde ICT-verstoringen te voorkomen dan wel een voorspoedig herstel na uitval te bevorderen. Continuïteit van de dienstverlening vormt daarbij het uitgangspunt.
- Samenwerking overheid en aanbieders in Nationaal Continuïteitsoverleg Telecom (op basis van H14 TW)
- Samenwerking overheid en vitale sectoren in Strategisch Overleg Vitale Infrastructuren en Nationaal Adviescentrum Vitale Infrastructuren
- Samenwerking overheid en bedrijfsleven in het programma Nationale Infrastructuur Cybercrime (informatieknooppunten) gericht op ICT aspecten in de diverse aangesloten sectoren (waaronder SCADA systemen)

Voorlichting, bewustwording en ketensamenwerking

Op dit terrein zijn de beleidsinspanningen zowel gericht op voorlichting en bewustwording (bewust en veilig gebruik van ICT door het bedrijfsleven in de vitale sectoren) als op informatiedeling (o.a. via samenwerking in de keten) en preventie, gericht op het tegengaan van cybercrime. Tot de veiligheidsketen behoren de private partijen die ICT en

telecommunicatiediensten leveren (alsmede hun belangrijkste leveranciers), de vitale gebruikers van ICT en telecom en de (overheids)partijen die vanuit inlichtingensfeer of in beleidsmatige zin een bijdrage kunnen leveren aan een optimaal presteren van deze keten. Hieronder volgt een opsomming van lopende en afgeronde activiteiten op dit vlak.

- Voorlichting in het kader van Nationale Veiligheid: gericht op burger, veiligheidsregio's en vitale bedrijfsleven
- Versterken informatieknooppunten rond ICT en vitale sectoren
- De in juni 2007 gehouden Oefening Shift Control was gericht op bewustwording en crisisbeheersing, de evaluatie ervan geeft o.a. aan dat communicatie en samenwerking in tijden van crisis verbeterd kunnen worden, wat zal leiden tot een intensievere oefenagenda.
- Binnen het programma DigiBewust wordt onder meer gerichte voorlichting over veilig gebruik van ICT gegeven aan de partners in de veiligheidsketen: particuliere gebruikers, MKB, onderwijs, e.a.
- De telecommunicatiesector is v.w.b. de openbaar aangeboden diensten voor een groot deel op (inter)nationale schaal georganiseerd en ook de ketensamenwerking houdt met deze schaal rekening. Hierbij worden alle partners in de veiligheidsketen betrokken.
- Binnen de landelijke crisisorganisatiestructuur wordt samen met LOCC en NCC gewerkt aan een nationaal responsplan gericht op een adequate respons bij grote ICT verstoringen.

Onderzoek en kennis

Om onderzoek en kennis op het gebied van ICT veiligheid te bevorderen zijn de banden met kennisinstellingen aangehaald en worden de mogelijkheden voor een gezamenlijke onderzoeksagenda onderzocht.

- Op basis van een inventarisatie van reeds lopende onderzoeken zal worden bezien welke aanvullende onderzoeksactiviteiten hiervoor benodigd zijn

Juridische randvoorwaarden

Binnen de maatschappijontwrichtende arena lijkt het juridisch kader toereikend voor alle partners in de veiligheidsketen om de maatregelen in preventieve en preparatiesfeer te treffen die nodig zijn. Dit laat onverlet dat lopende programma's gericht op het identificeren van keteneffecten en intersectorale afhankelijkheden nieuwe inzichten kunnen genereren, met inbegrip van juridische implicaties.

Intersectorale aanpak
De introductie van nieuwe technologieën (en daarmee afhankelijkheden) maakt structurele aandacht binnen de vitale infrastructuur voor de weerbaarheid en betrouwbaarheid van telecommunicatie/ICT noodzakelijk. Op basis ervan worden veel processen aangestuurd, en ook de afhankelijkheden tussen sectoren zijn in belangrijke mate telecommunicatie/ICT gerelateerd.

- Binnen het programma Bescherming Vitale Infrastructuur worden de intersectorale afhankelijkheden in 2008 op basis van scenario-ontwikkeling nader verkend, opdat een (nationale) risicobeoordeling mogelijk wordt. Op voorhand is duidelijk, dat telecommunicatie/ICT op vrijwel alle andere sectoren een belangrijke invloed heeft.
- Omgekeerd zal ook worden bezien wat de telecommunicatie/ICT-sector aanvullend kan doen om geprepareerd te zijn op dreigingen als overstromingen en pandemieën.

Internationaal
De internationale agenda met betrekking tot continuïteit omvat de bescherming van de vitale (informatie) infrastructuur (cybersecurity) en de weerbaarheid van ICT en telecommunicatie als sector.

- De Europese Commissie overweegt een richtlijn (EPCIP) omtrent de Europese samenwerking en afstemming rond 'Critical Infrastructure Protection'. Deze richtlijn is gericht op grensoverschrijdende gebruik van vitale infrastructuren (waaronder ICT en telecom) en vormt het kader waarbinnen lidstaten de onderlinge (grensoverschrijdende) samenwerking vorm kunnen geven.
- Rond SCADA-systemen (regel- en meetsystemen op afstand), die bij veel vitale infrastructuren worden toegepast, wordt in Europees verband kennis uitgewisseld, waarbij Engeland, Nederland en Zweden een trekkende rol vervullen.
- In diverse internationale gremia komt bescherming en weerbaarheid van ICT en telecommunicatie aan de orde: civiele NAVO; Europese Commissie, OESO, VN
- De samenwerkende Europese lidstaten ontwikkelen samen met de Europese Commissie een uitwerking van 'best practices' met betrekking tot de weerbaarheid van telecomdiensten. DG Information Society heeft hiertoe enkele studies laten verrichten. Het uitwisselen van best practices helpt om de aanpak internationaal op elkaar afgestemd te krijgen. Bovendien helpt het internationaal opererende telecombedrijven om de maatregelen generiek te implementeren en niet per lidstaat een andere aanpak te hoeven volgen.

Preventie en bestrijding cybercrime
Publiek-private samenwerking
Aanbieders en gebruikers van ICT en telecommunicatie maken deel uit van de veiligheidsketen, waarvan de ambitie is deze goed werkend te krijgen. Vooral op het gebied van preventie ligt de sleutel bij bewuste en alerte gebruikers.

- het programma NICC (Nationale Infrastructuur Cybercrime) is een tijdelijk programma om de bestaande partners in de veiligheidsketen (OM, politie, OPTA, GovCert, Consumentenautoriteit, CBP, e.d.) te ondersteunen en samen met de private sector instrumenten te ontwikkelen voor een effectieve preventie en samenwerking, bijvoorbeeld de ontwikkeling van een modelontwerp gericht op Notice & Takedown (dat wil zeggen filtering of blokkering van buitenlandse websites).
- Binnen het programma DigiBewust wordt samengewerkt tussen overheid en bedrijfsleven (aanbieders, softwareleveranciers) om de programma-activiteiten in te richten en inhoudelijk vorm te geven.

- Vertegenwoordigers van NL bedrijfsleven en kennisinstellingen zijn lid van of betrokken bij de permanent stakeholdersgroup van ENISA, het Europese agentschap dat programma's ontwikkelt voor een versterking van de bestrijding van Cybercrime.

Voorlichting, bewustwording en ketensamenwerking

Cruciaal voor het tegengaan van cybercrime is samenwerking tussen de bestaande partijen in de veiligheidsketen, waaronder het bedrijfsleven: aanbieders en gebruikers hebben daarin een rol. Preventie van cybercrime kan alleen als alle partijen in de veiligheidsketen (waaronder nadrukkelijk ook aanbieders en gebruikers) bewust omgaan met hun eigen veiligheid.

- Het programma DigiBewust richt zich onder meer op voorlichting, kennisuitwisseling en bewustwording bij (groot)gebruikers. De afgelopen periode is gewerkt met specifieke doelgroepen, waaronder de jeugd (onder in samenwerking met scholen), MKB en komend jaar zal de focus op senioren liggen.
- Via de service 'Waarschuwingsdienst' kan iedere Nederlander zich gratis abonneren op de door GovCERT afgegeven waarschuwingen rond kwetsbaarheden in systemen en virusdreigingen. De website van GovCERT geeft aan gebruikers allerlei tips.
- Op www.samentegencybercrime.nl is informatie te vinden over het programma NICC en de wijze waarop geïnteresseerden zich daarbij kunnen aansluiten. Het (tijdelijke) programma NICC is erop gericht de werkwijzen te ontwikkelen, waarop de partners in de veiligheidsketen hun rol optimaal kunnen vervullen. Het programma heeft daartoe PPS hoog in het vaandel staan.
- De VbbV brief over Pijler V besteed aandacht aan verdere toerusting en professionalisering van OM en politie
- Als onderdeel van de informatie uitwisseling tussen de ketenpartners, wordt onderzocht in welke mate tot een gezamenlijke trendrapportage gekomen kan worden

Onderzoek en kennis

Om onderzoek en kennis op het gebied van ICT veiligheid te bevorderen zijn de banden met kennisinstellingen aangehaald en wordt de wenselijkheid van een gezamenlijke onderzoeksagenda onderzocht.

- Via de informatieknooppunten en het programma DigiBewust vindt tussen private en publieke organisaties uit de vitale sectoren kennisuitwisseling plaats rond dreigingen en oplossingen met betrekking tot ICT verstoringen
- In OESO verband is een studie van de TU Delft vrijwel afgerond inzake 'economische incentives rond voorkomen en bestrijden cybercrime'

Juridische randvoorwaarden
Mogelijk vergt en effectief beleid van preventie en bestrijding van cybercrime nadere wet- en regelgeving. Waar in de praktijk tegen een dergelijke noodzaak wordt aangelopen, zal het kabinet adequaat reageren.

- Het uitwerken van de juridische randvoorwaarden met betrekking tot Notice & Takedown voor diverse vormen van criminaliteit (phishing, kinderporno, haatzaaien)

Intersectorale aanpak
Preventie en bestrijding van cybercrime vergt een gedifferentieerde aanpak, omdat diverse soorten van cybercrime andere partijen en andere omstandigheden betreffen. Dit neemt niet weg, dat in een praktische aanpak leerervaringen uitgewisseld kunnen worden om te bezien of deze toepasbaar kunnen zijn in een andere situatie.

- Uitwisseling ervaringen tussen sectorale informatieknooppunten onderling en met de overheidsdiensten (AIVD, GOVCERT, OM)

Internationaal
Cyberspace kent geen grenzen. Het internationale en dynamische karakter van cybercrime noodzaakt tot internationale samenwerking.

- In Europees, Civiel NAVO en OESO verband zal samenwerking met de internationale gemeenschap versterkt worden, waar dat passend en mogelijk is zal bij activiteiten of projecten kennis en ervaring ingebracht worden.
- Internationale samenwerking tussen CERTs en ISP’s zal meer gestimuleerd worden.