CYBER SECURITY RAAD

Aan:

de Minister van Veiligheid en Justitie
Mr. I.W. Opstelten
Schedeldoekshaven 100
2511 EX DEN HAAG

Den Haag, 12 december 2011.

Excellentie,

Graag brengen wij namens de Cyber Security Raad door middel van deze brief enkele zaken onder uw aandacht. Zoals u bekend, is onze samenleving in toenemende mate afhankelijk van een goed functionerende, betrouwbare en veilige digitale omgeving. De aandacht voor deze specifieke veiligheid blijkt echter lager dan gewenst, wat veel verstoringen en schade tot gevolg heeft. Gezamenlijke inspanningen om tot een beter begrip van het digitale domein te komen en in nauwe samenwerking tussen publieke partijen, private partijen en wetenschap aan oplossingen voor bestaande en toekomstige onveiligheid te werken zijn daarom van groot belang.

In dat kader heeft de Raad in haar laatste vergadering uitgebreid stilgestaan bij het concept rapport Cyber Security Beeld Nederland (CSBN). De Raad hecht er aan haar waardering uit te spreken voor de aansprekende en heldere wijze waarop actuele dreigingen in het digitale domein in kaart zijn gebracht.

De Raad herkent zich goed in deze eerste editie van het CSBN en onderschrijft de daarin genoemde meest relevante dreigingen. Zoals het CSBN laat zien, is er sprake van zowel een nadrukkelijke dreiging van cyber gerelateerde criminaliteit, als van een toenemende activiteit van statelijke actoren en van een toegenomen dreiging van digitale spionage.

Ten aanzien van het CSBN adviseert de Raad u echter wel om aan een tweetal onderwerpen aanvullende aandacht te laten besteden, deels in volgende edities van het CSBN, deels wellicht in een apart document.

Ten eerste gaat het daarbij om de plaats die deze dreigingen innemen in het grotere geheel van de driehoek *assets – threats – controls*, die immers alleen in onderling verband aangeeft welke risico's samenhangen met de onderkende dreigingen.

Correspondentie adres:
Secretariaat Cyber Security Raad
Schedeldoekshaven 200
2511 EZ Den Haag

Zonder een goed begrip van de specifieke belangen (*assets*) van de overheid en de vitale infrastructuur is het immers moeilijk om te komen tot een goede risicobeoordeling. Ook is het noodzakelijk om te weten welke controlemechanismen en beveiligingsmaatregelen nu al bestaan, om vast te kunnen stellen wat nog ontbreekt en waar met prioriteit aanvullende maatregelen nodig zijn.

Hiertoe dient (in aanvulling op reeds lopende activiteiten) een inventarisatie plaats te vinden van de digitale belangen van overheid en bedrijfsleven, waarbij als eerste aandacht wordt gegeven aan de vitale infrastructuur. Aansluitend moeten de bedreigingen en daarmee samenhangende kwetsbaarheden worden geanalyseerd. Samen met het periodieke CSBN vormt deze inventarisatie de basis om tot een gedegen risicobeoordeling te komen. De reeds aanwezige informatie uit onder andere de rapportages CAET en KWAS zal daarbij vanzelfsprekend worden gebruikt.

Hierbij dient de nadruk te liggen op het op orde krijgen van de bestaande situatie, dus het wegnemen van bestaande kwetsbaarheden. Daarbij zal afgestemd moeten worden met internationale initiatieven en samenwerkingsverbanden, omdat dreigingen in het digitale domein immers grensoverschrijdend zijn.

In deze risicobeoordeling kunnen de controlemechanismen c.q. het weerstandsvermogen en de veerkracht worden beoordeeld op de mate waarin zij de gewenste bescherming voor de onderkende belangen bieden. Hierdoor zijn overheid en bedrijfsleven in de toekomst beter in staat om gerichte keuzes te maken ten aanzien van de noodzakelijke maatregelen en investeringen op het brede terrein van digitale veiligheid.

Ten tweede gaat het om een nadere kwantificering van de met dreigingen en kwetsbaarheden samenhangende risico's (kans maal impact), onder meer op grond van onderkende aanvallen op de digitale omgeving en pogingen daartoe. Indien dergelijke kwantitatieve informatie mee wordt genomen in het periodiek verschijnende CSBN, kan dit de basis vormen voor een trendanalyse, die mede gebruik kan maken van de hiervoor geschetste inventarisatie van belangen en kwetsbaarheden. Samenwerking met de private sector is daarbij nodig om een zo compleet als mogelijk beeld op te bouwen.

Naar de mening van de Raad dienen daarom zowel het CSBN als de hiervoor geschetste inventarisatie in nauwe publiek-private samenwerking tot stand te komen – zo mogelijk vanuit het Nationaal Cyber Security Centrum. De Raad zal in voorkomend geval graag haar medewerking daar aan verlenen. Dit sluit naar de mening van de Raad ook aan op de wensen die in de Tweede Kamer zijn geuit met betrekking tot een betere bescherming van de digitale veiligheid.

De Raad wil, vanuit een strategische benadering, haar eigen bijdragen leveren om de veiligheid in het digitale domein te vergroten.

De Cyber Security Raad heeft daarom gemeend een vijftal prioriteiten te moeten stellen om haar eigen agenda voor het komende jaar praktisch in te vullen. Het betreft:

- Vergroten van het bewustzijn van cyber dreigingen bij publiek, overheid en bedrijfsleven (hiertoe zal onder meer worden voortgebouwd op de campagnes van ECP-EPN);
- Aandacht voor een pro-actieve benadering, naast preventieve maatregelen (de Raad zal waar nodig alle relevante spelers wijzen op de meest relevante deelterreinen binnen het domein digitale veiligheid);
- Beschikken over een actuele en betrouwbare dreigings- en risicoanalyse (een voortzetting van het nu verschenen concept rapport Cybersecurity Beeld Nederland, aangevuld met meer kwantitatieve informatie);
- Opbouwen van een adequate, door meerdere actoren gedragen response capaciteit (krijgt onder andere vorm in de publiek-private ICT Response Board en in het op te richten Nationaal Cyber Security Centrum, waarbij de Raad de inbreng van private kennis en deskundigheid zal stimuleren);
- Versterken en aansturen van onderzoek en kennisopbouw (langs de lijnen van de Onderzoeksagenda Digitale Veiligheid: National Cyber Security Research Agenda).

Verder wil de Raad benadrukken dat de wijze waarop overheid, bedrijfsleven en wetenschap samenwerken in de Cyber Security Raad, naar haar mening een goed voorbeeld is van de noodzakelijke gezamenlijke inspanning op het terrein van digitale veiligheid. Het in januari op te richten Nationale Cyber Security Centrum zal in haar verdere ontwikkeling een soortgelijke intensieve publiek-private samenwerking kennen.

De Raad gaat er van uit dat op die wijze de beschreven dreigingen op passende wijze kunnen worden bestreden. Waar het gaat over de uitvoering van maatregelen ter vergroting van de digitale veiligheid, gaat de Raad er van uit dat daarvoor zo goed als mogelijk gebruik zal worden gemaakt van de reeds in de publieke en private sector beschikbare expertise, kennis en oplossingen.

Hoogachtend,

Zelco Blok
Co-voorzitter

Erik Akerboom
Co-voorzitter

Correspondentie adres:
Secretariaat Cyber Security Raad
Schedeldoekshaven 200
2511 EZ Den Haag