Concept-wetsvoorstel gegevensverwerking en meldplicht cybersecurity

Beantwoording vragen Integraal afwegingskader voor beleid en regelgeving (IAK)

1. Wat is de aanleiding?

De meldplicht voor ICT-inbreuken is aangekondigd in een brief aan de Tweede Kamer van 6 juli 2012,[1] naar aanleiding van een verzoek van de Kamer om te komen tot de wettelijke vastlegging van een 'security breach notification' bij het Nationaal Cyber Security Centrum (NCSC, een onderdeel van het Ministerie van Veiligheid en Justitie) voor organisaties die betrokken zijn bij voor de samenleving vitale informatiesystemen.[2] Aanleiding voor dat verzoek was de elektronische inbraak bij het bedrijf DigiNotar in het najaar van 2011.

De versteviging van de wettelijke grondslag voor de taken van het NCSC en de daaraan gekoppelde bevoegdheid tot verwerking van (persoons)gegevens is, mede vanwege de wens om de positie van het NCSC te versterken (zie o.a. Kamerstukken 26 643, nrs. 272 en 286), aangekondigd in een brief aan de Tweede Kamer van 12 december 2013 (Kamerstukken 26 643, nr. 297).

2. Wie zijn betrokken?

Het wetsvoorstel is met name relevant voor aanbieders van vitale producten of diensten binnen de sectoren elektriciteit, gas, drinkwater, telecom, keren en beheren oppervlaktewater, financiën, overheid en transport, zoals energienetwerkbeheerders, drinkwaterbedrijven, telecombedrijven, beheerders van hoofdwaterkeringen, banken, het Havenbedrijf Rotterdam, de NV Luchthaven Schiphol en Luchtverkeersleiding Nederland. Het gaat om onderdelen van de vitale infrastructuur waarbij een ICT-inbreuk direct of indirect tot maatschappelijke ontwrichting kan leiden. De bedrijven of andere organisaties en de producten en diensten waarvoor de meldplicht gaat gelden, zullen worden aangewezen bij algemene maatregel van bestuur.

3. Wat is het probleem?

De samenleving wordt steeds afhankelijker van elektronische informatiesystemen, die bovendien onderling verweven zijn. Om cascade-effecten te voorkomen is het cruciaal dat vitale aanbieders het NCSC tijdig op de hoogte stellen van ernstige ICT-inbreuken, zodat het NCSC zo snel mogelijk er door advisering en hulpverlening aan kan bijdragen dat maatschappelijke ontwrichting wordt voorkomen of beperkt.

Het NCSC verwerkt gegevens die onder omstandigheden moeten worden aangemerkt als persoonsgegevens, met name IP-adressen,[3] e-mailadressen en domeinnamen[4] die op enigerlei wijze betrokken zijn bij digitale aanvallen. Voor die gegevensverwerking

---

[1] Kamerstukken II 2012/13, 26 643, nr. 247.
[2] Motie-Hennis-Plasschaert c.s., Kamerstukken II 2011/12, 26 643, nr. 202.
[3] Het IP-adres is een nummer waarmee een computer met internetverbinding kan worden geïdentificeerd. IP-adressen worden door het College bescherming persoonsgegevens over het algemeen als persoonsgegeven aangemerkt, zie *Cbp Richtsnoeren – Publicaties van persoonsgegevens op het internet*, 2007, p. 10.
[4] Een domeinnaam kan een persoonsgegeven zijn, bijvoorbeeld als de naam van de beheerder van de website er deel van uitmaakt.

ontbreekt een specifieke wettelijke grondslag. Voorts is er onvoldoende duidelijkheid over de geheimhouding van vertrouwelijk aan het NCSC verstrekte gegevens.

4. Wat is het doel?

Een melding van een ernstige ICT-inbreuk bij een vitale aanbieder aan het NCSC is enerzijds bedoeld om tijdig te kunnen inschatten hoe groot de impact en daarmee de potentiële maatschappelijke ontwrichting van een ICT-inbreuk 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, met name ook door andere vitale organisaties te waarschuwen en te adviseren.

De regels over gegevensverwerking beogen versteviging van de wettelijke grondslag voor de werkzaamheden van het NCSC, en de verwerking van persoonsgegevens in het bijzonder, en duidelijkheid over de verstrekking door het NCSC van vertrouwelijke gegevens aan derden.

5. Wat rechtvaardigt overheidsinterventie?

De meldplicht is gerechtvaardigd doordat de samenleving afhankelijk is geworden van elektronische informatiesystemen en betrokkenheid van het NCSC bij gebleken incidenten of kwetsbaarheden voor ook vitale systemen ertoe kan bijdragen dat maatschappelijke ontwrichting wordt voorkomen. Wettelijke regels voor de werkzaamheden van het NCSC zijn gerechtvaardigd omdat het NCSC toegang heeft tot een veelheid aan informatie over ICT-gerelateerde kwetsbaarheden en dreigingen teneinde zijn taken (hulpverlening, etc.) te vervullen. Het NCSC ontwikkelt zich steeds meer tot centraal meldpunt. De verwachting is dat door verdere intensivering van de samenwerking met (vitale) publieke en private partijen de informatiepositie van het NCSC nog verder wordt versterkt. Daarbij is het van groot belang om de vertrouwelijkheid van aan het NCSC verstrekte gegevens zo veel mogelijk te waarborgen.

6. Wat is het beste instrument?

Wetgeving is het beste instrument om het bij vraag 3 beschreven probleem op te lossen, om de bij vraag 5 aangegeven redenen.

7. Wat zijn de gevolgen voor burgers, bedrijven, overheid en milieu?

Voor de samenleving vitale partijen (bedrijven en overheidsorganisaties) kunnen door dit wetsvoorstel effectiever door het NCSC worden bijgestaan om de beschikbaarheid en betrouwbaarheid van hun producten en diensten te waarborgen of te herstellen. Dat is ook in het belang van niet-vitale partijen en van burgers. Als een ernstige ICT-inbreuk onder de meldplicht valt, dan veroorzaakt dat voor de getroffen aanbieder een bescheiden stijging van zijn administratieve lasten. Voor het milieu zijn er geen gevolgen.