BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

Post Bits of Freedom
Postbus 10746
1001 ES Amsterdam

Bank 55 47 06 512
KvK 34 12 12 86

M +31 613380036
E ton.siedsma@bof.nl
W https://www.bof.nl

Ivo Opstelten
Minister van Veiligheid en Justitie
Postbus 20301
2500 EH DEN HAAG

Betreft
Reactie op consultatie Wet gegevensverwerking en meldplicht cybersecurity

Amsterdam
6 maart 2015

Geachte minister Opstelten,

1. Graag reageert stichting Bits of Freedom op het wetsvoorstel voor gegevensverwerking en meldplicht cybersecurity.

2. Bits of Freedom ziet met vreugde dat dit wetsvoorstel op een aantal punten is verbeterd ten opzichte van het vorige wetsvoorstel over een meldplicht voor inbreuken op ICT-systemen dat werd voorgelegd ter consultatie.

3. In het bijzonder is het goed om te kunnen constateren dat de minister meerwaarde ziet in periodieke openbaring van meldingen over inbreuken op ICT-systemen.

4. Daarnaast is het goed dat het Nationaal Cyber Security Centrum (NCSC) nu ook de mogelijkheid krijgt om adequaat te handelen in situaties waarbij het NCSC de beschikking krijgt over (persoons)gegevens. Het NCSC is een organisatie die een grote meerwaarde heeft voor het verhogen van de Nederlandse digitale veiligheid. Daar hoort bij dat het NCSC ook voldoende is toegerust voor haar taken en dat het juridisch kader voor het NCSC wordt aangepast.

5. Bovenstaande neemt niet weg dat het voorstel op een aantal punten verbetering behoeft. In het vervolg zal Bits of Freedom deze punten behandelen.

6. Het betreft daarbij met betrekking tot de meldplicht het openbaar maken van informatie over meldingen, de noodzaak van sanctie en toezicht op naleving van de meldplicht door het NCSC en het verruimen van de

reikwijdte van de meldplicht. Voor de gegevensverwerking door het NCSC zal worden ingegaan op een beperking van het verzoeken om persoonsgegevens door het NCSC. Daarbij zal eerst worden ingegaan op de meldplicht en vervolgens op de gegevensverwerking door het NCSC.

Meldplicht

Transparantie over meldingen is essentieel

7. Om goed inzicht te kunnen verkrijgen in de feitelijke dreigingen voor de ICT-systemen in de vitale sectoren is transparantie over het aantal meldingen, type incidenten, de impact daarvan en de opvolging naar aanleiding van deze meldingen van essentieel belang.

8. Deze cijfers leveren daarnaast een bijdrage aan een vergroot bewustzijn bij burger, bedrijf en de overheid. Deze cijfers kunnen inzichtelijk maken of de digitale weerbaarheid van de aanbieders in vitale sectoren is gegroeid. Mocht er sprake zijn van een daling van de digitale weerbaarheid, dan kunnen deze cijfers aanleiding geven tot versterking van die weerbaarheid door overheid of bedrijfsleven. Op deze wijze wordt er door het openbaar maken van informatie over de meldplicht bijgedragen aan een betere bescherming van de ICT-systemen in vitale sectoren en daarmee wordt ook het belang van de burger beter gediend.

9. De minister gaat in de toelichting op het wetsvoorstel in op onze eerdere aanbeveling[1] om informatie over de meldingen actief openbaar te maken.[2] Daarbij geeft hij aan dat artikel 9 van het wetsvoorsel, over de verstrekking van vertrouwelijke gegevens, daar niet aan in de weg staat. Ook geeft hij een positieve reactie op periodieke en gespecificeerde openbaarmaking, overigens zonder dat daarbij herleidbare informatie geopenbaard wordt[3] Bits of Freedom is blij met deze opmerkingen. Deze opmerkingen krijgen echter ten onrechte geen vervolg in het wetsvoorstel zelf.

10. Zoals hierboven aangegeven levert een actieve openbaarmaking een effectieve bijdrage aan bewustwording en verbetering van de bescherming van ICT-systemen. Het is daarom belangrijk om in het wetsvoorstel een bepaling op te nemen over het actief periodiek, bijvoorbeeld per kwartaal, openbaarmaken van informatie over de meldplicht.

> Bits of Freedom adviseert om een bepaling in het wetsvoorstel op te nemen over periodieke openbaarmaking van gegevens over het aantal inbreuken per sector, de aard en de impact daarvan, en de opvolging naar aanleiding van deze meldingen.

1 Zie de reactie van Bits of Freedom op de consultatie Wetsvoorstel melding inbreuken elektronische informatiesystemen, p. 5.
2 Toelichting op het voorliggende wetsvoorstel, p. 10.
3 Toelichting op het voorliggende wetsvoorstel, p. 15.

Toezicht en sanctionering is noodzakelijk

11. Het belang van de meldplicht is groot. Het is dan ook van wezenlijk belang dat aan de meldplicht wordt voldaan. Om een effectieve meldplicht te garanderen is toezicht op en sanctionering van het niet nakomen van die meldplicht volgens Bits of Freedom noodzakelijk.[4] De minister is echter van mening dat sanctie en toezicht niet noodzakelijk is, mede omdat de noodzaak van delen van incidenten op dit moment kennelijk breed gedragen wordt.[5]

12. Toezicht op het nakomen van de meldplicht en eventuele sanctionering hoeft geen verandering te brengen in de bestaande praktijk. Voor de bedrijven die nu al de noodzaak van de meldplicht zien en zich aan de meldplicht houden, zal niets veranderen. Het is daarentegen wel een noodzakelijke drijfveer voor de bedrijven die de meldplicht niet op prijs stellen en voor bedrijven die de beveiliging van hun ICT-systemen niet op orde hebben.

13. Daarnaast zijn er, mocht in de toekomst de noodzaak van delen niet meer breed gedragen worden, voldoende waarborgen aanwezig zijn om de meldplicht effectief te laten functioneren. Wetgeving hoeft immers niet alleen gebaseerd te zijn op de praktijk van vandaag, maar moet rekening houden met gewijzigde situaties in de toekomst. Dat geldt zeker voor wetgeving over aanbieders van vitale diensten.

14. Een ander argument om nu toezicht en sanctionering op naleving van de meldplicht mogelijk te maken, hangt samen met de NIB-richtlijn. Zoals de minister zelf al aangeeft, is het mogelijk dat op grond van de NIB-richtlijn toezicht en sanctionering op naleving van de meldplicht moet worden ingevoerd. Nederland zou vooruit zou lopen op toekomstige Europese verplichtingen door nu vast toezicht en sanctionering toe te voegen aan dit wetsvoorstel. Het zou tevens consistent zijn; bij de meldplicht datalekken is bewust gekozen om vooruit te lopen op mogelijke Europese verplichtingen. Er is geen reden om dat hier niet ook te doen.

15. Vooruitlopen op Europese ontwikkelingen heeft in dit geval nog een extra voordeel: door toezicht en sanctionering nu bij dit wetsvoorstel integraal te regelen, worden implementatiekosten voor overheid en bedrijfsleven in de toekomst een stuk lager.

4 Zie de reactie van Bits of Freedom op de consultatie Wetsvoorstel melding inbreuken elektronische informatiesystemen, p. 1 en 2.
5 Aldus de minister op p. 6 van de toelichting bij deze wet.

Het toezicht moet bij het NCSC komen

16. Zoals Bits of Freedom eerder al bepleitte, moet toezicht op de naleving en de mogelijkheid om sancties op te leggen bij niet-naleving van de meldplicht bij het NCSC belegd worden.[6]

17. De minister geeft in de toelichting bij deze wet aan dat als op grond van de NIB-richtlijn een meldplicht en sanctie bij niet nakoming van de meldplicht verplicht wordt gesteld, hij voornemens is toezicht op naleving van de meldplicht en sanctionering bij de sectorale toezichthouders neer te leggen.[7]

18. Hier ontstaat de vreemde situatie dat de organisatie die de melding moet ontvangen niet kan controleren of de meldplicht is nageleefd en niet kan sanctioneren bij niet-naleving. Tegelijkertijd ontstaat ook voor de sectorale toezichthouder een vreemde situatie. Deze zal toezicht moeten houden op een meldplicht terwijl de melding niet bij hem ingediend hoeft te worden.

19. Deze situatie is onwenselijk. Meldplicht, toezicht en sanctie zouden in één hand moeten liggen. Als het NCSC verantwoordelijk is voor het ontvangen van de melding, dan moet het NCSC ook toezicht kunnen houden en eventueel sancties kunnen uitdelen als de meldplicht niet wordt nageleefd.

> Bits of Freedom adviseert om een sanctie op te nemen voor het niet nakomen van de meldplicht. Daarnaast moet het NCSC worden aangewezen als toezichthouder op het naleven van de meldplicht.

Reikwijdte meldplicht moet ruimer worden

20. Het ministerie heeft, anders dan Bits of Freedom eerder bepleitte[8], ten onrechte ervoor gekozen om DDoS-aanvallen niet onder de meldplicht te brengen. De meldplicht moet bijdragen aan het "voorkomen of beperken van onderbrekingen van de beschikbaarheid of betrouwbaarheid"[9] van diensten van aanbieders in vitale sectoren. DDoS-aanvallen kunnen die beschikbaarheid eveneens ernstig inperken.

21. Wanneer een DDoS-aanval plaatsvindt bij een dienst in een vitale sector, kan dat grote consequenties hebben en eventueel kunnen leiden tot maatschappelijke ontwrichting. Bij de recente DDoS-aanval op bedrijf Prolocation is de site van de Rijksoverheid vrijwel de hele dag platgelegd. In de toekomst zal nog veel meer dienstverlening alleen nog digitaal verlopen. Dat zal ook gelden voor diensten uit vitale sectoren. Een DDoS-aanval kan

6 Zie de reactie van Bits of Freedom op de consultatie Wetsvoorstel melding inbreuken elektronische informatiesystemen, p. 2 en 3.
7 Toelichting op het voorliggende wetsvoorstel, p. 6.
8 Zie de reactie van Bits of Freedom op de consultatie Wetsvoorstel melding inbreuken elektronische informatiesystemen, p. 3.
9 Toelichting op het voorliggende wetsvoorstel, p. 2.

dan grote, ontwrichtende schade aanrichten als die dienst niet bereikbaar is. Een snelle, verplichte melding kan dan cruciaal zijn.

22. Het verdient daarom aanbeveling om die DDoS-aanvallen die wel tot maatschappelijke ontwrichting kunnen leiden wel onder de meldplicht te brengen, zodat het NCSC desgewenst ondersteuning kan bieden en een bijdrage kan leveren aan het beperken van eventuele maatschappelijke ontwrichting.

> Bits of Freedom adviseert om DDoS-aanvallen die zorgen voor beperkingen in de beschikbaarheid van een dienst op te nemen in de meldplicht.

Gegevensverwerking

23. Het is goed dat de wettelijke grondslag voor de taken van het NCSC en de grondslag voor gegevensverwerking door het NCSC beter verankerd wordt, zeker wanneer die gegevensverwerking betrekking heeft op persoonsgegevens. Toch is er een aantal onduidelijkheden die Bits of Freedom graag opgehelderd ziet.

24. Het is niet duidelijk waar de grenzen liggen van de voorgestelde bevoegdheid voor het NCSC om te verzoeken om gegevens te verstrekken. Artikel 4 van het wetsvoorstel geeft het NCSC de mogelijkheid om ''eenieder'' te verzoeken gegevens te verstrekken. Daaronder moeten ook persoonsgegevens worden verstaan.[10] Artikel 4 is dus niet beperkt tot verzoeken aan vitale aanbieders of publiekrechtelijke organisaties. Uit de toelichting blijkt niet duidelijk waarom het verzoek om gegevens te verstrekken aan eenieder gericht zou moeten kunnen worden. Daarnaast is er geen begrenzing in de aard van de gegevens die opgevraagd zouden kunnen worden.

25. Bits of Freedom acht het voor de controleerbaarheid noodzakelijk dat het beleid voor verzoeken op basis van artikel 4 zo wordt ingericht dat onder meer inzichtelijk is hoeveel verzoeken er door het NCSC wordt gedaan en aan wie die verzoeken zijn gericht. Dat is extra belangrijk omdat ontvangers van het verzoek weliswaar niet verplicht zijn mee te werken, maar daar mogelijk niet van op de hoogte zijn en zich toch verplicht voelen om mee te werken.

26. Daarnaast wordt uit het wetsvoorstel en de toelichting niet duidelijk hoe de verstrekking van deze verkregen informatie aan derden ingeperkt gaat

10 Toelichting op het voorliggende wetsvoorstel, p. 8.

worden. Zoals Bits of Freedom het begrijpt, valt verdere verwerking van de verkregen informatie niet noodzakelijkerwijs onder artikel 9 van het wetsvoorstel. Het zou goed zijn om nader aandacht te besteden aan de inperking van de verdere verspreiding van de op grond van artikel 4 van het wetsvoorstel verkregen informatie.

> Bits of Freedom adviseert om de reikwijdte van artikel 4 van het wetsvoorstel in te perken.

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd. Uiteraard ben ik graag bereid om het bovenstaande nader toe te lichten, mocht daaraan behoefte bestaan.

Hoogachtend,

Ton Siedsma