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 (0)6 13 38 00 36
E ton.siedsma@bof.nl
W https://www.bof.nl

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

Amsterdam
17 september 2013

Betreft
Reactie op consultatie Wetsvoorstel melding inbreuken elektronische informatiesystemen

Geachte Minister Opstelten,

1. Graag reageert stichting Bits of Freedom op het wetsvoorstel voor een meldplicht voor inbreuken op elektronische informatiesystemen.

2. Bits of Freedom is zeer verheugd dat het ministerie dit wetsvoorstel heeft gepubliceerd. We onderschrijven het doel dat de wet probeert te bereiken, namelijk het vergroten van de cyber security bij organisaties in de vitale sectoren. De vele inbreuken in de afgelopen jaren onderstrepen de noodzaak van deze meldplicht.

3. Toch zijn er de nodige verbeteringen in het wetsvoorstel noodzakelijk. Het doel van de meldplicht wordt onvoldoende gerealiseerd. Dat komt omdat de wetgeving onvoldoende effectief is en de reikwijdte te beperkt. Daarnaast geeft het parlement de regie om kaders vast te stellen teveel uit handen. Tot slot is er onvoldoende transparantie over de uitvoering en opvolging van de meldplicht.

4. Hieronder lichten wij bovenstaande opmerkingen nader toe.

<u>De regeling is onvoldoende effectief</u>

5. Het is de bedoeling van het wetsvoorstel om maatschappelijke ontwrichting te voorkomen en een veiligheidscultuur te creëren. Een meldplicht is dan een goed middel om snel helderheid te krijgen over mogelijke maatschappelijke risico's. Ook kan er dankzij de meldplicht adequate hulp geboden worden om verdere maatschappelijke verstoring tegen te gaan.

6. Om de meldplicht bij te laten dragen aan de vergroting van cyber security in vitale sectoren is het noodzakelijk dat aan de meldplicht wordt voldaan. Het wetsvoorstel dient daarom te waarborgen dat deze meldplicht wordt nageleefd. Deze waarborgen ontbreken in dit wetsvoorstel.

7. Er staat geen boete op het niet nakomen van de meldplicht. Bovendien is er geen instantie aangewezen die kan controleren of er aan de meldplicht wordt voldaan. Er wordt uitgegaan van de goede wil van organisaties die onder het bereik van de wet vallen om de meldplicht na te leven. Zo is deze meldplicht in de praktijk een meldverzoek. Dat is onwenselijk.

> Onderzoek wijst uit dat bedrijven die hun processen goed op orde hebben wel zullen rapporteren en de bedrijven die hun beveiliging niet goed op orde hebben niet melden.[1] Daarmee wordt in de praktijk vervolgens alleen aan de meldplicht voldaan door de 'good guys', terwijl het de bedoeling is dat ook de 'bad guys', die het met de beveiliging van hun systemen niet zo nauw nemen, de meldplicht nakomen.

8. Daarom moet er een mogelijkheid bestaan om te controleren of er aan de plicht wordt voldaan en het nakomen van deze plicht desnoods af te dwingen.

9. Ten eerste moet er een sanctie op het niet-melden worden geïntroduceerd. De Memorie van Toelichting (MvT) stelt ten onrechte dat een sanctie de drempel om meldingen te doen kan verhogen.[2] De prikkel van een sanctie draagt bij aan het (versneld) realiseren van de 'just culture' binnen de vitale sectoren.

10. Ten tweede moet een toezichthoudende organisatie worden aangewezen die de naleving van de meldplicht controleert. Het NCSC is vanwege de noodzakelijke specifieke kennis hiervoor de meest geschikte organisatie. Het is de vraag hoe het NCSC achter het bestaan van een inbreuk moet komen, als zij niet over een effectief middel beschikken om te controleren of aan de meldplicht is voldaan. Daarbij vraagt Bits of Freedom zich af of het NCSC momenteel over de capaciteit beschikt om deze taak op zich te nemen, ook wanneer er geen sprake is van een controleverplichting door het NCSC.

> Het NCSC heeft in het verleden laten zien grote capaciteitsproblemen te hebben, zoals gebleken is bij de aanpak van het Pobelkabotnet.[3]

11. Het is eveneens onduidelijk in welke gevallen het NCSC hulp zal bieden in plaats van alleen de melding in ontvangst te nemen. De taakstelling en opvolging van een melding door het NCSC is daarmee onvoldoende gepreciseerd.

---

1 Jane Winn, Are 'Better' Security Breach Notification Laws Possible? *Berkeley Technology Law Journal, Vol. 24, 2009.*
2 MvT p. 2.
3 Kamerstukken II 2012/13, 26 643, nr. 272, p. 2.

12. De suggestie dat het NCSC eventueel een sectorale toezichthouder in kan schakelen,[4] is onvoldoende waarborg voor naleving van de meldplicht. Zo zal het eventuele aangescherpte toezicht te laat plaatsvinden.

> 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. Ook moet de taakstelling van het NCSC nader gespecificeerd worden en dient het NCSC de capaciteit te krijgen die nodig is om deze meldplicht effectief te ondersteunen.

De reikwijdte van de meldplicht is te beperkt

13. Ook de meldplicht zelf moet worden uitgebreid. Alleen daadwerkelijke inbreuken op de veiligheid en de integriteit van een systeem moeten onder dit voorstel worden gemeld.[5] DDoS-aanvallen vallen hier volgens de Memorie van Toelichting niet onder. Bits of Freedom acht dit onjuist.

14. Het wetsvoorstel geeft geen eenduidige definitie van beveiliging. Een veelgebruikte definitie van informatiebeveiliging richt zich op de beschikbaarheid, vertrouwelijkheid en integriteit van deze systemen. Er is dus ook sprake van een inbreuk op de beveiliging bij een verlies van de beschikbaarheid van een dienst.

15. Het is dan ook niet gek dat een DDoS-aanval onder de wetsbepaling valt, ook al wordt die vervolgens in de toelichting hiervan uitgesloten. Wanneer er sprake is van een DDoS-aanval die een systeem plat legt, is er immers sprake van een daadwerkelijke inbreuk. De dienst die via het systeem wordt geleverd, is dan namelijk niet bereikbaar. Daarmee wordt eveneens voldaan aan de twee cumulatieve voorwaarden die de toelichting stelt, namelijk een daadwerkelijke inbreuk op de veiligheid, die vervolgens de beschikbaarheid van de dienst kan onderbreken.

16. Er zijn zwaarwegende redenen om DDoS-aanvallen onder de meldplicht te laten vallen. Een DDoS-aanval kan namelijk een 'stepping stone' zijn voor andere aanvallen of als afleidingsmanoeuvre dienen. Om deze redenen is een snelle melding van een DDoS-aanval juist cruciaal voor het beschermen van de continuïteit en beschikbaarheid van vitale infrastructuren.

17. De regel zou dus moeten zijn: een DDoS-aanval wordt gemeld als er sprake is van een "belangrijke mate van maatschappelijke ontwrichting". Het niet hoeven melden van een DDoS-aanval zou een uitzondering moeten zijn, die

4 MvT p. 5.
5 MvT p. 3.

intern deugdelijk gemotiveerd moet worden. Deze deugdelijke motivering moet later gecontroleerd kunnen worden door het NCSC.

> Bits of Freedom adviseert om de melding van DDoS-aanvallen op te nemen in de meldplicht.

De wetgever geeft de regie uit handen

18. Belangrijke aspecten van deze wet zullen bij Algemene Maatregel van Bestuur (AMvB) geregeld worden. Voor de invulling hiervan zal overleg met de organisaties in de vitale sectoren plaatsvinden. Onder de nader in te vullen aspecten valt in ieder geval welke organisaties aan de meldplicht moeten voldoen, een specifieke regeling voor in welke gevallen gemeld moet worden en wat er precies gemeld moet worden.

    Een goed voorbeeld hiervan is de verstoring van de beschikbaarheid of betrouwbaarheid van een dienst. De verstoring hiervan moet in "belangrijke mate" zijn. Wat "een verstoring in belangrijke mate" van een dienst is, moet nog blijken uit overleg met organisaties uit de vitale sectoren.

19. Het parlement dient het beleid vast te stellen en te controleren. Door de invulling van deze voorwaarden grotendeels aan overleg met de sector over te laten, geeft het parlement de regie uit handen. Daarnaast gaat het parlement akkoord met de mogelijkheid dat de uitwerking in lagere regelgeving anders uitpakt dan met deze wet wordt beoogd.

20. Dit acht Bits of Freedom onwenselijk. Een duidelijkere omschrijving van de voorwaarden waaronder de meldplicht van toepassing is, zou dit probleem oplossen zonder dat dit ten koste gaat van de flexibiliteit van de wet.

> Bits of Freedom adviseert om de voorwaarden waaronder de meldplicht moet worden nageleefd duidelijker te definiëren, evenals op welke organisaties de meldplicht van toepassing is.

Transparantie leidt tot grotere cyber security

21. Een melding hoeft volgens de Memorie van Toelichting in beginsel niet met het publiek gedeeld te worden gemaakt als er geen schadelijke gevolgen zijn. Er wordt gesteld dat het belang van de organisatie zwaarder kan wegen dan openbaar maken. Ook wordt gesteld dat de maatschappelijke onrust groter kan worden door openbaarmaking van de melding.[6] Bits of Freedom is van mening dat transparantie juist wenselijker is.

22. Transparantie zorgt voor vertrouwen in de organisatie en leidt tot

6 MvT, p. 8.

bewustwording bij organisaties. Het imago van een organisatie wordt meer beschadigd door geheimzinnigheid dan door openheid. Maar zelfs als dit imago wel beschadigd zou worden, dan nog dient het imago van organisaties ondergeschikt te zijn aan cyber security en niet andersom.

23. Openbaarheid komt het onderzoek naar cyber dreigingen ten goede. Dit kan de cyber security vergroten. Ook kan openbaarheid de bewustwording bij andere organisaties en bij de consument vergroten.

24. Proactieve transparantie over het aantal meldingen, de inhoud en opvolging daarvan en in welke sectoren deze inbreuken plaatsvinden, is daarom vitaal voor het bereiken van de doelstelling van het wetsvoorstel. Dat geldt niet alleen voor inbreuken waarin daadwerkelijk (maatschappelijke) schade geleden is, maar voor alle gedane (of niet gedane) meldingen over inbreuken.

> Bits of Freedom adviseert gegevens over het aantal inbreuken per sector, de aard en de impact daarvan, en de opvolging naar aanleiding van deze meldingen periodiek - bijvoorbeeld per kwartaal - openbaar te maken.
>
> Bits of Freedom wil benadrukken dat deze gegevens geopenbaard kunnen worden zonder dat deze herleidbaar zijn tot een specifieke organisatie.

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