Nederlandse Vereniging van Banken

Michael Samson
Adviseur Informatica
t + 31 20 55 02 837
m + 31 6 55 72 06 96
e samson@nvb.nl

Ministerie van Veiligheid en Justitie
Postbus 20301
2500 EH DEN HAAG

Datum 16 september 2013
Referentie BR1986

Betreft: Reactie op wetsvoorstel melding inbreuken elektronische informatiesystemen

Geachte lezer,

Bij deze willen we u bedanken voor de mogelijkheid te reageren op dit wetsvoorstel. Onderstaand treft u onze reactie.

Algemeen
Het wetsvoorstel beschrijft op hoofdlijnen de huidige werkwijze van de banken met het NCSC. Banken delen, op basis van reciprociteit informatie over incidenten met het NCSC. Op dit moment zien de NVB en de banken het NCSC als een ondersteunende partij. En die ondersteuning door het NCSC vereist input vanuit de sector(en). De kennisdeling op basis van die reciprociteit is de kracht van de huidige vorm van samenwerking.
De NVB en de banken zijn ook betrokken bij de ICT Response Board. Ook daar zullen banken – waar relevant en nodig – informatie delen.
De recente DDoS aanvallen zijn een goed voorbeeld hoe de samenwerking werkt. In het verslag van de Ministers van Financiën en van Veiligheid en Justitie staat daarover o.a.: “Naar aanleiding van de geconstateerde verstoringen is er terstond intensief contact gelegd tussen de banken en de betrokken instanties, onder meer met de ministeries van Veiligheid en Justitie, Financiën en De Nederlandsche Bank (DNB).”

Doelstelling/uitgangspunt wetsvoorstel
De NVB en de banken vinden dat het wetsvoorstel averechts zou kunnen gaan werken. In plaats van een werkwijze, die is gebaseerd op vertrouwen en op reciprociteit, wordt nu een wettelijk kader geschapen waarbinnen de informatie moet worden geleverd aan het NCSC.
Het NCSC krijgt in het wetsvoorstel een meer toezichthoudende rol. Het risico is dan reëel dat de verhoudingen tussen de sector(en) en het NCSC verandert. Mogelijk leidt dit tot een situatie die veel minder “voelt” dan een publiek-private partnership.
De banken nemen er verder kennis van dat DDoS aanvallen in het wetsvoorstel buiten scope blijven.

Concluderend stellen de NVB en de banken dan ook, dat dit wetsvoorstel de wederzijdse samenwerking, gebaseerd op reciprociteit, negatief beïnvloedt.

De NVB vindt dat een alternatief voor het wetsvoorstel bijvoorbeeld in de vorm van een “manifest van samenwerking” effectiever zal werken in de praktijk..

NVB en de banken vinden het wel reëel, dat er eisen worden gesteld aan het melden van security incidenten voor specifieke sectoren. Deze meldingen zullen dan – voor de sectoren waar dat mogelijk is – moeten worden gemeld aan de eigen toezichthouder. Voor de banken geldt al dat de WFT[1] eist dat een bank de toezichthouder informeert over incidenten die een ernstig gevaar vormen voor de integere uitoefening van het bedrijf in het kader van de eisen aan beheerste en integere bedrijfsvoering.

Vertrouwelijkheid van informatie
Voor de banken en de NVB is, de vertrouwelijkheid van gedeelde informatie een groot punt van zorg, zowel in het huidige wetsvoorstel, als ook al in de huidige situatie.
Voor de financiële sector geldt, dat vertrouwelijke mededelingen van banken aan DNB onder de geheimhoudingsplicht vallen van de WFT. Deze mededelingen van DNB aan de Minister vallen ook buiten de WOB (WFT, artikel 1.47 Lid 2).
De banken denken dat er de ruimte voor discussie is doordat art. 10 lid 1 sub c van de WOB spreekt over bedrijfs- en fabricagegegevens. Deze formulering is voor verschillende uitleg vatbaar en leidt op zijn minst tot procedures bij de rechter waar verweer tegen gevoerd moet worden. Dat is niet bevorderlijk voor een goed samenwerkingsklimaat tussen het NCSC, de NVB en de banken. Incidentgegevens zullen niet altijd kwalificeren als bedrijfs- of fabricage gegevens. Gegevens met betrekking tot de wijze van aanvallen zullen er bij voorbeeld wellicht niet onder vallen. Ook is de vraag hoe de vertrouwelijkheid moet worden gewaarborgd als sprake is van een keten van meerdere partijen, waar de melder een schakel in vormt. Informatie over andere ketenonderdelen valt vermoedelijk evenmin onder een eventuele uitzondering voor de melder. De banken willen graag dat deze wetgeving expliciet duidelijk maakt welke vertrouwelijke informatie niet op basis van de WOB kan worden opgevraagd.

Een andere vraag in het kader van vertrouwelijkheid van gegevens is de vraag, wat er mag worden gedaan door het NCSC met de aangeleverde informatie.
Artikel 6 biedt verder ook nog het NCSC de mogelijkheid om de gegevens van de aanbieder nationaal en internationaal te gebruiken voor het geven van advies. Dit betekent dat andere partijen mogelijk de beschikking krijgen over zeer gevoelige en vertrouwelijke gegevens van de aanbieder. Dit is – zonder instemming – van de aanbieder niet wenselijk, met name vanuit de genoemde optiek van vertrouwelijkheid van informatie.

Dit is de kern van ons commentaar. Onderstaand volgt het verdere inhoudelijke commentaar op het wetsvoorstel.

[1] Wet Financieel Toezicht

Algemene opmerkingen bij het wetsvoorstel
Indien u dit wetsvoorstel wilt doorzetten, geven we onderstaande inhoudelijke reactie op het voorstel. Als u besluit de richting van een *Manifest van Samenwerking* in te slaan, dan dringen we er ook op aan rekening te houden met onderstaande aanbevelingen.

De meeste van de genoemde punten zouden ook aandachtspunten kunnen zijn die aandacht krijgen in de Algemene Maatregel van Bestuur (AMvB) per sector.

- *Onduidelijkheid wetsvoorstel*
  Het is van groot belang dat de onderliggende AMvB voor de financiële sector in goed overleg met de sector zal worden ingevuld. Het wetsvoorstel is op zich erg vaag.
  Wij adviseren in ieder geval een eigen AMvB voor de financiële sector. Het wetsvoorstel spreekt van 'een ICT-inbreuk die in belangrijke mate leidt of kan leiden tot een inbreuk op de veiligheid of een verlies van integriteit'. Belangrijke mate dient o.i. te worden gekoppeld aan de vitale functies van de banken: betalings- en effectenverkeer. Het is wenselijk zo concreet mogelijk te benoemen wanneer "in belangrijke mate" sprake is van een inbreuk op deze veiligheid en hoe moet worden omgegaan met de term "kan leiden". De invulling zal niet moeten leiden tot te veel meldingen die in tweede instantie blijken "mee te vallen".
- *Relatie met uitbreiding WBP betreffende data lekken*
  NVB en de Banken zien in feite twee wetten met een grote overlap, weliswaar met andere doelen. Er zijn behoorlijk wat inbreuken denkbaar op elektronische informatiesystemen die ook datalekken van persoonsgegevens tot gevolg hebben. Hoe waarborgen deze wetsvoorstellen dat sectoren niet met dubbele informatieverplichtingen komen te zitten?
- *Banken hebben al meldplicht over incidenten richting DNB;*
  Niet alleen banken, maar ook andere kritieke infrastructuren staat onder toezicht van door de overheid aangestelde toezichthouders. Hierbij hebben zij vaak al een meldplicht als het gaat om incidenten die aan bepaalde criteria voldoen. Dat is voldoende voor het uitoefenen van een zorgvuldig en betaalbaar toezicht. Uw opmerking over de beperkte toename van de administratieve lasten (zie ook bij de **inhoudelijke reactie** over administratieve lasten) is niet realistisch en in zijn algemeenheid veel te laag;
- *Beschikbaar stellen informatie*
  De NVB en de banken vinden het ongewenst dat een andere instantie dan de bank zelf (en in uitzonderlijke gevallen DNB) bepaalt of en zo ja welke gegevens beschikbaar worden gesteld aan derden en/of aan het publiek.
  Artikel 6 van het wetsvoorstel geeft de minister en feitelijk dus het NCSC de ruimte om naar eigen inzicht informatie aan andere bedrijven en zelfs het publiek door te geven. Aanbieders mogen niet terughoudend zijn met het leveren van inhoudelijke informatie. Banken en/of de NVB (afhankelijk van de situatie) dienen en zullen deze verantwoordelijkheid nemen.
  In de memorie van toelichting geeft de wetgever aan dat dit artikel de vertrouwelijkheid van informatie waarborgt. NVB en de banken dringen er op aan dat er minimaal een aanpassing dient te komen in de regelgeving over het openbaar maken van gegevens. Bijvoorbeeld zou de wet (of de AMvB) kunnen vastleggen dat als een instelling en het NCSC geen overeenstemming kunnen bereiken over publicatie van gegevens dit moet worden geëscaleerd naar de minister en de Raad van Bestuur van de betreffende instelling(en).
- *Onverwijld melden*
  Het wetsvoorstel spreekt over het "onverwijld" melden van incidenten. Dit zal niet altijd mogelijk zijn. Ten eerste is niet altijd direct bekend, dat een incident grootschalige gevolgen kan of gaat hebben. Ten tweede is op dat moment vaak slechts beperkt informatie beschikbaar. Tot slot (en daar is nu ervaring opgedaan bij de DDoS incidenten) betreft het vaak informatie uit een keten, beginnend bij de private sector die wordt getroffen, maar met links naar andere sectoren en naar de overheid. Het is niet altijd duidelijk waar informatie vandaan moet komen. En die informatie is ook niet altijd direct beschikbaar bij de aanbieder.
  Wij adviseren in de wet duidelijk onderscheid te maken tussen de termen onverwijld (is tijdig) melden en de volledigheid van de melding (gegeven de fase waarin de melding wordt gedaan)..

- *Welke informatie moet worden gedeeld?*
  In artikel 4 staat bij onverwijld melden ook, dat het NCSC onverwijld “alle overige gegevens die nodig zijn” kan opvragen. Dit is een vrijbrief om (bijna) alles op te vragen. Het is niet wenselijk dit toe te staan. NVB en banken gaan ervan uit dat overige op te vragen informatie ten hoogste wordt vastgesteld in onderling overleg;
- *Wie meldt?*
  Het wetsvoorstel gaat over het meldplicht door de aanbieder. Er dient een heldere scheidslijn te komen tussen aanbieder, afnemer en verantwoordelijkheden. Nu lijkt de verantwoordelijkheid te liggen bij de aanbieder, terwijl een andere partij in de keten nalatig kan zijn;
- *Verplicht hulp aan sectoren*
  Banken in Nederland beschikken over professionele IT en information security organisaties. Het is niet de rol van de overheid te bepalen waar en wanneer banken behoefte hebben aan hulp in geval banken met een incident worden geconfronteerd.
  De huidige samenwerking laat organisaties vrij om hulp te bieden of te vragen en dat is naar onze mening de enige manier waarop zo’n samenwerking succesvol kan zijn;
- *Rol NCSC*
  De rol van het NCSC ligt op de in het wetsvoorstel genoemde punten niet vast. Welke formele rol heeft het NCSC bij de ondersteuning van bedrijven? Wat is precies de rol van het NCSC in het maken van risico inschattingen?
- *Just culture*
  De banken ondersteunen – en zijn ook voortrekkers geweest – van een veiligheidscultuur waarin het leren van incidenten vooropstaat. Dit wordt in het wetsvoorstel “*just culture”* genoemd. Het hele wetsvoorstel is in feite strijdig met deze “just culture” gedachte.
- *Meldplichtige partijen*
  Hoe worden in deze wet partijen als Google, Paypal, Marktplaats, etc.. meegenomen? Vallen deze partijen ook onder deze wet?

Inhoudelijke reactie bij generieke deel Memorie van Toelichting

Memorie van Toelichting; punt 2. Algemeen

Wij onderschrijven de doelstelling hier genoemd, om de meldplicht zo licht als mogelijk te houden. Doelstelling van de samenwerking in het NCSC is primair kennisdeling en wederzijdse hulp.
De opmerking die daarbij wel dient te worden gemaakt, is dat de uitwisseling, zoals die nu plaats vindt, gebeurt onder het zogenoemde *“Traffic Light Protocol” (TLP)*. De zender bepaalt daarbij de mate van vertrouwelijkheid van de informatie en bepaalt daarmee ook, in hoeverre de informatie buiten de sector kan en mag worden gedeeld. Uiteraard zal het TLP binnen redelijkheid moeten worden gebruikt. Dat is ook de huidige praktijk.

Memorie van Toelichting; punt 2. Meldplichtige partijen

Wij adviseren hierbij aan te sluiten op de producten en diensten die ook al vanuit de optiek vitaal worden meegenomen. Dit is ook het uitgangspunt bij het Alerteringssyteem Terrorismebestrijding. De NVB verwacht dat de “grenzen” van de huidige producten en diensten die vitaal zijn, opnieuw worden bekeken, ook voor het ATb. We gaan ervan uit, dat de genoemde aanwijzing in overleg met de sector zal plaatsvinden.

Memorie van Toelichting; punt 2. Vertrouwelijkheid

In deze paragraaf wordt gewezen op het belang van vertrouwelijkheid. Artikel 6 van de wetgeving gaat hierop in.
Daarmee geeft het wetsvoorstel aan, dat vertrouwelijkheid belangrijk is. De NVB en de banken zijn, zoals al eerder in deze reactie is aangegeven, bezorgd over de opvraagbaarheid van gedetailleerde, vertrouwelijke informatie. De NVB en de banken zien graag meer duidelijkheid over informatie die wel en die niet opvraagbaar is.

Memorie van Toelichting; punt 2. Sectorale meldplichten; verhouding tot wetsvoorstel meldplicht datalekken en verhouding tot EU-richtlijnen

In de memorie van Toelichting wordt aandacht besteed aan de administratieve lasten door verschillende Nederlandse wetgeving, als ook op Europese wetgeving rond data inbreuken en security inbreuken.
Op dit moment is e.e.a niet concreet te maken. We verwachten – en rekenen op – grote zorgvuldigheid ten aanzien van de administratieve lasten, maar ook ten opzichte van een Europees level playing field. Het is niet wenselijk dat in Nederland veel zwaardere eisen gelden, die leiden tot hogere lasten voor de Nederlandse financiële sector (en andere sectoren), vergeleken met het buitenland.
Memorie van Toelichting 4: Administratieve lasten
NVB en de banken ondersteunen het uitgangspunt van minimale extra administratieve lasten.
Wij herkennen ons niet in de gemaakte rekensom. Op het moment dat door het NCSC gevraagde informatie afwijkt van al eerder geleverde informatie, zullen – zeker bij serieuze inbreuken, waarbij veel informatie moet worden verzameld en gedeeld – de kosten per incident aanzienlijk zijn.
Wij adviseren deze informatie niet te concretiseren in deze regelgeving.

Per artikel. Memorie van Toelichting en wetsvoorstel
Artikel 1 en 2
Banken en NVB gaan ervan uit, dat “aanwijzing met de betrokken bewindspersoon” voor de financiële sector inhoudt, dat de sector via het Ministerie van Financiën wordt betrokken bij deze aanwijzing.
Artikel 3
Hierboven is al uitgebreid ingegaan op de constateringen dat de termen “in belangrijke mate”, “kan leiden” en “onverwijld” onvoldoende concreet zijn. Dit moet nader worden ingevuld.
De Memorie van Toelichting spreekt – wat de laatste term betreft – over “zo onverwijld als mogelijk”. Dat laatste lijkt een betere term.
Artikel 3 en 4
De wetgeving op dit punt is duidelijk. De Memorie van Toelichting dient te kunnen melden, dat de additionele informatie die het NCSC vraagt, tot stand komt in overleg met de sector, in ons geval de NVB en de banken.
Verder zouden de NVB en de banken hier graag een nuancering willen zien over aan te leveren informatie en de waarborg van vertrouwelijkheid, ook in het kader van de WOB.
Artikel 5
Waarvan acte. Wij onderschrijven het belang dat de AMvB goed duidelijk moet maken in welke gevallen deze afspraken gelden en op welke wijze wordt bepaald welke extra informatie wordt – en kan worden – geleverd.
Artikel 6
Hier is in deze reactie al uitgebreid op ingegaan. Belangrijk vinden de NVB en de banken dan ook dat verzoeken u in deze paragraaf altijd in afstemming met de aanbieder en/of de sector te doen. De aanbieder/sector is immers de partij, die het meest weet wat er speelt.

Nederlandse Vereniging van Banken

We hopen onze punten van zorg op deze manier voldoende te hebben aangeduid en toegelicht. Uiteraard kunt u voor vragen met mij contact opnemen.

Met vriendelijke groet,

Wim Mijs
Directeur

Kopie
de heer W. van Gemert (Ministerie van V&J; directeur cyber security)