Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2012–2013

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

2113

Vragen van de leden **Dijkhoff** en **Aukje de Vries** (beiden VVD) aan de ministers van Veiligheid en Justitie en van Financiën over *het bericht «Banken te laks met de aanpak van cybercrime»* (ingezonden 20 maart 2013).

Antwoord van minister **Opstelten** (Veiligheid en Justitie) mede namens van minister van Financiën (ontvangen 1 mei 2013). Zie ook Aanhangsel Handelingen, vergaderjaar 2012–2013, nr. 1939.

Vraag 1
Kent u het bericht «Banken te laks met aanpak van cybercrime»?[1]

Antwoord 1
Ja.

Vraag 2 en 3
Waarom werken de banken volgens u onvoldoende mee aan het tegengaan van cybercriminaliteit terwijl de Nederlandse Vereniging van Banken (NVB) aangeeft zich niet in uw kritiek te herkennen? Kunt u de verschillen in opvatting verklaren?
Wat is voor u de aanleiding geweest een werkgroep in te richten om digitale aanvallen op bankrekeningen van consumenten tegen te gaan terwijl sinds 2011 de Korps landelijke Politiediensten (KLPD), het Landelijk Parket, de banken en Centre for Protection of the National Infrastructure (CPNI.NL) samenwerken in de Electronic Crimes Taskforce (ECTF) die zich richt op het voorkomen en aanpakken van digitale criminaliteit zoals fraude met internet-bankieren? Wat is de toegevoegde waarde van de werkgroep? Waarom bent u niet tevreden over de houding van de banken in dit overleg?

Antwoord 2 en 3
De samenwerking met de bankensector is goed. Er zijn geregeld contacten, ook op technisch niveau, als het gaat om detectie. Technische maatregelen leveren ook successen op: de Nederlandse Vereniging van Banken heeft op 2 april 2013 bericht dat de fraude met internetbankieren in de tweede helft van 2012 met 60% is gedaald ten opzichte van de eerste helft van 2012.[2]

[1] Financieel Dagblad, 15 maart 2013
[2] http://www.nvb.nl/nieuws/2013/1812/scherpe-daling-fraude-internetbankieren.html

ah-tk-20122013-2113
ISSN 0921 - 7398
's-Gravenhage 2013

Gezien de ernst van de dreiging van cybercrime moet evenwel over de hele linie een nog grotere inspanning dan nu al het geval is worden geleverd, ook door de bancaire sector. Ik wil de samenwerking verder uitbouwen en gezamenlijk optrekken om de huidige en komende problemen het hoofd te bieden. Er is met name winst te behalen in de operationele samenwerking met het bedrijfsleven. Samen met het bedrijfsleven, waaronder de banken, ga ik daarom de komende jaren investeren in verbeterde signalering, detectie en informatie-uitwisseling. Er is hierover geen verschil van opvatting, zoals onder andere mag blijken uit de brief die de Minister van Financiën en ik uw Kamer op 16 april 2013 stuurden naar aanleiding van de recente DDOS-aanvallen op enkele Nederlandse banken en de operationele maatregelen die wij naar aanleiding daarvan in ons onderlinge overleg van 15 april 2013 hebben genomen. Zoals vermeld in deze brief zal door de banken een liaison in het Nationaal Cyber Security Centrum worden geplaatst om de intensieve samenwerking te bestendigen.
Met de groep publieke en private partijen die in het in vraag 1 aangehaalde bericht wordt genoemd, doelde ik op de bestaande Electronic Crimes Taskforce (ECTF).

Vraag 4
Welke afspraken zijn er gemaakt tussen de overheid en de banken over de aanpak van cybercrime? Komen de banken de gemaakte afspraken na? Zijn volgens u de gemaakte afspraken voldoende om cybercrime te bestrijden, zo nee, op welke onderdelen zouden de afspraken moeten worden aangepast?

Antwoord 4
Banken en overheid werken in de strijd tegen cybercrime op vele verschillende fronten met elkaar samen, onder andere in verbanden zoals de ECTF en het skimmingpoint. De daar gemaakte afspraken worden nagekomen door de deelnemende partijen. Daarnaast wordt door de financiële sector op constructieve wijze samengewerkt binnen het Information Sharing and Analysis Centre (ISAC) voor de financiële sector. Deze Financial-ISAC, waarbinnen publieke en private partijen samenwerken door het delen van informatie en kennis over ICT-kwetsbaarheden en -dreigingen in het digitale domein, is aangesloten bij het Nationaal Cyber Security Centrum (NCSC).
Een terrein waar nog winst te boeken valt is het werken met zogenaamde barrièremodellen. Bij het werken met barrièremodellen heeft de overheid een leidende rol. Binnen een barrièremodel wordt gedetailleerd bekeken hoe een criminele organisatie of een crimineel verdienmodel werkt. Hierdoor kan worden nagegaan waar de criminele organisatie of het criminele model het meest kwetsbaar is. Op basis daarvan kan worden bepaald welke partij uit het samenwerkingsverband zo effectief mogelijk kan ingrijpen. Opsporing en vervolging zijn ultimum remedium. Eerst moeten we er met elkaar alles aan hebben gedaan om zaken veiliger te maken en gebruikers bewuster. Ik verwijs verder naar mijn antwoord op vragen 2 en 3.

Vraag 5
Klopt het dat sinds vorig jaar banken datalekken en hackersaanvallen verplicht moeten melden? Zo ja, hebben de banken zich aan de meldplicht gehouden? Heeft u zich al een keer genoodzaakt gezien uw bevoegdheden aan te wenden omdat banken zich niet hielden aan de meldplicht, zo ja, kunt u toelichten in welke situaties hier sprake van is geweest?

Antwoord 5
Banken moeten al geruime tijd op grond van de Wet op het financieel toezicht (Wft) incidenten verplicht melden aan De Nederlandse Bank (DNB). Een incident op grond van de Wft is een gedraging of gebeurtenis die een ernstig gevaar vormt voor de integere bedrijfsuitoefening. Datalekken en hackersaanvallen die kwalificeren als incident, moeten dus worden gemeld aan DNB. Voor zover DNB kan overzien wordt de meldplicht door de banken nageleefd. DNB ontvangt enkele meldingen per jaar van DDOS-aanvallen op Nederlandse banken.
In aanvulling op de hiervoor beschreven meldplicht wordt momenteel door het ministerie van Veiligheid en Justitie gewerkt aan twee wetsvoorstellen. In het eerste wetsvoorstel worden onder andere banken verplicht om datalekken (inbreuken op beveiligingsmaatregelen voor persoonsgegevens) te melden

aan het College bescherming persoonsgegeven (CBP). In het tweede wetsvoorstel worden banken verplicht om inbreuken op de veiligheid en integriteit van hun informatiesystemen die het betalings- of effectenverkeer onderbreken en een (potentieel) maatschappelijk ontwrichtende werking hebben, te melden aan het NCSC (dit betreft de security breach notification).

Vraag 6
Vormt naming en shaming een risico ten opzichte van het belang via het Nationaal Cyber Security Centrum (NCSC) te weten welke aanvallen en lekken er zijn om gerichter de cybercrime te kunnen aanpakken en meer kennis te kunnen vergaren? Is het te verkiezen dat bedrijven in vertrouwen hun lekken kunnen melden in plaats van verzwijgen uit angst voor negatieve publiciteit?

Antwoord 6
Naming en shaming zijn geen onderdeel van uitgangspunten van de security breach notification die ik naar aanleiding van de motie Hennis-Plasschaert[3], in samenwerking met het Ministerie van Financiën, aan het uitwerken ben. Het is van belang om informatie te delen met het NCSC zodat gewerkt kan worden aan het verminderen van kwetsbaarheden en indien noodzakelijk hulp geboden kan worden. In mijn brief van 6 juli 2012[4] heb ik dan ook aangegeven dat vertrouwelijkheid en de door het NCSC te bieden hulp belangrijke uitgangspunten zijn bij de uitwerking van de wettelijke meldplicht. Het wetsvoorstel hieromtrent zal spoedig in consultatie gebracht worden.

[3] Kamerstukken II, vergaderjaar 2011–2012, 26 643, nr. 202 herdruk.
[4] Kamerstukken II, vergaderjaar 2011–2012, 26 649, nr. 247.