Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2013–2014

Aanhangsel van de Handelingen

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

1072

Vragen van de leden **Nijboer** en **Oosenbrug** (beiden PvdA) aan de Ministers van Financiën en van Veiligheid en Justitie over *de gevoeligheid voor cyberaanvallen van Nederlandse banken* (Ingezonden 23 april 2013).

Antwoord van Minister **Dijsselbloem** (Financiën), mede namens de Minister van Veiligheid en Justitie (ontvangen 30 januari 2014)

Vraag 1
Bent u bekend met het artikel «Eurocommissaris Kroes: Bank laks met beveiligen»?[1]

Antwoord 1
Ja.

Vraag 2
Bent u het ermee eens dat de zekerheid en veiligheid van online betalen en bankieren geborgd moeten zijn, zeker in een tijd dat steeds meer betalingen digitaal plaatsvinden? Zo ja, hoe is dit geborgd in het beleid van het kabinet in samenspraak met de sector en de toezichthouders?

Antwoord 2
Veilig kunnen betalen is een noodzakelijke randvoorwaarde voor het behouden van het vertrouwen in het elektronisch betalingsverkeer. Zowel banken, als toezichthouder DNB en ikzelf zijn daarvan doordrongen. De robuustheid van het elektronisch betalingsverkeer wordt tevens gemonitord door het Maatschappelijk Overleg Betalingsverkeer. De meest recente uiting daarvan is het rapport «Analyse van de robuustheid van het elektronisch betalingsverkeer», dat in november 2013 aan u is aangeboden.

Vraag 3
Hoeveel storingen in het online betalingsverkeer van de Nederlandse banken zijn bij u bekend sinds 1 januari 2013 en wat was de totale en gemiddelde storingsduur?

[1] «Eurocommissaris Kroes: Bank laks met beveiligen», De Telegraaf, Pagina 11, 19 april 2013

ah-tk-20132014-1072
ISSN 0921 - 7398
's-Gravenhage 2014

Antwoord 3
Als gevolg van de DDOS-aanvallen hebben zich in het verleden diverse storingen in de internetbankieromgeving voorgedaan. De gemiddelde storingsduur is mij niet bekend. Wel is een nadere toelichting op de storingen die hebben plaatsgevonden in het voorjaar van 2013 opgenomen in een brief aan Uw Kamer, dd 16 april 2013[2].

Vraag 4
Kunt u een inschatting maken van de maatschappelijke kosten van de storingen in het online betalingsverkeer sinds 1 januari 2013?

Antwoord 4
Een inschatting van de maatschappelijke kosten is moeilijk te maken. Anders dan bij een storing in bijvoorbeeld het energienet, is het niet zo dat bij een storing in een bepaald betaalkanaal, bijvoorbeeld een storing bij het pinnen, bijna per definitie sprake is van schade. Zo is het bij een pinstoring vaak nog mogelijk om te betalen met een andere betaalwijze. Een alternatief voor een pintransactie is bijvoorbeeld een creditcard-transactie of het betalen met contant geld. In de rapportage «Analyse van de robuustheid van het betalingsverkeer», opgesteld in opdracht van het Maatschappelijk Overleg Betalingsverkeer en aan u aangeboden begin november 2013, is meer informatie opgenomen over de vraag welke betaalkanalen geheel of gedeeltelijk een alternatief voor elkaar kunnen vormen.

Vraag 5
Hoeveel geld hebben de vier grootste Nederlandse banken sinds 1 januari 2012 uitgetrokken ter beveiliging van het online betalingsverkeer?

Antwoord 5
In de rondetafelbijeenkomst die u op 31 mei 2013 hebt gehouden is als ik mij goed herinner door de banken een ruwe schatting gedaan van de kosten van beveiliging van het online betalingsverkeer. Dit zou neerkomen op 70 tot 100 miljoen euro per jaar. In dit bedrag zijn dan nog geen personeelskosten begrepen.

Vraag 6
Hebben Nederlandse banken een meldingsplicht aan de Nederlandsche Bank en/of het National Cyber Security Centrum (NCSC) bij een digitale storing of cyberaanval? Zo ja, hoe is deze vormgegeven? Zo nee, waarom niet?

Antwoord 6
Ja. Zoals is aangegeven in de beantwoording van vragen van de leden Dijkhoff en de Vries d.d. 25 april d.d. 2013 hebben banken reeds geruime tijd op grond van de Wet op het financieel toezicht de verplichting om incidenten aan DNB te melden. 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. DNB ontvangt enkele meldingen per jaar van bijvoorbeeld DDOS-aanvallen op Nederlandse banken.
In 2013 bestond op het moment van de DDoS-aanvallen nog geen formele meldplicht aan het NCSC. Inmiddels is een wetsvoorstel in consultatie gebracht dat gaat over het melden van security breaches. De Tweede Kamer is d.d. 13 december 2013 nader geïnformeerd over dit wetgevingstraject.

Vraag 7
Welke eisen vloeien voort uit de wet of worden gesteld door de Nederlandsche Bank aan de veiligheid en beveiliging van de digitale infrastructuur en het online betalingsverkeer van Nederlandse banken en hoe wordt daar toezicht op gehouden?

---

[2] Brief van de Ministers van Financiën en van Veiligheid en Justitie, Kamerstukken II, 2012–2013, nr. 28 684, nr. 379.

Antwoord 7
DNB houdt in het reguliere toezicht op instellingen in het oog of die instellingen een integere en beheerste bedrijfsuitoefening hebben. Daarbij wordt onder meer meegenomen of de banken voldoen aan de aanbevelingen die de Europese Centrale Bank op dit punt heeft afgekondigd[3]. Vanuit haar oversight-taak ziet DNB er eveneens op toe dat het betalingsverkeer goed blijft functioneren. In de nog bij het parlement in te dienen Wijzigingswet Financiële Markten 2015 heb ik een expliciete grondslag opgenomen op basis waarvan nadere regels kunnen worden gesteld om de goede werking van het betalingsverkeer te borgen. Ik heb dit nader toegelicht in de brief die ik u in november 2013 heb gezonden[4].

Vraag 8
Deelt u de opvatting van eurocommissaris Kroes dat door de uitwisseling van informatie op het gebied van cyberaanvallen deze effectiever kunnen worden aangepakt? Zo ja, hoe staat u tegenover een uitwisseling van informatie op dit punt in nationaal of Europees verband en op welke wijze kan het NCSC mogelijk aan deze uitwisseling bijdragen? Zo nee, waarom niet?

Antwoord 8
Ja, in zijn algemeenheid is informatie-uitwisseling zowel op Nationaal als op Europees niveau van het grootste belang bij het bestrijden van cyberaanvallen. In diverse antwoorden op kamervragen (o.a. de beantwoording van de vragen van het lid Gesthuizen en de leden Oosenbrug en Recourt d.d. 7 mei 2013) is aangegeven dat het NCSC het centrale informatieknooppunt inzake informatie over cyberaanvallen in Nederland is. Uw Kamer is meest recentelijk d.d. 13 december 2013 geïnformeerd over de wijze waarop deze rol verder wordt vormgegeven.

[3] European Central Bank: «Recommendations for the security of internet payments», januari 2013, Frankfurt
[4] Kamerstukken II, 2013–2014, 27 863, nr. 52