Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2014–2015

Aanhangsel van de Handelingen

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

1195

Vragen van de leden **Nijboer** en **Oosenbrug** (beiden PvdA) aan de Ministers van Financiën en van Binnenlandse Zaken en Koninkrijksrelaties over *het artikel «Beveiligingslek banken maakte phishing mogelijk»* (ingezonden 14 januari 2015).

Antwoord van Minister **Dijsselbloem** (Financiën) (ontvangen 3 februari 2015).

Vraag 1
Bent u bekend met het artikel «Beveiligingslek banken maakte phishing mogelijk»?[1]

Antwoord 1
Ja.

Vraag 2
Deelt u de mening dat het onacceptabel is dat de websites van banken zo eenvoudig aan te passen zijn door kwaadwillenden? Bent u er ook zo van geschrokken dat bij alle grote Nederlandse consumentenbanken dit beveiligingslek is geconstateerd?

Antwoord 2
De websites van banken dienen robuust te zijn en een veilig betalingsverkeer te waarborgen. Het is goed dat de onderzoeker het betreffende lek heeft gemeld. Dit maakt dat banken maatregelen kunnen nemen om het probleem te verhelpen. De Nederlandse banken en de overheid spannen zich in om een zo veilig mogelijke dienstverlening te leveren. De beveiliging zal in de praktijk echter nooit voor honderd procent waterdicht zijn.
De bancaire sector heeft onder meer een beleid voor *responsible disclosure* opgesteld en dit breed ingevoerd.[2] In dit openbaringsbeleid kunnen personen die kwetsbaarheden signaleren in een bancair systeem op een verantwoordelijke wijze dit melden bij de betreffende bank, waarna het vervolgens wordt opgelost. In deze casus is gehandeld conform het door de banken opgestelde *responsible disclosure* beleid.
Gezien de ontwikkeling van cyberdreigingen heeft DNB de eisen die zij stelt aan onder toezicht staande instellingen wat betreft de analyse en beheersing

[1] http://www.nu.nl/binnenland/3970812/beveiligingslek-banken-maakte-phishing-mogelijk.html
[2] Kamerstuk 26 643, nr. 342.

ah-tk-20142015-1195
ISSN 0921 - 7398
's-Gravenhage 2015

van IT-risico's vanaf dit jaar verzwaard. Banken moeten aantonen hun beheersprocessen continu te evalueren en (indien nodig) te verbeteren. De complexiteit van de IT-infrastructuur en de maatregelen die de detectie van en reactie op cyberdreigingen verbeteren, zijn daarbij belangrijke aandachtspunten.

Vraag 3
Is dit beveiligingslek gebruikt door criminelen voor phishingpraktijken? Volgens het artikel komen soortgelijke beveiligingslekken vaak voor; in hoeverre is die constatering correct? Bent u bekend met eerder gebruik van soortgelijke beveiligingslekken?

Antwoord 3
De banken testen zelf op beveiligingslekken en zorgen dat hun systemen regelmatig worden geüpdate. Banken nemen bij het testen voor de invoering van software mitigerende maatregelen om kwetsbaarheden in productie te voorkomen. Het probleem van de in het artikel genoemde «cross site scripting» is vaker geconstateerd en eerder aangepakt door de banken. De Betaalvereniging Nederland heeft aangegeven niet bekend te zijn met aanvallen waarin gebruik werd gemaakt van het aangekaarte lek of vergelijkbare lekken.

Vraag 4
Wordt er gegarandeerd dat iedere consument of ondernemer die middels deze phishingpraktijken gedupeerd is snel en volledig de schade door banken vergoed krijgt?

Antwoord 4
Volgens de Betaalvereniging Nederland zal bij de aangekaarte vorm van phising er niet snel sprake zijn van grove nalatigheid. Het uitgangspunt is dat indien consumenten schade leiden, de banken de schade vergoeden tenzij er sprake is van grove nalatigheid. Voor de beantwoording van deze vraag verwijs ik u graag naar de Kamerbrief «Initiatiefnota over veilig en betrouwbaar bankieren in de 21e eeuw» d.d. 18 december 2014.(Kamerstuk 34 033, nr. 3)

Vraag 5
Vindt u dat banken genoeg investeren in het beveiligen van hun ICT-infrastructuur? In hoeverre werken banken samen op het gebied van digitale beveiliging? Zijn banken verplicht beveiligingsproblemen die zij ontdekken te delen met concurrerende banken? Zou dit de veiligheid van online bankomgevingen ten goede kunnen komen?

Antwoord 5
Banken en andere schakels in het betalingsverkeer investeren in het beveiligen van de interbancaire infrastructuur. DNB beoordeelt als toezichthouder op de bedrijfsvoering van banken in hoeverre deze investeringen afdoende zijn. Banken bewaken zelf continu de veiligheid van hun websites en gebruiken tevens het *responsible disclosure* beleid hiervoor.
Het delen van informatie en samenwerking tussen banken op dit terrein vindt al plaats. Banken hebben diverse overleggen, waarin ze onderling, maar ook samen met de overheid overleggen over potentiële beveiligingsproblemen en mogelijk te nemen maatregelen. Hier wordt ook informatie gedeeld over het *responsible disclosure* beleid en de ervaringen hiermee.

Vraag 6
In het verleden heeft ook DigiD vergelijkbare beveiligingsproblemen gehad; in hoeverre zijn dit soort beveiligingsproblemen uit te sluiten? Hoe kwetsbaar zijn andere overheidsloketten, zoals van gemeentes, provincies en de politie?

Antwoord 6
Dergelijke beveiligingsproblemen zijn nooit helemaal uit te sluiten. Voor het veiliger ontwikkelen, beheren en aanbieden van webapplicaties en bijbehorende infrastructuur kunnen partijen binnen maar ook buiten de overheid gebruik maken van de ICT-beveiligingsrichtlijnen voor webapplicaties van het Nationaal Cyber Security Centrum (NCSC). Deze ICT- beveiligingsrichtlijnen

voor webapplicaties van het NCSC zijn in samenwerking met de Auditdienst Rijk (ADR), Logius, OWASP Nederland, Kwaliteitsinstituut Nederlandse Gemeenten (KING), Belastingdienst, diverse gemeenten en marktpartijen tot stand gekomen.[3]

[3] https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html