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

2947

Vragen van de leden **Verhoeven** en **Berndsen-Jansen** (beiden D66) aan de Minister van Veiligheid en Justitie over *het bericht dat hackers 1,2 miljard inloggegevens en 500 miljoen e-mailadressen hebben gestolen* (ingezonden 7 augustus 2014).

Antwoord van Minister **Opstelten** (Veiligheid en Justitie) (ontvangen 5 september 2014).

Vraag 1
Bent u bekend met het bericht «Hackers stelen 1,2 miljard inloggegevens en 500 miljoen e-mailadressen»?[1]

Antwoord 1
Ja.

Vraag 2
Kunt u de claim van cybersecurity bedrijf Holden Security bevestigen?

Antwoord 2
Deze claim kan ik bevestigen noch ontkennen. Behalve de mediaberichten is vooralsnog geen feitelijke informatie beschikbaar.

Vraag 3
Zijn er ook Nederlandse bedrijven, organisaties of overheidsinstellingen getroffen door de Russische hackers? Zo neen, kunt u ervoor zorgdragen dat het Nationaal Cyber Security Centrum dit zo snel mogelijk uitzoekt zodat de getroffen partijen de kwetsbaarheden op hun websites kunnen verhelpen en gebruikers geïnformeerd kunnen worden?

Antwoord 3
Het NCSC heeft direct contact gezocht met Hold Security om meer informatie te krijgen. Tot dusverre is door Hold Security geen gedetailleerde informatie gedeeld met het NCSC over de buitgemaakte data.
Buiten de mediaberichten is geen feitelijke informatie beschikbaar waardoor de precieze impact van de datadiefstal niet is vast te stellen. Het is daarmee

[1] Tweakers, 6 augustus 2014, http://tweakers.net/nieuws/97664/hackers-stelen-1-komma-2-miljard-inloggegevens-en-500-miljoen-e-mailadressen.html

ah-tk-20132014-2947
ISSN 0921 - 7398
's-Gravenhage 2014

onbekend welke organisaties en individuen mogelijk zijn geraakt, of hier Nederlandse partijen tussen zitten en via welke websites de gegevens zijn buitgemaakt.
Het NCSC staat conform haar reguliere rol in nauw contact met haar internationale partners om aanvullende informatie te verkrijgen. Op basis van de beperkt beschikbare feitelijke informatie heeft het NCSC haar doelgroep van rijksoverheid en vitale sectoren geïnformeerd.

Vraag 4
Hoe verhoudt deze situatie zich tot het wetsvoorstel meldplicht datalekken?[2] Moeten getroffen partijen dergelijke datalekken melden na inwerkingtreding van dit wetsvoorstel?

Antwoord 4
Het wetsvoorstel meldplicht datalekken strekt ertoe de huidige Wet bescherming persoonsgegevens (Wbp) te versterken. Naast de bestaande verplichtingen om persoonsgegevens op behoorlijke en zorgvuldige wijze te verwerken en op passende wijze tegen verlies of onrechtmatige verwerking te beveiligen, zal de Wbp – na inwerkingtreding van dit wetsvoorstel – een verplichting bevatten om inbreuken op de beveiliging van persoonsgegevens te melden aan de toezichthoudende instantie (College bescherming persoonsgegevens) en aan de getroffen personen. Van belang is dat deze meldingen onverwijld geschieden, opdat zo snel mogelijk duidelijk wordt welke maatregelen de getroffen organisatie heeft genomen of voorstelt te nemen om de negatieve gevolgen van de inbreuk te verhelpen. Daarnaast dient de getroffen organisatie aan te geven welke maatregelen de getroffen personen zelf kunnen nemen om de nadelige gevolgen van de inbreuk te beperken. Hierbij kan worden gedacht aan het wijzigen van wachtwoorden. Niet ieder denkbaar datalek valt onder de wettelijke meldplicht. Of een datalek moet worden gemeld is afhankelijk van de aard en de omvang van de inbreuk en de aard van de getroffen persoonsgegevens. Dit is ter beoordeling van de individuele verantwoordelijke. In zijn algemeenheid geldt dat bij een hack als waarvan in de berichtgeving sprake is, waarbij inloggegevens en emailadressen zouden zijn buitgemaakt, een melding al snel gepast zal zijn in verband met risico's op misbruik van deze persoonsgegevens, zoals identiteitsfraude en andere vormen van (financiële) fraude.

Vraag 5
Kunt u aangeven of het Nationaal Cyber Security Centrum reeds op de hoogte is van de kwetsbaarheden die mogelijk aanwezig zijn geweest zowel voor het aanleggen van het botnet als voor de extractie van database gegevens via SQL-injectie? Gaat het hier om voorheen onbekende kwetsbaarheden of reeds bekende kwetsbaarheden die nog niet verholpen waren?

Antwoord 5
Buiten de mediaberichten is geen feitelijke informatie beschikbaar waardoor niet aan te geven is of de informatie daadwerkelijk via SQL-injectie verkregen is. In de media wordt aangegeven dat criminelen de gegevens zouden hebben verkregen van ruim 400.000 verschillende websites afkomstig uit zowel de VS als daarbuiten. De gegevens zouden onder andere zijn buitgemaakt door misbruik te maken van SQL-injectie, een veel voorkomende kwetsbaarheid die aanwezig was (en mogelijk nog is) in de betreffende 400.000 websites.

Vraag 6
In hoeverre kan een eventuele vorm van terughacken een rol spelen bij het beperken van de schade als deze van botnet?

Antwoord 6
Gezien de tot nu toe bekende informatie is weinig te zeggen of in dit bijzondere geval binnendringen in deze geautomatiseerde werken een rol zou kunnen spelen bij het beperken van de schade die is ontstaan door het gebruik van het botnet. In het algemeen kan wel gesteld worden dat de

[2] Kamerstuk 33 662

uitbreiding van de mogelijkheden voor politie en Openbaar Ministerie die deel uitmaken van het wetsvoorstel Cybercrime III in de toekomst bij zullen dragen aan de bestrijding van botnets. In het bijzonder het binnen dringen in een geautomatiseerd werk geeft de mogelijkheid om bijvoorbeeld command en controlservers van botnets te onderzoeken en zonodig uit te schakelen. Daarna kan ook in kaart gebracht worden welke computers in het botnet zitten en kan verdere actie genomen worden om deze computers daar uit te (laten) verwijderen. Dit zal dan zeker bijdragen aan het beperken van de schade.