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

2429

Vragen van de leden **Van Oosten** en **Dijkhoff** (beiden VVD) aan de Staatssecretaris van Veiligheid en Justitie over *ftp-servers die onvoldoende beveiligd zijn waardoor privégegevens van burgers te zien zijn* (ingezonden 14 mei 2014).

Antwoord van Minister **Opstelten** (Veiligheid en Justitie) (ontvangen 3 juli 2014). Zie ook Aanhangsel Handelingen, vergaderjaar 2013–2014, nr. 2155.

Vraag 1
Heeft u kennisgenomen van de uitzending van Reporter Radio waarin naar voren komt dat ftp-servers onvoldoende beveiligd zijn, waardoor privacygevoelige gegevens van duizenden burgers en bedrijven door iedereen in te zien zouden zijn?[1]

Antwoord 1
Ja.

Vraag 2 en 3
Klopt het dat privégegevens van burgers en bedrijven misbruikt kunnen worden door slecht beveiligde ftp- servers? Zijn er bij u gevallen bekend van burgers en/of bedrijven die de dupe zijn geworden van misbruik van gegevens die zijn opgevraagd bij slecht beveiligde ftp-servers? Zo ja, om hoeveel gevallen van misbruik gaat het? Om hoeveel gevallen van onbeveiligde servers gaat het?
Welke (juridische) waarborgen zijn er om de privacygegevens van burgers op ftp-servers te beschermen?

Antwoord 2 en 3
Ja, het is mogelijk dat gegevens die op een slecht of onbeveiligde ftp-server worden geplaatst door kwaadwillenden worden misbruikt. Hierbij dient te worden bedacht dat informatiebeveiliging primair een eigen verantwoordelijkheid van burgers, bedrijven en overheden is. Daar waar gewerkt wordt met persoonsgegevens geldt in generieke zin het kader van de Wet bescherming persoonsgegevens (Wbp). In aanvulling hierop kan afhankelijk van de sector sprake zijn van aanvullende sectorale wet- en regelgeving. Overigens geldt

[1] Reporter Radio, 11 mei 2014 (http://www.radio1.nl/item/194795-Een%20fraudegevoelig%20digitaal%20lek.html)

ah-tk-20132014-2429
ISSN 0921 - 7398
's-Gravenhage 2014

voor gegevensopslag en -verwerking met behulp van deze servers in de privésfeer dat de Wbp niet van toepassing is (uitzondering voor activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden, art. 2, tweede lid, onder a, Wbp).
Alle bedrijven en overheden die persoonsgegevens verwerken moeten aan de eisen van de Wbp voldoen. Zo ook aan artikel 13 dat gaat over het adequaat beveiligen van persoonsgegevens. Dit betekent het nemen van passende technische en organisatorische maatregelen, rekening houdend met de stand van de techniek en afgezet tegen de risico's die met de specifieke gegevensverwerking(en) zijn gemoeid.
Het CBP heeft richtsnoeren uitgebracht over beveiliging van persoonsgegevens. Deze richtsnoeren leggen uit hoe het CBP bij het onderzoeken en beoordelen van beveiliging van persoonsgegevens in individuele gevallen de beveiligingsnormen uit de Wbp toepast. De richtsnoeren vormen de verbindende schakel tussen enerzijds het juridisch domein, met daarbinnen de eisen uit de Wbp, en anderzijds het domein van de informatiebeveiliging, waarin de noodzakelijke kennis en kunde aanwezig is om daadwerkelijk aan die eisen te voldoen. Het CBP is met toezicht en handhaving van de Wbp belast.
Aanscherpingen van het juridisch kader inzake bescherming van persoonsgegevens zijn in voorbereiding, zowel op Europees niveau (algemene verordening gegevensbescherming) als op nationaal niveau (wijziging van de Wet bescherming persoonsgegevens in verband met de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens en de uitbreiding van de bestuurlijke boetebevoegdheid van het College bescherming persoonsgegevens).
Bij het Nationaal Cyber Security Centrum zijn door partijen binnen de doelgroep van Rijksoverheid en vitale sectoren geen meldingen gedaan van partijen die getroffen zijn door misbruik van gegevens naar aanleiding van het gebruik van slecht beveiligde of onbeveiligde FTP-servers.
De omvang van het aantal onbeveiligde servers valt niet exact aan te geven. Middels op het internet beschikbare zoeksystemen kunnen, zoals in de uitzending benadrukt wordt, inderdaad lijsten met FTP-servers geïndexeerd worden. Het is echter onmogelijk om van deze servers, zonder deze te betreden, aan te geven of deze persoonsgegevens bevatten of dat het voor de aard van de informatie die op deze servers staat noodzakelijk is om hier beveiliging op toe te passen.

Vraag 4 en 5
Welke maatregelen nemen het ministerie en het Nationaal Cyber Security Centrum om burgers en bedrijven (beter) te beschermen tegen misbruik van slecht beveiligde ftp-servers? Welke verantwoordelijkheden hebben burgers om zelf hardware en software veilig in te richten?
Hoe beoordeelt u het standpunt van hoogleraar Cyber Security Bart Jacobs dat aanbieders van software voor ftp-servers gebruikers moeten waarschuwen voor de (potentiële) gevaren?

Antwoord 4 en 5
Vanuit het Ministerie van Veiligheid en Justitie en het daaronder ressorterende Nationaal Cyber Security Centrum (NCSC) wordt uitvoerig aandacht besteed aan het verhogen van de digitale weerbaarheid. Hiertoe is in oktober 2013 de tweede Nationale Cyber Security Strategie (NCSS-2) gepubliceerd. De NCSS-2 bevat een uitgebreid actieprogramma. Zo wordt onder meer ingezet op het verhogen van de bewustwording van burgers en bedrijven middels de jaarlijkse campagne Alert Online. De campagne Alert Online zal dit jaar van 27 oktober tot 6 november gehouden worden.
Dit jaar ligt de focus op kennis over cybersecurity, juist om partijen zelf in staat te stellen om de juiste acties te ondernemen.
Ten aanzien van onbeveiligde apparatuur, w.o. FTP-servers, dient opgemerkt te worden dat het NCSC hier met regelmaat in haar publicaties voor heeft gewaarschuwd. Een voorbeeld hiervan is de reeds in december 2012 gepubliceerde factsheet «beveilig apparaten gekoppeld aan internet».
Bedrijven en instellingen zijn zoals gezegd, zelf primair verantwoordelijk voor informatiebeveiliging en zoals in de NCSS-2 reeds aangegeven mag daarbij een zekere mate van basis-cyberhygiëne verwacht worden, bijvoorbeeld bij het omgaan met persoonlijke gegevens op het internet.

Tot slot kan ik aangeven dat ik de analyse van hoogleraar Bart Jacobs, tevens lid van de Cyber Security Raad, deel en dat deze aansluit op de in de NCSS-2 geschetste rol voor het bedrijfsleven als leverancier. De Cyber Security Raad heeft in haar advies bij het opstellen van de NCSS-2 vastgesteld dat er een nadrukkelijke interactie moet zijn tussen de aanbieders van producten en diensten en de gebruikers ervan, zeker als het gaat om de veiligheidsaspecten zoals het gebruik van sterke wachtwoorden of het hanteren van specifieke veiligheidsinstellingen op apparatuur. In de NCSS-2 is daarbij dan ook aangegeven dat leveranciers een specifieke verantwoordelijkheid (zorgplicht) richting hun klanten hebben en dat security en privacy by design meer dan nu standaard ontwerpbeginselen dienen te zijn.