Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2016–2017 **Aanhangsel van de Handelingen**

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

753

Vragen van de leden **Oosenbrug** en **Recourt** (beiden PvdA) aan de Minister van Veiligheid en Justitie over *het bericht «Niet melden cybercrime is vaak verstandiger»* (ingezonden 25 oktober 2016).

Antwoord van Minister **Van der Steur** (Veiligheid en Justitie) (ontvangen 14 december 2016). Zie ook Aanhangsel Handelingen, vergaderjaar 2016–2017, nr. 501.

Vraag 1
Kent u het bericht «Niet melden cybercrime is vaak verstandiger»?[1]

Antwoord 1
Ja.

Vraag 2
Hoe zijn de ervaringen, zowel van het bedrijfsleven als van de overheid, in landen waar al langer een meldplicht datalekken bestaat?

Antwoord 2
Beantwoording van deze vraag is complex omdat er geen centrale registratie wordt bijgehouden waaruit gegevens over andere landen te genereren zijn. Een overzicht op het detailniveau zoals gevraagd, zou een uitgebreid landen vergelijkend onderzoek vergen en dat is binnen het tijdsbestek voor de beantwoording van deze Kamervragen niet mogelijk. Ook is het lastig om landen onderling te vergelijken, omdat de situatie ten aanzien van cybercrime in landen erg verschillend kan zijn.

Vraag 3
Deelt u de mening dat «voorlichting» aan bedrijven van een ex-officier van justitie over de nadelen van een melding niet door de beugel kan? Zo nee, waarom niet?

Antwoord 3
De geïnterviewde persoon is reeds lange tijd werkzaam als advocaat en niet meer als officier van justitie. Het betreft derhalve geen voorlichtingsactiviteiten van het Openbaar Ministerie. Het melden van criminaliteit is van groot

[1] Financieel Dagblad 24 oktober 2016

ah-tk-20162017-753
ISSN 0921 - 7398
's-Gravenhage 2016

belang voor de aanpak ervan, zowel in individuele zaken als ten behoeve van de beleidsmatige aanpak.

Vraag 4
Klopt het beeld dat de advocaat schetst dat serieuze meldingen van cybercrime geen passend vervolg krijgen? Zo ja, hoe vaak wordt er opgetreden na een serieuze melding van cybercrime en hoe vaak heeft dat tot vervolging en een veroordeling geleid?

Antwoord 4
Het beeld dat er door het OM en de politie geen vervolg wordt gegeven aan serieuze cybercrime meldingen, herken ik niet. Uit het «Jaarbericht OM 2015» volgt dat er vorig jaar 32 complexe en 124 reguliere cybercrime onderzoeken zijn uitgevoerd.
In geval van een aangifte van cybercrime door een bedrijf maken het OM en de politie aan de hand van diverse criteria, zoals de aanwezigheid van opsporingsindicaties, de geleden schade en de mate van afscherming van de gepleegde strafbare feiten, de keuze aan welke onderzoeken en aangiftes vervolg kan worden gegeven. Cybercrimezaken met serieuze en ingrijpende implicaties zullen om die reden vrijwel altijd in onderzoek worden genomen. Het *niet*melden van serieuze cybercrimezaken is om die reden nooit verstandig.
Dat neemt niet weg dat opsporingsonderzoeken naar cybercrime vaak complexe onderzoeken zijn vanwege het feit dat de aanpak van cybercrime een steeds internationaler karakter krijgt en structureel moet worden samengewerkt met buitenlandse (opsporings-)autoriteiten. Ook de mate van afscherming en encryptie door criminelen is van dien aard dat het voor justitie en politie een steeds grotere uitdaging wordt om bewijs te verzamelen tegen een identificeerbare verdachte. Als een verdachte vervolgens is geïdentificeerd, is in diverse zaken gebleken dat deze zich in een buitenland bevindt, hetgeen de vervolging verder compliceert.
Ik herken mij derhalve niet in het beeld dat meldingen van serieuze cybercrime geen vervolg krijgen, maar de problematiek die samenhangt met deze vorm van criminaliteit brengt mee dat in een beperkt aantal van de onderzochte zaken in Nederland, een daadwerkelijke veroordeling van een identificeerbare verdachte volgt. Om meer zicht te krijgen op bewijsmateriaal en de verdachten die zich met dit soort serieuze cybercrime bezighouden, is het wetsvoorstel CCIII naar uw Kamer gestuurd.

Vraag 5
Wat is uw reactie op de uitspraak van de ex-officier van justitie waarin hij verwacht dat «steeds meer bedrijven het melden achterwege zullen laten»? Welke beleidsmatige consequenties verbindt u daaraan?

Antwoord 5
Om de indruk van straffeloosheid te voorkomen en daarmee toename van cybercrime tegen te gaan, is het in het belang van overheid, burger en bedrijven om slachtofferschap van criminaliteit te melden. Het blijft daarom belangrijk de aangiftebereidheid te bevorderen, bijvoorbeeld door middel van de bewustwordingscampagne «Alert Online». Melden van datalekken dient daarnaast het publieke belang van cyber Security en het private belang van degenen wier gegevens ongewenst zijn verspreid. Naleving van de regels ter zake onder andere door handhaving is het uitgangspunt.

Vraag 6
Gaat u de Autoriteit Persoonsgegevens (AP) extra middelen verschaffen om prioriteit te kunnen geven aan het doen van onderzoek naar het weloverwogen achterwege laten van een melding? Zo nee, waarom niet?

Antwoord 6
De AP monitort de effecten van de invoering van de meldplicht datalekken. Binnenkort bespreek ik de resultaten van de monitor over het eerste halfjaar van 2016 met de AP.

Vraag 7
Deelt u de mening dat, gezien de verwachting dat in 2021 de helft van de misdaden cybercrime-gerelateerd zal zijn, er bij beleidsmakers en in de strafrechtketen een forse inspanning nodig is om cybercriminelen aan te pakken? Zo ja, hoe gaat u dit vorm geven? Zo nee, waarom niet?[2]

Antwoord 7
Het inmiddels zesde Cyber security beeld Nederland 2016 en de daarbij behorende beleidsreactie[3] schetst de zorgelijke ontwikkeling in de periode van mei 2015 tot en met april 2016 van een toenemende en reële dreiging in het digitale domein. Deze dreigingen zijn onder andere gericht op diefstal van geld en kostbare commerciële informatie. Cybercriminelen hebben zich ontwikkeld tot zeer geavanceerde actoren wier capaciteiten in een aantal gevallen gelijk staan met die van staten. Cybercrime is daarmee zowel kwantitatief als kwalitatief een groeiend probleem voor de Nederlandse samenleving.
Met een doorontwikkeling van de cybersecurityaanpak en de gerichte aanpak van cybercriminaliteit moet Nederland de volgende stap zetten om in het digitale tijdperk mee te blijven komen. Overheid en bedrijfsleven moeten hierbij elk hun verantwoordelijkheid pakken. Het kabinet investeert vanaf 2017 structureel in cybersecurity en de aanpak van cybercrime. Daarnaast werkt de politie aan het verder opbouwen van de reeds voorziene capaciteit van technisch specialisten in de regionale eenheden.

Vraag 8
Kunt u de vragen beantwoorden vóór de plenaire behandeling in de Kamer van de begroting van uw ministerie voor het jaar 2017 (voorzien in week 48)?

Antwoord 8
Dat is niet gelukt.

[2] http://nos.nl/nieuwsuur/artikel/2111280-over-vijf-jaar-helft-misdaad-door-cybercriminelen.html
[3] Kamerstuk 30 977, nr. 63.