Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2016–2017

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 441

BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 23 januari 2017

Bij deze brief treft u, mede namens de Minister van Veiligheid en Justitie, de antwoorden aan op de vragen die de vaste commissie voor Binnenlandse Zaken op 22 december jl. heeft gesteld over het manipuleren van verkiezingen door hacks en nepnieuws. Bij de beantwoording van deze vragen heb ik ook de vragen meegenomen die zijn gesteld op 20 december jl. bij de regeling van werkzaamheden (Handelingen II 2016/17, nr. 37, item 34).

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
R.H.A. Plasterk

kst-26643-441
ISSN 0921 - 7371
's-Gravenhage 2017

Vragen en antwoorden

Vraag 1
Wat voor bedreigingen ziet het kabinet voor de organisatie van en het verloop van de komende Tweede Kamer verkiezingen door mogelijke manipulatie van de verkiezingen door middel van hacks of nepnieuws door buitenlandse mogendheden of andere kwaadwillenden?

Antwoord
Inmenging of beïnvloeding door statelijke actoren in/van onze verkiezingen is volstrekt ongewenst. De bescherming van de democratische rechtsorde, waarvan vrije en eerlijke verkiezingen cruciale pijlers zijn, is van vitaal belang.

Het kabinet kan niet uitsluiten dat statelijke actoren baat kunnen hebben bij beïnvloeding van de politieke besluitvorming en van de publieke opinie in Nederland en daartoe middelen zullen inzetten om te proberen die beïnvloeding ook te realiseren. De afgelopen jaren is in vele documenten heel duidelijk aangegeven dat het kabinet zich bewust is van dit risico. Ik verwijs hierbij naar de jaarverslagen van de AIVD en het Cybersecuritybeeld Nederland 2016 (CSBN 2016) (Kamerstuk 26 643, nr. 420) en de beleidsreactie daarop.

In aanloop naar de verkiezing van de leden van de Tweede Kamer moeten we daarom uiteraard zeer alert zijn en niet naïef denken dat in Nederland niets mogelijk is. Het vertrouwen in de integriteit van het verkiezingsproces is in Nederland groot waardoor ook de betrouwbaarheid van de uitslag van de verkiezing van de leden van de Tweede Kamer niet ter discussie wordt gesteld. Dat is een groot goed dat beschermd moet worden.

Het is dus zaak om goed te analyseren waar er kwetsbaarheden kunnen zijn. Ik denk hierbij aan:
- de organisatie van de verkiezing zelf, het stemproces en het proces om de uitslag te bepalen van de verkiezing van de leden van de Tweede Kamer;
- de fysieke en digitale beveiliging van personen;
- opinievorming en informatieverstrekking.

Die analyse voert het kabinet uiteraard uit, maar dat zouden ook alle organisaties moeten doen die op enigerlei wijze betrokken zijn bij de campagne in aanloop naar de verkiezing en bij de verkiezing zelf. Men is immers primair zelf verantwoordelijk voor de eigen (informatie)beveiliging. Waar dat moet en kan wordt er vanuit de rijksoverheid ondersteuning geleverd. Dat kan verschillende vormen hebben zoals de fysieke beveiliging van personen, maar het kan ook gaan om concrete suggesties om de beveiliging te verbeteren, door informatie te geven over hoe kwetsbaarheden kunnen worden geïdentificeerd, waar deskundigheid te vinden is voor het uitvoeren van penetratietesten, etc.
In de antwoorden op de volgende vragen wordt hier nader op ingegaan.

Vraag 2
Welke stappen onderneemt het kabinet om politieke partijen en politici te behoeden voor hacks door buitenlandse mogendheden of andere organisaties die de verkiezingen willen manipuleren?

Antwoord
Politieke partijen zijn uiteraard primair zelf verantwoordelijk voor het organiseren van hun informatiebeveiliging. Tegelijkertijd werkt het kabinet permanent aan het vergroten van het bewustzijn rondom cybersecurity, in het bijzonder ook in relatie tot de verkiezingen in maart 2017. Met het oog

daarop heeft de NCTV vanuit zowel fysiek als digitaal perspectief aandacht voor een veilig verloop van de campagneactiviteiten van de partijen die deelnemen aan de verkiezingen en van de dag van de verkiezing. De NCTV heeft in samenwerking met de Nederlandse inlichtingen- en veiligheidsdiensten specifiek ten aanzien van digitale veiligheid een bijeenkomst voor de ICT-verantwoordelijken van politieke partijen georganiseerd. Hierin zijn conform de reguliere werkwijze het dreigingsbeeld en handelingsperspectieven besproken. In gezamenlijkheid wordt bezien welke vervolgacties nodig zijn. Hierover kunnen in het openbaar geen verdere mededelingen worden gedaan.

Ook andere (reguliere) contacten met politieke partijen worden door het Ministerie van BZK benut om mogelijke risico's en kwetsbaarheden met de politieke partijen te bespreken.

Vraag 3
Welke stappen onderneemt het kabinet om manipulatie van de verkiezingen door middel van gehackte peilingen en nepnieuws te voorkomen?

Antwoord
In Nederland voeren private bedrijven opiniepeilingen uit. Deze bedrijven zijn zelf verantwoordelijk voor de beveiliging van hun infrastructuur, dus ook voor het voorkomen van hacks. De media bepalen zelf welke selectie zij uit het nieuwsaanbod maken. De media dienen daarbij zelf af te wegen of er sprake kan zijn van nepnieuws. De rol van de overheid beperkt zich, gelet op de onafhankelijkheid van de media, tot het stimuleren van awareness dat er nepnieuws kan worden verspreid.

Vraag 4
Is het kabinet bereid samen met de organisatie van de Tweede Kamer de veiligheid van het ICT- en mailsysteem van de Tweede Kamer te beoordelen op het gebied van cyberveiligheid?

Antwoord
Ja, uiteraard met inachtneming van de eigen verantwoordelijkheid van de Tweede Kamer voor de veiligheid van het eigen ICT- en mailsysteem. Het NCSC zal, indien het presidium dit verzoekt, de ICT-organisatie ondersteuning verlenen als het gaat om dreigingen en incidenten met betrekking tot de systemen van de Tweede Kamer (informeren, adviseren, bijstand bij het treffen van maatregelen).

Vraag 5
Is het kabinet zich bewust van concrete pogingen in het recente verleden om via hacks verkiezingen in Nederland te manipuleren?

Antwoord
Hiervoor zijn geen aanwijzingen.

Vraag 6
Is het verkiezingsproces zelf kwetsbaar voor hacks, bijvoorbeeld bij het doorgeven van de uitslag van stembureaus naar het hoofdstembureau en van de hoofdstembureaus naar het centraal stembureau? Welke maatregelen neemt het kabinet om de risico's in het verkiezingsproces te beperken?

Antwoord
Het stemproces en het proces om de uitslag van de verkiezing te berekenen zijn in beperkte mate gedigitaliseerd. Het stemmen door de kiezer en tellen van de stemmen die door de kiezer worden uitgebracht gebeurt sinds 2007 weer helemaal handmatig. Langs digitale weg hacken

van het stemmen en van het tellen van de stembiljetten in het stemlokaal is dus niet mogelijk.

Voor het berekenen van de uitslag wordt bij de verkiezing van de leden van de Tweede Kamer gebruik gemaakt van programmatuur[1] die in opdracht van het centraal stembureau, zijnde de Kiesraad[2], is ontwikkeld en wordt onderhouden. De Kiesraad is zelf uiteraard alert op de beveiliging (van het gebruik) van deze programmatuur.

De Kiesraad stelt de programmatuur beschikbaar aan de gemeenten en de hoofdstembureaus. De programmatuur wordt door de Kiesraad op CD-roms naar de gemeente gestuurd. Het Ministerie van BZK en de Kiesraad zullen in aanloop naar de verkiezing van de leden van de Tweede Kamer gemeenten en hoofdstembureaus uitdrukkelijk wijzen op de instructies die gelden voor het gebruik van de programmatuur die de Kiesraad ter beschikking stelt en op het belang van de naleving van de instructies. Zou er desondanks, om welke reden dan ook, aanleiding zijn om aan de integriteit van de gebruikte programmatuur te twijfelen, dan kan de juistheid van de berekende uitslag altijd worden gecontroleerd aan de hand van de uitkomsten van de tellingen die de stembureaus in het stemlokaal handmatig hebben uitgevoerd en die zijn vastgelegd in de (papieren) processen-verbaal van de stembureaus.

Vraag 7
Van hoeveel landelijke politici (Kamerleden en leden van het kabinet) heeft u aanwijzingen dat zij worden afgeluisterd of dat hun email gehacked wordt?

Antwoord
In het openbaar worden hierover geen mededelingen gedaan.

[1] OSV: Ondersteunde Software Verkiezingen
[2] De Kiesraad is centraal stembureau voor de verkiezingen van de leden van de Tweede Kamer, de leden van de Eerste Kamer en van de Nederlandse leden van het Europees parlement.