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

675

Vragen van de leden **Agnes Mulder**, **Van Helvert** en **Amhaouch** (allen CDA) aan de Ministers van Infrastructuur en Milieu en van Binnenlandse Zaken en Koninkrijksrelaties over *het bericht «Andere zorgen over kerncentrale Tihange»* (ingezonden 18 november 2016).

Antwoord van Minister **Schultz van Haegen-Maas Geesteranus** (Infrastructuur en Milieu) (ontvangen 6 december 2016).

Vraag 1
Bent u bekend met het bericht «Andere zorgen over kerncentrale Tihange»?[1]

Antwoord 1
Ja.

Vraag 2
Deelt u de mening dat het zeer alarmerend is dat de veiligheidsplannen van de kerncentrale op internet staan?

Antwoord 2
Ja. De beveiliging van informatie, primaire systemen e.d. moet optimaal zijn.

Vraag 3
Bent u van plan dit aan te kaarten bij uw Belgische collega aangezien er ook veel Nederlandse gemeenten zijn waarvan de veiligheid hierdoor in het geding komt? Kunt u de Kamer informeren over dit gesprek?

Antwoord 3
De ANVS heeft deze kwestie besproken met het FANC. Ik zal dit ook doen als ik contact heb met mijn Belgische collega Jambon.

Vraag 4
Zijn er normen of regels afgesproken ter beveiliging van computers bij organisaties en bedrijven die een groot risico kunnen vormen voor de nationale en internationale veiligheid zowel in Nederland, België, als in EU-verband? Zo nee, wat gaat u daar aan doen?

[1] De Limburger, 17 november 2016

ah-tk-20162017-675
ISSN 0921 - 7398
's-Gravenhage 2016

Antwoord 4
Ja. Er zijn voor de nucleaire sector regels vastgesteld voor de beveiliging van computers. Deze regels vloeien onder meer voort uit internationale aanbevelingen, zoals die van het Internationaal AtoomEnergie Agentschap (IAEA). Deze regels zijn opgenomen in de Regeling beveiliging nucleaire inrichtingen en splijtstoffen en de referentiescenario's Cyber Security (i.c. Design Basis Threat Cyber Security). De referentiescenario's worden momenteel geactualiseerd. De ANVS ziet toe op de naleving van deze regels.
Deze referentiescenario's worden opgesteld door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV)/Nationaal Cyber Security Centrum (NCSC), de Algemene Inlichtingen- en Veiligheid (AIVD), en de Landelijke Eenheid Politie. Met de nucleaire vergunninghouders wordt over deze regels overleg gevoerd.
Tot slot komt de nucleaire sector te vallen onder de onlangs in uw Kamer behandelde Wet gegevensverwerking en meldplicht cybersecurity (Kamerstuk 34 388). In deze wet wordt geregeld dat Nederlandse vitale sectoren vooraf gedefinieerde incidenten moeten melden aan het NCSC.
Cyberbeveiliging is in België een specifiek onderdeel van nucleaire beveiliging. Het wordt niet letterlijk vermeld in de wetteksten. In het Koninklijke Besluit van 17 oktober 2011, houdende de categorisering en de bescherming van nucleaire documenten, staat dat de exploitanten van de nucleaire installaties de nucleaire documenten (dus ook digitale documenten) moeten beschermen. Daarnaast was cyberbeveiliging opgenomen in de stresstests van 2011. Op basis daarvan hebben de exploitanten maatregelen genomen. Het Federaal Agentschap voor Nucleaire Controle (FANC) ziet erop toe dat deze maatregelen worden uitgevoerd.
Het FANC geeft aan dat de besturingssystemen in het nucleaire gedeelte van de kerncentrales analoog zijn en daarom niet zijn aangesloten op een (externe) server. Deze systemen zijn totaal geïsoleerd en kunnen dus nooit het onderwerp uitmaken van een cyberaanval.
Het FANC werkt hierbij intensief samen met het Centrum voor Cybersecurity België, de Belgische tegenhanger van de NCSC.

Vraag 5
Kunt u deze vragen vóór het Algemeen overleg Nucleiare veiligheid voorzien op 7 december 2016 beantwoorden?

Antwoord 5
Ja.