Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

Aanhangsel van de Handelingen

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

1517

Vragen van lid **Kathmann** (PvdA) aan de Ministers van Justitie en Veiligheid en van Economische Zaken en Klimaat en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over *het rapport Kwetsbaar door software – Lessen naar aanleiding van beveiligingslekken door software van Citrix* (ingezonden 20 december 2021).

Antwoord van Minister **Yeşilgöz-Zegerius** (Justitie en Veiligheid) en Minister **Adriaansens** (Economische Zaken en Klimaat) en Staatssecretaris **Van Huffelen** (Binnenlandse Zaken en Koninkrijksrelaties) (ontvangen 31 januari 2022). Zie ook Aanhangsel Handelingen, vergaderjaar 2021–2022, nr. 1338.

Vraag 1
Bent u bekend met het rapport van de Onderzoeksraad voor Veiligheid en het bericht *Fundamenteel ingrijpen is nodig voor Nederlandse digitale veiligheid*?[1]

Antwoord 1
Het kabinet is bekend met het rapport van de Onderzoeksraad voor Veiligheid OVV «Kwetsbaar door software – lessen naar aanleiding van beveiligingslekken door software van Citrix» en het bijbehorende bericht van de OVV. Zoals aangegeven in de Kamerbrief van 16 december 2021 zal het kabinet het rapport zorgvuldig bestuderen en binnen de wettelijke reactietermijn van zes maanden schriftelijk richting de OVV reageren. Uw Kamer zal daarover worden geïnformeerd.[2]

Vraag 2
Bent u het eens met de stelling dat de veiligheid van software allereerst de verantwoordelijkheid is van de softwarefabrikant en dat deze fabrikanten meer zouden moeten investeren om de veiligheid van software voortdurend te verbeteren? Zo nee, waarom niet? Zo ja, wat gaat u doen om te zorgen dat deze verantwoordelijkheid in de praktijk feitelijk bij softwarefabrikanten komt te liggen?

[1] Onderzoeksraad voor Veiligheid, 16 december 2021, Fundamenteel ingrijpen is nodig voor Nederlandse digitale veiligheid (https://www.onderzoeksraad.nl/nl/page/19862/fundamenteel-ingrijpen-is-nodig-voor-nederlandse-digitale-veiligheid)
[2] Kamerstuk 26 643, nr. 808

ah-tk-20212022-1517
ISSN 0921 - 7398
's-Gravenhage 2022

Antwoord 2
Zoals aangegeven in de Nederlandse Cybersecurity Agenda en de Roadmap Digitaal Veilige Hard- en Software zijn organisaties in de eerste plaats zelf verantwoordelijk voor cybersecurity. Voor softwarefabrikanten geldt dat zij primair verantwoordelijk zijn voor de digitale veiligheid van de door hen aangeboden producten en diensten. Daarnaast kunnen afnemers van ICT-producten en diensten (consumenten en organisaties) de vraag naar digitaal veilige ICT-producten en diensten stimuleren. Dit stimuleert aanbieders om te investeren in de digitale veiligheid van hun ICT-producten en diensten. De overheid staat voor de publieke belangen, stimuleert marktpartijen om hun eigen verantwoordelijkheid te nemen en is zelf ook een afnemer van ICT-producten en diensten. Zoals de OVV aangeeft zijn alle partijen van elkaar afhankelijk om de digitale veiligheid in de samenleving en economie te borgen. De afgelopen kabinetsperiode is met een samenhangend pakket aan maatregelen in de Roadmap Digitaal Veilige Hard- en Software ingezet op het verhogen van het digitale veiligheidsniveau van ICT-producten en diensten. Over de jaarlijkse voortgang van de Roadmap Digitaal Veilige Hard- en Software bent u geïnformeerd door de Minister van Economische Zaken en Klimaat op 30 november 2021.[3] Voorbeelden van maatregelen uit deze roadmap zijn de inzet van EZK voor de begin dit jaar gerealiseerde Europese cybersecurity markttoegangseisen voor draadloos verbonden apparaten onder de *Radio Equipement Directive*, de ontwikkeling van Europese cybersecurity certificering voor ICT-producten, diensten en processen onder de *Cyber Security Act*, een non-paper over de in ontwikkeling zijnde *Cyber Resilience Act* als horizontale Europese regulering voor de cybersecurity van ICT-producten en diensten en de door BZK en EZK ontwikkelde cybersecurity inkoopeisen voor alle overheidsorganisaties. De Roadmap Digitaal Veilige Hard- en Software is onderdeel van de rijksbrede Nederlandse Cybersecurity Agenda. Over de jaarlijkse voortgang van de Nederlandse Cybersecurity Agenda bent u voor het laatst geïnformeerd op 28 juni 2021.[4]
Daarnaast wordt momenteel gewerkt aan het ontwikkelen van een integrale Nederlandse Cybersecuritystrategie waarin met name ook de ambities uit het coalitieakkoord nader worden uitgewerkt. Deze strategie wordt zodra gereed met uw Kamer gedeeld. De digitale veiligheid van ICT-producten en diensten zal hier integraal onderdeel van zijn. Ook zal uiteraard worden bezien op welke wijze het kabinet de verschillende aanbevelingen van de OVV kan meenemen ten behoeve van de ontwikkeling van deze strategie en het verder versterken van het cybersecuritystelsel in Nederland en Europa.

Vraag 3
Hoe gaat u invulling geven aan het advies om een voortrekkersrol te nemen voor Nederlandse organisaties en consumenten om gezamenlijk veiligheidseisen te formuleren en af te dwingen bij softwarefabrikanten?

Antwoord 3
Zoals aangegeven bij vraag 1 is het kabinet het OVV-rapport zorgvuldig aan het bestuderen en zal het voor de zomer hierop een kabinetsreactie geven. Het rapport van de OVV laat zien dat cybersecurity een complex vraagstuk is en de aanbevelingen van de OVV in samenhang moeten worden bezien. Er is niet één afzonderlijke maatregel die de digitale veiligheid kan realiseren. Bij de besluitvorming over de opvolging van deze aanbeveling zal het bestaande instrumentarium in volle breedte in ogenschouw moeten worden genomen. Een voorbeeld hiervan is de Baseline Informatiebeveiliging Overheid (BIO), die van kracht is op de aanschaf van ICT-producten en diensten door de overheid. De BIO schrijft voor dat overheidsorganisaties ook bij inkoop op basis van risicomanagement bepalen aan welke veiligheidseisen bijvoorbeeld ICT-producten en -diensten moeten voldoen. Om hen daarbij te helpen, hebben de Ministeries van BZK en EZK gezamenlijk een inkoophulpmiddel ontwikkeld, de zogenaamde ICO-wizard.[5] De overheid is een grote afnemer van ICT-producten en diensten en kan als grote marktpartij de vraag in de markt stimuleren naar digitaal veilige ICT-producten en diensten.

---

[3] Kamerstuk 26 643, nr. 801
[4] Kamerstuk 26 643, nr. 767
[5] https://www.bio-overheid.nl/ico-wizard/

Vraag 4
Wat gaat u ondernemen om bij softwarefabrikanten af te dwingen dat ze meer investeren in structurele en toetsbare oplossingen voor veiligheidsproblemen in software, in plaats van dat softwarefabrikanten de softwaregebruikers overladen met patches en updates?

Antwoord 4
Europese samenwerking op dit terrein is van groot belang. Een voorbeeld van een van de huidige maatregelen is de inzet op de ontwikkeling van Europese cybersecuritycertificeringschema's onder de *Cyber Security Act*. De Cyber Security Act is het Europese raamwerk waarbinnen cybersecuritycertificeringsschema's worden ontwikkeld voor verschillende categorieën ICT-producten, diensten en processen. Nederland zet hierbij in op de ontwikkeling van een certificeringschema voor softwarebeveiliging. Ook voor deze vraag geldt dat het kabinet de aanbevelingen op dit vlak nog nader zal bestuderen en daarop zal ingaan in de eerdergenoemde kabinetsreactie.

Vraag 5
Hoe gaat u opvolging geven aan het advies om softwarefabrikanten aansprakelijk te stellen voor de gevolgen van softwarekwetsbaarheden?

Antwoord 5
Zoals aangegeven bij vraag 1 is het kabinet het OVV-rapport zorgvuldig aan het bestuderen. Het wettelijk vastleggen van de verantwoordelijkheid van fabrikanten voor veilige software en hun aansprakelijkheid voor de gevolgen van eventuele kwetsbaarheden zal op Europees niveau geregeld moeten worden. De OVV heeft deze aanbeveling dan ook gericht aan de Europese Commissie. Eventuele inzet in lijn met deze aanbeveling vanuit het kabinet zou dan ook gericht zijn op het beïnvloeden van besluitvorming hierover op Europees niveau.

Vraag 6
Hoe gaat u invulling geven aan de aanbeveling van de Onderzoeksraad voor Veiligheid om op Europees niveau kwaliteitseisen aan software te stellen om softwarefabrikanten te dwingen verantwoordelijkheid te nemen voor de veiligheid van hun product?

Antwoord 6
Zoals aangegeven in de beantwoording op vraag 5 is deze aanbeveling van de OVV gericht aan de Europese Commissie. Vanwege het grensoverschrijdende karakter van de markt voor ICT-producten en – diensten ligt het in algemene zin voor de hand om dergelijke eisen op te leggen in internationaal en Europees verband. Gedurende de afgelopen periode heeft Nederland zich op basis van de Roadmap Digitaal Veilige Hard- en Software sterk gemaakt voor Europese maatregelen zoals cybersecurity certificering van ICT-producten, diensten en processen onder *de Cyber Security Act* en wettelijke cybersecurityeisen voor Europese markttoegang voor verbonden apparaten onder de *Radio Equipment Directive*.
Ook gaat Nederland actief het gesprek aan met de Europese Commissie over de ontwikkeling van horizontale regulering voor de cybersecurity van ICT-producten en diensten via de *Cyber Resilience Act*. Hiervoor is een non-paper opgesteld en aangeboden aan Uw Kamer op 14 december 2021.[6]

[6] https://www.tweedekamer.nl/kamerstukken/detail?id=2021D49776&did=2021D49776