Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2016–2017

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 477

BRIEF VAN DE STAATSSECRETARIS VAN VEILIGHEID EN JUSTITIE

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 21 juni 2017

Hierbij bied ik uw Kamer het Cybersecuritybeeld Nederland 2017 (CSBN 2017) aan[1]. Deze brief is aangekondigd in mijn brief aan uw Kamer over de stand van zaken wannacry-ransomware en aanvallen op vitale infrastructuur van 2 juni jl.[2] en tijdens het plenaire debat hierover van 6 juni jl. (Handelingen II 2016/17, nr. 83, item 21). Het CSBN 2017 is onder verantwoordelijkheid van de Nationaal Coördinator Terrorismebestrijding en Veiligheid in samenwerking met de publieke en private sector tot stand gekomen. Dit beeld biedt inzicht in de belangen, dreigingen, weerbaarheid en daarmee samenhangende ontwikkelingen op het gebied van cybersecurity over de periode mei 2016 tot en met april 2017. De kernbevindingen en conclusies worden in deze brief toegelicht en worden onderschreven door de Cyber Security Raad. Daarnaast ga ik in deze brief in op de vraag over aansprakelijkheid van softwareproducenten en aansprakelijkheidsrecht zoals gesteld door het lid Helder tijdens het plenaire debat van 6 juni jl. (Handelingen II 2016/17, nr. 83, item 21), conform toezegging u hier voor de zomer over te informeren.

Cybersecuritybeeld Nederland 2017

Het CSBN 2017 maakt zichtbaar dat de grootste dreiging nog steeds uitgaat van beroepscriminelen en statelijke actoren. Beroepscriminelen richten zich in toenemende mate op grote bedrijven voor financieel gewin. Statelijke actoren intensiveren hun ondermijnende digitale activiteiten. Naast digitale economische en politieke spionage en sabotage, worden digitale middelen ingezet voor de beïnvloeding van democratische processen. Ook wordt zichtbaar dat veel organisaties afhankelijk zijn van een beperkt aantal aanbieders van digitale infrastructuurdiensten waardoor de maatschappelijke impact bij verstoring groot kan zijn. Het beeld laat daarnaast zien dat de digitale weerbaarheid van individuen en

[1] Raadpleegbaar via www.tweedekamer.nl.
[2] Kamerstuk 26 643, nr. 464.

kst-26643-477
ISSN 0921 - 7371
's-Gravenhage 2017

organisaties achter blijft bij de dreiging. Daarnaast heeft de kwetsbaarheid van het internet der dingen geleid tot verstorende aanvallen die de noodzaak tot het versterken van de digitale weerbaarheid onderschrijven.

Gegeven de zich sterk ontwikkelende dreiging zijn er in 2016 concrete acties ingezet op het gebied van publiek-private samenwerking en het intensiveren van de detectie van digitale dreigingen en de aanpak van cybercrime. Vanaf 2017 is een aantal intensiveringen in de begroting van het Ministerie van Veiligheid en Justitie opgenomen teneinde de Nederlandse cybersecurity verder te versterken. Deze acties en intensiveringen blijven, gezien het zorgelijke beeld van 2017, onverminderd relevant. Gezien het grensoverschrijdende karakter van het digitale domein, valt het dreigingsbeeld in Nederland niet los te zien van internationale ontwikkelingen en inspanningen[3].

Het beeld laat zien dat investeren in de toekomst nodig zal blijven voor de verhoging van de digitale weerbaarheid. Conform eerdere toezegging worden hiertoe ronde tafelsessies met het bedrijfsleven en overige stakeholders georganiseerd. De eerste ronde tafelsessie heeft reeds plaatsgevonden. Een tweede sessie zal gezamenlijk met het Ministerie van OCW en EZ en NWO (dcypher) worden vormgegeven en ingaan op het stimuleren van cybersecurity in het onderwijs. Een derde sessie zal in het teken staan van accreditering en certificering.

Aansprakelijkheid

Het lid Helder heeft vragen gesteld over de aansprakelijkheid van softwareproducenten. Zij vraagt of een producent aansprakelijk is voor schade van de gebruikers van zijn software, indien hij een update voorhanden heeft die deze schade had kunnen voorkomen, maar deze niet verstrekt. Ook vraagt zij of het bestaande aansprakelijkheidsrecht wel toereikend is voor ICT-producten of -diensten. Er kan sprake zijn van aansprakelijkheid op grond van wanprestatie, productaansprakelijkheid of onrechtmatige daad.

Een softwareleverancier kan aansprakelijk zijn op grond van wanprestatie (o.m. artikel 6:74 van het Burgerlijk Wetboek, hierna: BW). Dat is het geval als de software niet voldoet aan de veiligheid die is overeengekomen of die de afnemer redelijkerwijs mocht verwachten. Relevant in dit verband is, dat er op dit moment in EU-verband wordt onderhandeld over een richtlijnvoorstel over consumentencontracten voor de levering van digitale producten en diensten, waaronder software (COM (2015) 634). Daarbij is specifieke aandacht voor updates die moeten voorkomen dat software wordt geïnfecteerd door virussen. Het richtlijnvoorstel houdt onder meer in dat als de verkoper de updates heeft beloofd door te voeren of de consument dit redelijkerwijs mocht verwachten, maar dit niet gebeurt, de consument de schade die hij daardoor lijdt, kan verhalen op de verkoper.

Voorts geldt dat een softwareproducent aansprakelijk kan zijn voor schade in de privésfeer op grond van productaansprakelijkheid (artikel 6:185 BW). De gedachte achter de productaansprakelijkheid is dat de producent schade vergoedt die zijn product veroorzaakt, ook als hem geen verwijt te maken is. De bescherming van de afnemers staat voorop. De producent is kort gezegd aansprakelijk voor een productie-, informatie- of ontwerpgebrek, waardoor de software niet de veiligheid biedt die ervan mag worden verwacht. Hij kan zich wel verweren tegen aansprakelijkheid,

[3] Zoals weergegeven in Digitaal bruggen slaan, een aanzet tot een Internationale Cyberstrategie (Kamerstuk 26 643, nr. 447).

bijvoorbeeld door te stellen dat het op grond van de stand van de technische kennis op het tijdstip waarop hij de software leverde, onmogelijk was het bestaan van het veiligheidsgebrek te kennen.

Een onrechtmatige daad is ten slotte aan de orde als de softwareproducent of -leverancier verwijtbaar iets doet of nalaat, waardoor de softwaregebruiker schade lijdt (artikel 6:162 BW). Hiervan zou sprake kunnen zijn als een voorhanden zijnde update niet wordt doorgevoerd.

De huidige wettelijke bepalingen laten de rechtspraktijk de ruimte om rekening te houden met specifieke kenmerken van software en ransomware, en met de verschillende verantwoordelijkheden van producent, leverancier en afnemer.

Meer in het algemeen moet aansprakelijkheid gezien worden in relatie tot de vraag hoe gekomen kan worden tot het leveren van cybersecure producten en diensten op gebied van ICT. Hiertoe onderzoekt het kabinet, in overleg met het bedrijfsleven, op welke wijze de cyberveiligheid van het Internet of Things versterkt kan worden[4]. Tevens steunt het kabinet de ontwikkeling op EU-vlak om te komen tot een veiliger Digitale Eengemaakte markt, onder meer via standaardisering en certificering.

Gezien de omvang van het onderwerp is dit een brede maatschappelijke uitdaging op het gebied van digitalisering waarop geen *one-size-fits-all* benadering mogelijk is. Evenals bij de motie van de leden Hijink-Tellegen inzake de verkenning naar een Digital Trust Centre (Kamerstuk 26 643, nr. 474), behelst het vraagstukken waarbij gekeken moet worden naar zowel het samen met de markt ontwikkelen van nieuwe samenwerkingsvormen alsmede naar aansluiting op bestaande structuren.

Daarom vraagt het kabinet de Cyber Security Raad om te komen tot een advies met betrekking tot de kansen en dreigingen van het Internet of Things. Hiermee kan verkend worden welke nationale en internationale mogelijkheden er bestaan om in gezamenlijkheid verder te werken aan de digitale veiligheid van producten en diensten. Ook zal ik de Cyber Security Raad vragen om, in het licht van de motie van de leden Hijink-Tellegen (Kamerstuk 26 643, nr. 474), te komen met een advies aan mij en het Ministerie van Economische Zaken over informatie-uitwisseling inzake cybersecurity en cybercrime. In het bijzonder wordt gevraagd in te gaan op hoe gekomen kan worden tot een landelijk dekkend stelsel van informatieknooppunten, het bevorderen van informatie-uitwisseling en delen van advies.

De Staatssecretaris van Veiligheid en Justitie,
K.H.D.M. Dijkhoff

[4] Kamerstukken 29 544 en 33 009, nr. 773.