Ministerie van Justitie en Veiligheid

> Retouradres Postbus 20301 2500 EH Den Haag

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Juridische en Operationele Aangelegenheden

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Ons kenmerk
2777622

Uw kenmerk
2019Z25159

Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen.

Datum 24 januari 2020
Onderwerp Antwoorden Kamervragen over het bericht 'Minister Grapperhaus pleit bij Europese Unie voor achterdeur in encryptie'

In antwoord op uw brief van 13 december 2019 deel ik u mee dat de schriftelijke vragen van het Van Dam (CDA) inzake het bericht 'Minister Grapperhaus pleit bij Europese Unie voor achterdeur in encryptie', worden beantwoord zoals aangegeven in de bijlage bij deze brief.

De Minister van Justitie en Veiligheid,

Ferd Grapperhaus

Antwoorden Kamervragen van de minister van Justitie en Veiligheid op de vragen van het lid Van Dam (CDA) over het bericht 'Minister Grapperhaus pleit bij Europese Unie voor achterdeur in encryptie' (ingezonden 13 december 2019, nr. 2019Z25159)

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Juridische en Operationele Aangelegenheden

Datum
24 januari 2020

Ons kenmerk
2777622

Vraag 1
Bent u bekend met het bericht 'Minister Grapperhaus pleit bij Europese Unie voor achterdeur in encryptie' dd. 5 december 2019 op Tweakers.net? 1)

Antwoord vraag 1
Ja.

Vraag 2
Wat zijn – op hoofdlijnen – de technische mogelijkheden om een achterdeur in te bouwen in versleutelde software en diensten? Kunt u deze vraag specifiek beantwoorden voor (a) Whatsapp, (b) Telegram en (c) voor platforms die door specifieke doelgroepen (bijvoorbeeld criminelen) zelf zijn opgezet?

Vraag 3
Zou het een optie zijn om bij wet de sleutellengte van encryptie te beperken tot een zodanig niveau dat professionele diensten als de politie en de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) een reële mogelijkheid krijgen om encryptie te kraken, anders dan amateurs?

Antwoord vraag 2 en 3
Het breder gebruik van encryptie, onder meer door het standaard instellen van versleuteling bij communicatie tussen personen, maakt het opsporen van strafbare feiten lastiger en soms onmogelijk. De mogelijkheden om rechtmatige toegang tot communicatie te verkrijgen en de voor- en nadelen daarvan worden momenteel bezien. Daarbij hecht ik aan overleg met publieke en private partijen en streef ik naar oplossingen binnen de kaders van het kabinetsstandpunt over encryptie uit 2016. Uw Kamer is hierover bij brief van 4 januari 2016 geïnformeerd.[1]

Vraag 4
Hoe groot schat u de kans in dat bij het toegankelijk maken van thans ge-encrypt berichtenverkeer zoals Whatsapp en Telegram criminelen eigen zelf-encrypte voorzieningen gaan opzetten en daar gebruik van gaan maken?

Antwoord vraag 4
Het opzetten van eigen voorzieningen voor het versturen van encrypted berichten is mogelijk en niet bij wet verboden. Er zijn dan ook bedrijven die voorzieningen voor het versturen van encrypted berichten aanbieden. In het kader van strafrechtelijke onderzoeken zijn niettemin bij bedrijven reeds berichten in beslag genomen en heeft het OM berichten in onversleutelde vorm kunnen inzien.

[1] Kamerstuk 26643 nr. 383

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Juridische en Operationele Aangelegenheden

Datum
24 januari 2020

Ons kenmerk
2777622

Vraag 5
Leidt het inbouwen van een achterdeur per definitie tot het hebben van inzicht in alle communicatie die via een bepaalde dienst of software gedeeld wordt, of is het mogelijk om de toegang te beperken tot specifiek berichtenverkeer tussen specifieke deelnemers?

Antwoord vraag 5
Zoals aangegeven in het antwoord op de vragen 2 en 3 streef ik naar oplossingen binnen de kaders van het kabinetsstandpunt over encryptie uit 2016. Dergelijke oplossingen zouden toegang moeten bieden tot communicatie tussen specifieke deelnemers of van een specifieke deelnemer.

Vraag 6
Welke mogelijkheden bestaan er om buiten platforms of diensten zicht te krijgen op de communicatie die via software en diensten tot stand komt, bijvoorbeeld door zicht te krijgen op toetsenbordaanslagen? Is er aanvullende wetgeving nodig om langs die weg rechtmatig bewijs te verzamelen of mag dat nu al?

Antwoord vraag 6
De Wet computercriminaliteit III bevat de bevoegdheid tot binnendringen in een geautomatiseerd werk. Daarnaast is het mogelijk een technisch hulpmiddel te plaatsen op een geautomatiseerd werk zodra de politie daar de fysieke toegang toe heeft, bijvoorbeeld na het betreden van de plaats waar het geautomatiseerd werk aanwezig is. Elke mogelijkheid brengt bepaalde kosten, risico's en privacy-inbreuken met zich mee en voor elke mogelijkheid gelden specifieke wettelijke voorwaarden en waarborgen. Zoals gemeld in het antwoord op vraag 2 en 3 worden de mogelijkheden om rechtmatige toegang tot communicatie te verkrijgen en de voor- en nadelen daarvan bezien.

1) Tweakers, 5 december 2019, https://tweakers.net/nieuws/160786/minister-grapperhaus-pleit-bij-europese-unie-voor-achterdeur-inencryptie.html