

2019Z25159

Vragen van het lid **Van Dam** (CDA) aan de Minister van Justitie en Veiligheid over het bericht «Minister Grapperhaus pleit bij Europese Unie voor achterdeur in encryptie» (ingezonden 13 december 2019).

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

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?

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?

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?

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

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?