Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2014–2015

Aanhangsel van de Handelingen

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

2677

Vragen van de leden **Verhoeven** en **Hachchi** (beiden D66) aan de Staatssecretaris van Veiligheid en Justitie, de Ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Defensie over *het bericht dat kwetsbaarheden in encryptiesoftware door Amerikaanse inlichtingendiensten zijn gebruikt* (ingezonden 2 juni 2015).

Mededeling van Staatssecretaris **Dijkhoff** (Veiligheid en Justitie) mede namens de Ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Defensie (ontvangen 24 juni 2015)

Vraag 1
Kent u het wetenschappelijk artikel over kwetsbaarheden in het Diffie-Hellman-sleuteluitwisselingsprotocol?[1]

Vraag 2
Deelt u de mening van de wetenschappers dat het zeer aannemelijk is dat de National Security Agency (NSA) via deze kwetsbaarheden toegang heeft verkregen tot VPN- (Virtual Private Network), SSH- (Secure Shell) en TLS (Transport Layer Security) verkeer? Zijn er bij u signalen bekend dat ook inlichtingendiensten van andere landen of niet-statelijke actoren deze kwetsbaarheden hebben gebruikt?

Vraag 3
Bent u van mening dat de Nederlandse overheid toegang zou moeten hebben tot versleutelde data via bestaande kwetsbaarheden of door het (laten) inbouwen van kwetsbaarheden?

Vraag 4
Is er sprake van een eenduidig kabinetsbreed beleid ten opzichte van onbekende kwetsbaarheden, oftewel 0-days, of worden in verschillende ministeries verschillende afwegingen gemaakt? Worden alle door de overheid ontdekte, of via het Nationaal Cyber Security Centrum (NCSC) gemelde, 0-days bij de maker van de software gemeld?

[1] https://weakdh.org/imperfect-forward-secrecy.pdf

ah-tk-20142015-2677
ISSN 0921 - 7398
's-Gravenhage 2015

Vraag 5
Maken defensie, inlichtingendiensten, politie of andere overheidsinstanties ook gebruik van 0-days of alleen van reeds bekende kwetsbaarheden?

Vraag 6
Deelt u de mening dat vertrouwen in veilige digitale communicatie en infrastructuur essentieel is voor een goed functionerende digitale economie? Hoe verhoudt zich dat tot een overheid die actief gebruik maakt van kwetsbaarheden in software?

Mededeling

Hierbij bericht ik u, mede namens de ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Defensie dat de schriftelijke vragen van de leden Verhoeven en Hachchi (beiden D66) over het bericht dat kwetsbaarheden in encryptiesoftware door Amerikaanse inlichtingendiensten zijn gebruikt (ingezonden 2 juni 2015) niet binnen de gebruikelijke termijn kunnen worden beantwoord, aangezien nog niet alle benodigde informatie ontvangen is. Ik streef ernaar de vragen zo spoedig mogelijk te beantwoorden.