

Ministerie van Veiligheid en Justitie

> Retouradres Postbus 20011 2500 EA Den Haag

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

Directie Cyber Security

Turfmarkt 147
2511 DP Den Haag
Postbus 20011
2500 EA Den Haag
www.nctv.nl

Ons kenmerk

2137654

Uw kenmerk

2017Z12365

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

Datum 12 oktober 2017

Onderwerp Antwoorden Kamervragen over het feit dat er een groei van 122% is
geconstateerd in varianten van ransomware

Hierbij bied ik u mede namens de minister van Economische Zaken de
antwoorden aan op vragen van het lid Van der Lee (GroenLinks) inzake het feit
dat er een groei van 122% is geconstateerd in varianten van ransomware.

De Minister van Veiligheid en Justitie,

S.A. Blok

Antwoorden op schriftelijke vragen van het lid Van der Lee (GroenLinks) aan de ministers van Economische Zaken en van Veiligheid en Justitie over het feit dat er een groei van 122% is geconstateerd in varianten van ransomware (ingezonden 20 september 2017, 2017Z12365).

Datum
12 oktober 2017
Ons kenmerk
2137654

Vraag 1

Bent u bekend met het rapport dat beveiligingsbedrijf SecureWorks heeft gepubliceerd over de forse wereldwijde groei in het aantal nieuwe varianten van ransomware? 1)

Antwoord op vraag 1

Ja.

Vraag 2

Verwacht u dat de groei van 122% meer nieuwe varianten van ransomware in 2016 ten opzichte van het jaar daarvoor, zich op vergelijkbare wijze zal doorzetten in dit jaar en de jaren daarna? Of kan er zelfs een nog hardere, exponentiële groei optreden?

Antwoord op vraag 2

In het op 21 juni jongstleden aan uw Kamer aangeboden Cybersecurity Beeld Nederland 2017 (CSBN 2017) komt naar voren dat ransomware een groeiend onderdeel van cybercriminaliteit is¹. Ondanks het feit dat de ontwikkelingen op het gebied van ransomware nauwlettend worden gevolgd, is de precieze mate waarin deze trend zich in de komende jaren zal voortzetten moeilijk te voorspellen. De opeenvolgende cybersecuritybeelden laten zien dat ransomware gegroeid is tot het middel bij uitstek voor beroepscriminelen. Hoewel er geen reden is om aan te nemen dat ransomware de komende jaren zal verdwijnen, is niet te voorzien hoeveel varianten van ransomware er in de toekomst zullen zijn. Het is belangrijk om constant passende maatregelen te blijven treffen. Het kabinet heeft daarom bij Prinsjesdag aanvullende middelen voor cybersecurity gereserveerd, zie ook het antwoord op vraag 3 en 4.

Vraag 3

Deelt u de mening dat de Nederlandse samenleving en economie nog onvoldoende bestand is tegen deze harde groei in ransomware, met alle schade voor de economie en de privacy van dien?

Vraag 4

Deelt u de mening dat deze harde groei in ransomware ook noopt tot een verdere versterking van de cybersecurity bovenop het staande beleid? Zo nee, waarom niet? Zo ja, welke vervolgstappen zijn volgens u het meest urgent dan wel effectief?

Antwoord op vraag 3 en vraag 4

Zoals d.d. 21 juni reeds aangegeven blijft de digitale weerbaarheid in Nederland achter bij de dreiging, mede door de groei van ransomware. Daarom is het zaak extra te investeren in het versterken van de Nederlandse digitale veiligheid en de bewustwording over cybersecurity te vergroten. Het ministerie van Veiligheid en

¹ Kamerbrief d.d. 21 juni 2017 (Kamerstuk 26643, nr. 477)

Justitie stimuleert in samenwerking met het ministerie van Economische Zaken bewustwording over cybersecurity onder meer door middel van de portal veiliginternetten.nl en de op 2 oktober jongstleden gestarte jaarlijkse campagne 'alert online', waarin ondernemers en burgers meer bewust worden gemaakt van hun online en digitale veiligheid.

Directie Cyber Security

Datum

12 oktober 2017

Ons kenmerk

2137654

Vanwege de toenemende dreigingen op cybergegebied stelt het kabinet vanaf 2018 structureel een extra bedrag van 26 miljoen beschikbaar als eerste aanzet ter verbetering van de digitale veiligheid. Met deze investering wordt de digitale veiligheidsketen (AIVD, MIVD, Politie en OM) versterkt. Met dit bedrag kan de politie onder andere nieuw personeel werven om de aanpak van cybercriminaliteit te versterken en kunnen per jaar meer onderzoeken worden opgestart.

Verder werken het ministerie van Economische Zaken en het ministerie van Veiligheid en Justitie onder gebruikmaking van bovengenoemd extra bedrag nauw samen in het opzetten van een Digital Trust Centre, om ook het niet als vitaal aangemerkte gedeelte van het bedrijfsleven weerbaarder te maken op cybergegebied.

Vraag 5

Kunt u ook beschrijven welke stappen nu op Europees niveau worden gezet om bijvoorbeeld op het terrein van producteisen en certificering ervoor te zorgen dat de beveiliging van apparaten die in een netwerk kunnen worden gebruikt naar een hoger plan wordt getild?

Antwoord op vraag 5

Op 13 september jongstleden heeft de Europese Commissie een reeks nieuwe voorstellen gepresenteerd op het gebied van cybersecurity. Een van deze voorstellen behelst een verordening die onder meer strekt tot het oprichten van een Europees kader voor cyberbeveiligingscertificering voor ICT-producten en -diensten. In de komende periode gaan de Europese lidstaten in samenwerking met de Europese Commissie over deze voorstellen in overleg. Na behandeling van de Commissievoorstellen in de ministerraad zult u geïnformeerd worden over de eerste Nederlandse reactie op deze voorstellen.

1) <https://www.nu.nl/tech/4924541/aantal-nieuwe-vormen-van-ransomware-in-2016-sterk-toegenomen.html>