Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2019–2020

26 643 Informatie- en communicatietechnologie (ICT)

28 684 Naar een veiliger samenleving

Nr. 678 **BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 22 april 2020

Bij brief van 6 februari 2020[1] vroeg uw Kamer mij om een reactie op de berichtgeving dat de Universiteit Maastricht losgeld heeft betaald aan hackers. Het lid Verhoeven (D66) heeft over dezelfde berichtgeving op 23 januari schriftelijke vragen mij gesteld. Voor mijn reactie op uw verzoek verwijs ik allereerst naar de antwoorden van 23 maart 2020 op deze Kamervragen[2].

Uitgangspunt in de aanpak van ransomeware is dat het van belang is om altijd aangifte te doen en het onwenselijk is om losgeld te betalen. Door aangifte kunnen politie en justitie passende maatregelen nemen. Aangifte draagt daarnaast bij aan het brede inzicht in de aard en de omvang van deze vorm van criminaliteit waardoor ook op langere termijn een betere aanpak kan worden ontwikkeld en passende preventieve maatregelen kunnen worden genomen. Door losgeld te betalen worden criminele activiteiten beloond en gestimuleerd. Daarnaast is de verwachting van de politie dat het betalen van losgeld leidt tot meer aanvallen van ransomware.

Uitgangspunt in het cybersecuritystelsel is dat organisaties primair zelf verantwoordelijk zijn voor digitale weerbaarheid. Het is voor publieke en private organisaties daarom van belang dat cybersecurity voldoende aandacht krijgt in de bedrijfsvoering en dat organisaties de nodige maatregelen nemen om te voorkomen dat zij slachtoffer worden van een aanval van ransomware. De overheid treedt op waar nodig, onder meer door opsporing, vervolging en attributie. Via preventiecampagnes, advies en het communiceren van concrete handelingsperspectieven, zoals het maken van back-ups, worden burgers en organisaties geïnformeerd over veiligheid en internet, bijvoorbeeld via veiliginternetten.nl, het Digital Trust Center en het Nationaal Cyber Security Centrum (NCSC). Ik heb uw Kamer over de brede aanpak van cybersecurity recent uitgebreid

[1] Brief VKC JenV.
[2] Aanhangsel Handelingen II 2019/20, nr. 2184.

kst-26643-678
ISSN 0921 - 7371
's-Gravenhage 2020

geïnformeerd in de kabinetsreactie op het Rapport van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) over digitale ontwrichting.[3] Naast bredere bewustwording over cybersecurity staan cybercrime en slachtofferschap daarvan centraal in de integrale aanpak cybercrime[4] waarover ik uw Kamer periodiek informeer.

In reactie op berichtgeving waaraan het lid Verhoeven in de hiervoor genoemde Kamervragen naar verwees, ben ik in mijn antwoorden op die vragen ook ingegaan op de mogelijke rol van verzekeringen tegen cybercriminaliteit. Verzekeringsmaatschappijen zouden extra nadruk op adequate cybersecurity van hun verzekeringsnemers kunnen generen door specifieke eisen te stellen, zoals het regelmatig maken van een back-up. Tot slot heeft het mijn voorkeur dat de verzekeraar niet het losgeld vergoedt dat in handen van criminelen terecht komt, maar juist de geleden schade door het niet betalen van dit losgeld. Mijn opvattingen heb ik bij het Verbond van Verzekeraars onder de aandacht gebracht. Het Verbond van Verzekeraars heeft mij laten weten dat zij de geuite zorgen onder de aandacht zal brengen van de leden en hierover met hen in gesprek zal gaan. Voor verzekeraars geldt al jaren als beleid het uitgangspunt dat verzekeringscriminaliteit niet mag lonen. Dat laat onverlet dat verzekeraars de schade die wordt veroorzaakt door crimineel handelen van derden aan hun verzekerden vergoeden. Verzekeraars zijn zich bewust van de grote maatschappelijke gevolgen van het betalen van losgeld, net als andere gevolgen van cybercriminaliteit waarvoor gedupeerde verzekerden schadeloos kunnen worden gesteld door hun verzekeraar. Bedrijven die zich verzekeren tegen cyberrisico's zijn in de regel zich bewuster van de risico's en beter beschermd, maar kunnen desondanks slachtoffer zijn van cybercriminelen.

De Minister van Justitie en Veiligheid,
F.B.J. Grapperhaus

[3] Kamerstukken 26 643 en 30 821, nr. 673.
[4] Voor meer informatie over de aanpak van cybercrime verwijs ik u naar eerder brieven over de integrale aanpak cybercrime en in het bijzonder naar voortgangsbrief aan uw kamer daarover – Kamerstuk 28 684, nr. 564.