Ministerie van Veiligheid en Justitie

> Retouradres Postbus 20301 2500 EH Den Haag

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA Den Haag

Directie Cyber Security
ACSB

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

Ons kenmerk
2128801

Bijlagen
1

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

Datum 20 september 2017

Onderwerp Reactie inzake cyberaanval met ransomware en voortgang moties uit Wannacry-debat

In reactie op uw verzoek in de procedurevergadering d.d. 28 juni jl. (kenmerk 2017Z09173/2017D19298) informeer ik uw Kamer hierbij over de cyberaanval met cryptoware die Not-Petya genaamd is. Tevens ga ik in dat licht in op de voortgang van de moties die zijn ingediend bij het debat inzake de Wannacry-ransomware d.d. 6 juni jl. Tot slot ga ik kort in op de door uw Kamer aan de Minister van Veiligheid en Justitie gestelde vraag inzake een uitgevoerde haalbaarheidsstudie naar een Cybertestbed.

Uitbraak cyberaanval met cryptoware
Op dinsdag 27 juni jl. zijn wereldwijd, met name in Oekraïne, organisaties getroffen door de Not-Petya cryptoware-infectie. Ook in Nederland zijn organisaties geraakt. De initiële besmetting lijkt plaats te hebben gevonden via een update van de boekhoudsoftware van een Oekraïens softwarebedrijf en verspreiding via een Oekraïense nieuwswebsite. De cryptoware is geavanceerd en maakt gebruik van diverse methodes, waaronder reeds bekende kwetsbaarheden in Microsoft-besturingssystemen die ook gebruikt zijn bij de recente Wannacry uitbraak. Daarbij kan bij deze cryptoware, anders dan bij Wannacry, de computer volledig onbruikbaar worden.

Hoewel er in de media veel aandacht was voor de aanval, met name voor de gevolgen bij APM Terminals, heeft dit niet geresulteerd in concrete maatschappelijke ontwrichting binnen Nederland. Dit komt mede doordat de aanval niet specifiek gericht lijkt te zijn op Nederlandse organisaties en klanten van de getroffen bedrijven (deels) gebruik konden maken van alternatieve dienstverleners. Dat neemt niet weg dat er wel degelijk sprake is van een serieuze impact. Voor zover bij het NCSC bevestigd, zijn vier Nederlandse bedrijven besmet. Er zijn geen besmettingen binnen de Rijksoverheid of vitale infrastructuur bekend.

De recente cryptoware-besmetting ondersteunt het beeld dat de cyberweerbaarheid van organisaties nog niet altijd gelijke pas houdt met de ontwikkeling van dreigingen. Dit beeld kwam reeds naar voren in het jaarlijkse cybersecuritybeeld Nederland (CSBN). Daarmee benadrukt deze casus het belang van investeren in cybersecurity en het belang van het ontwikkelen van een steeds verder dekkend stelsel van cybersecurity-organisaties.

Economische schade
Het kwantificeren van de exacte omvang van de economische schade voor Nederland van dergelijke aanvallen is uitermate complex. Dit komt onder andere doordat onduidelijk is in hoeverre klanten van getroffen bedrijven makkelijk een alternatief kon worden geboden door het getroffen bedrijf, door andere Nederlandse aanbieders of dat klanten uitweken naar het buitenland. Ook is onbekend hoe structureel dergelijke verschuivingen naar andere bedrijven of andere landen zijn. Het is daarom voor mij niet mogelijk bedragen met enige nauwkeurigheid te noemen. De eigenaar van de terminal heeft inmiddels via de media aangegeven dat sprake is van serieuze schade doch dat een daadwerkelijke inschatting pas bij de volgende kwartaalcijfers goed te maken is. Duidelijk is evenwel dat de getroffen bedrijven significant tijd hebben moeten investeren in het werken aan, of wachten op, herstel van de getroffen systemen en in die tijd geen productie konden draaien. Het is daarom aannemelijk dat cyberaanvallen als deze voor getroffen bedrijven een aanzienlijke financiële impact hebben.

Maatregelen Nationaal Cyber Security Centrum tijdens deze cyberaanval
Reeds op 14 maart jl. heeft het Nationaal Cyber Security Centrum (NCSC) van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) van mijn ministerie, via onder meer zijn website, gewaarschuwd over de kwetsbaarheden in het Microsoft-besturingssysteem die ten grondslag liggen aan de Wannacry en Not-Petya uitbraak en daarbij advies gegeven over te nemen maatregelen voor de kwetsbaarheden in het Microsoft-besturingssysteem.

Toen het NCSC op 27 juni jl. vernam van de Not-Petya cyberaanval, is onverwijld contact gezocht met getroffen partijen en is de impact op Nederland, en in het bijzonder de Rijksoverheid en vitale infrastructuur, bezien. Naast de directe communicatie met organisaties binnen de Rijksoverheid en vitale infrastructuur heeft het NCSC langs diverse kanalen, waaronder twitter, zijn website en veiliginternetten.nl, organisaties en burgers in Nederland in algemene zin gewaarschuwd en geadviseerd over te treffen maatregelen.

Digital Trust Centre (DTC)
Deze casus laat zien dat hoewel er geen sprake was van maatschappelijke ontwrichting, zich wel degelijk een relevante maatschappelijke impact manifesteert. Bij deze casus betrof het organisaties die geen deel uitmaken van de Rijksoverheid of de vitale infrastructuur. De recente cryptoware-infectie laat daarmee zien dat het zaak is, in aansluiting op de rol van het NCSC, zoals besproken in het plenair debat over Wannacry d.d. 6 juni jl., te werken aan een dekkend stelsel van cybersecurity-organisaties. In de motie van de leden Hijink (SP) en Tellegen (VVD) van 13 juni jl. (26643, nr. 474) is de regering reeds verzocht om in overleg te treden met maatschappelijke organisaties over de oprichting en vormgeving van een DTC teneinde bedrijven en maatschappelijke organisaties te informeren, adviseren en concrete hulp en ondersteuning te bieden voor het verbeteren van cybersecurity.

Mede in het licht van de Not-Petya-casus acht ik het van belang om te investeren in het verhogen van de digitale weerbaarheid buiten de vitale infrastructuur. De minister van Economische Zaken heeft uw Kamer, mede namens mij, in verband met het voorgaande geïnformeerd, in een brief die tegelijkertijd met deze brief naar uw Kamer wordt verzonden, over de wijze waarop het niet als

vitaal aangemerkte bedrijfsleven, actiever dan nu, naar een hoger weerbaarheidsniveau wordt gebracht.

Volledigheidshalve is in de bijlage tevens een overzicht opgenomen van de in het licht van de andere moties reeds ingezette acties.

Cybertestbed
In het AO Nationale Veiligheid d.d. 29 juni jl. heeft het lid van Engelshoven (D66) de minister van Veiligheid en Justitie verzocht om in te gaan op de door the Hague Security Delta uitgevoerde studie naar een Cybertestbed. Tevens is gevraagd naar de wijze waarop de overheid omgaat met programma's inzake het vinden van kwetsbaarheden. Tot slot is gevraagd of de overheid het belang van investeren in onderzoek naar cybersecurity erkent.

Ik kan u daarbij aangeven dat wij bekend zijn met de studie naar een Cybertestbed. Ik hecht er echter wel aan om te benadrukken dat de vraag of een Cybertestbed meerwaarde heeft voor onderzoekers en bedrijven in de vitale infrastructuur in de eerste plaats een vraag is die primair bij hen thuishoort en niet voor hen door de overheid ingevuld dient te worden. De afgelopen jaren is wel nadrukkelijk geïnvesteerd in publiek-private samenwerking en de verbinding met onderzoek. De realisatie Dcypher als platform is daar het concrete voorbeeld van. Ik zal de vraag hoe wordt aangekeken tegen het Cybertestbed dan ook in dat platform laten agenderen.

Ten aanzien van het omgaan met kwetsbaarheden kan ik aangeven dat Nederland en in het bijzonder het Nationaal Cyber Security Centrum juist een van de koplopers is geweest in het bevorderen van de samenwerking met ethische hackers in het kader van responsible disclosure. Die rol blijft de overheid, en het NCSC in het bijzonder, uiteraard vervullen. In het belang hiervan wordt ook in toenemende mate internationaal omarmd.

Komende periode
Tot slot vroeg het lid Van Engelshoven naar het belang van investeren in het licht van onderzoek. Dat belang herken ik volledig, daarom is, mede dankzij een bijdrage van het Internal Security Fund van de EU, in 2017 een derde Small Business Innovation Research (SBIR) tender op het gebied van cybersecurity opengesteld, o.a. om Nederland voor te bereiden op de veiligheidsuitdagingen in de periode 2017-2019. In algemene zin staat wat mij betreft het belang van investeren voorop. De Not-Petya casus heeft wederom laten zien dat cybersecurity in de breedte investeringen vergt om Nederland digitaal weerbaar te maken. Daartoe zal in 2018 door het Kabinet een investering van 26 miljoen plaatsvinden. Daarmee zal o.a. de oprichting van het DTC worden vormgegeven en zullen de eerste noodzakelijke stappen in een verdere verhoging van de digitale weerbaarheid worden gezet.

De Staatssecretaris van Veiligheid en Justitie,

K.H.D.M. Dijkhoff

Bijlage 1: Voortgang aangenomen moties Wannacry-debat

Motie nr. 91684 van de leden Verhoeven (D66) en Buitenweg (GL) over een jaarlijkse test van de vitale ICT-infrastructuur

In het debat d.d. 6 juni jl. is reeds aangeven dat het verhogen van de digitale weerbaarheid van vitale organisaties verder zal worden vormgegeven door middel van de implementatie van de Netwerk en informatiebeveiligingsrichtlijn. Een concept-wetsvoorstel ter implementatie van deze richtlijn is deze zomer in consultatie gebracht en zal dit najaar in verdere procedure worden gebracht.

Motie nr. 91686 van het lid Krol (50Plus) over het pro-actief delen van kennis over digitale veiligheid

Het pro-actief delen van kennis heeft een prominente plek in het nationale cybersecurity beleid. Zoals aangegeven in het debat zal ook dit jaar de campagne Alert Online worden gehouden. Dit jaar vindt de campagne plaats van 2 tot en met 13 oktober met als thema Cybersecurity helden.

Motie nr. 91687 van het lid Verhoeven (D66) over het mandaat van het NCSC om (semi)-publieke instellingen te helpen bij cybersecurity

Inmiddels is het wetsvoorstel gegevensverwerking en meldplicht cybersecurity aangenomen door de Eerste Kamer. De inwerkingtreding zal plaatsvinden per 1 oktober a.s. Daarmee wordt onder meer voorzien in een wettelijke vastlegging van de taken van het NCSC. Om ook andere partijen actief van kennis te voorzien, zal zo veel mogelijk worden samengewerkt met het op te richten Digital Trust Centre (zie ook bovenstaand in het licht van de motie Hijjink-Tellegen)

Motie nr. 91689 van de leden Hijink (SP) en Verhoeven (D66) over maatregelen om consumenten te beschermen tegen slecht beveiligde apparatuur

De Kamer zal later dit jaar door Ministerie van Economische Zaken nader worden geïnformeerd over de roadmap digitale veilige hard- en software. In deze roadmap wordt beoogd een overzicht op hoofdlijnen te schetsen van de reeds verrichte activiteiten en de alsnog op te pakken activiteiten op het gebied van digitale veiligheid van hard- en software door publieke en private partijen.