Ministerie van Veiligheid en Justitie

> Retouradres Postbus 20011 2500 EA Den Haag

Directie Cyber Security
Beleid

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

Ons kenmerk
2084119

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

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

Datum 2 juni 2017
Onderwerp Stand van zaken wannacry-ransomware en aanvallen op vitale infrastructuur

In de Regeling van Werkzaamheden d.d. 16 mei jl. heeft uw Kamer mij verzocht om in navolging van het d.d. 16 mei jl. gehouden Mondeling Vragenuur te komen met een brief naar aanleiding van de uitbraak van de zogeheten "Wannacry-ransomware" en een in dit licht te houden debat. In aanvulling hierop is mij in de procedurevergadering van de Vaste Kamercommissie van Veiligheid en Justitie d.d. 17 mei jl. verzocht om in te gaan op het bericht "Overheden en energiesector besmet met gijzelsoftware". Middels deze brief informeer ik u over de huidige stand van zaken inzake de uitbraak van de Wannacry-ransomware en genoemde berichtgeving.

Uitbraak Wannacry-ransomware
Op vrijdag 12 mei jl. was wereldwijd sprake van een uitbraak van de zogeheten Wannacry-ransomware. Hierover heeft het onder de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) ressorterende Nationaal Cyber Security Centrum (NCSC) gelijk een bericht doen uitgaan. Naast het feit dat hier sprake was van ransomware, ofwel gijzelsoftware, bevatte de aanval een worm-mechanisme waardoor de ransomware snel en ongecontroleerd werd verspreid. Hiertoe maakte de aanval gebruik van een kwetsbaarheid in Microsoft-besturingssystemen. Microsoft had reeds voordat de uitbraak plaatsvond een patch voor de kwetsbaarheid geschreven en breed beschikbaar gesteld. Door het NCSC is reeds d.d. 14 maart gewaarschuwd voor de kwetsbaarheid inclusief bijbehorend handelingsperspectief. In het Mondeling Vragenuur d.d. 16. mei jl. heb ik reeds aangegeven dat de impact in Nederland zeer beperkt is gebleven. Weliswaar was er sprake van een besmetting bij Qpark die uitgebreid in de media behandeld is, doch dit incident heeft geenszins geresulteerd in maatschappelijke ontwrichting.

Ook in de periode na de Wannacry-uitbraak zijn geen meldingen van besmettingen bij de Rijksoverheid en in de vitale infrastructuur met de Wannacry-ransomware bij het NCSC binnengekomen. Ongeacht het feit dat in Nederland grootschalige impact is uitgebleven, is de Wannacry-casus een krachtig signaal dat cybersecurity publiek en privaat serieuze aandacht blijft behoeven. Daarnaast onderstreept deze casus een aantal essentiële pijlers van het beleid van de afgelopen jaren.

Ten eerste het belang van publiek-private samenwerking. Zoals bij deze casus te zien was, heeft een beveiligingsonderzoeker een belangrijke bijdrage geleverd door de internationale cybergemeenschap te informeren. Door nauwe samenwerking tussen partijen, zoals Computer Emergency Response Teams (CERT), is verdere verspreiding van de ransomware actief tegengegaan. Het NCSC investeert en participeert actief in de samenwerking met deze beveiligingsonderzoekers en de internationale CERT-community. Ook kan geconstateerd worden dat deze casus het belang eens te meer aangeeft van het verhelpen, ofwel patchen, van kwetsbaarheden. Daarbij is de informatievoorziening tussen het NCSC en bijvoorbeeld aanbieders binnen de vitale infrastructuur cruciaal.

Daarnaast is een internationale aanpak in de opsporing van belang. De internationale impact van de aanval laat bij uitstek zien dat het digitale domein een internationale aanpak vergt. In Europees verband hebben Europol en Eurojust hierbij een belangrijke rol. Daarnaast is een goede samenwerking tussen landen, ook landen buiten de EU, van essentieel belang, bijvoorbeeld in het kader van het Cybercrimeverdrag. De Nederlandse opsporingsdiensten dragen hier actief aan bij.

Tot slot onderstreept deze casus het belang van adequate wet- en regelgeving. Gegeven de impact die we in het buitenland zien is wet- en regelgeving hierin zowel van belang om de digitale weerbaarheid van onder meer van vitale infrastructuren te versterken als om daar waar nodig binnen de opsporing te beschikken over adequate opsporingsbevoegdheden. In dat laatste voorziet het aan het parlement aangeboden wetsvoorstel Computercriminaliteit III. Wat het eerste betreft is het wetsvoorstel ter implementatie van de Europese Netwerk- en InformatieBeveiligingsrichtlijn (NIB) in voorbereiding, dat onder meer voorziet in de verplichting van vitale aanbieders om passende beveiligingsmaatregelen te treffen en toezicht op de naleving daarvan.

Berichtgeving inzake overheden en energieleverancier
Op 17 mei jl. heeft het AD in aansluiting op de berichtgeving over de Wannacry-ransomware een artikel opgesteld over "Overheden en een energieleverancier die getroffen zouden zijn door ransomware".

Op verzoek van het AD hebben wij een overzicht van bij het NCSC gemelde cyberincidenten verstrekt. Dit overzicht was desgevraagd reeds eerder ook aan andere media verstrekt..

Het genoemde overzicht bevat uiteenlopende meldingen. In bovengenoemd artikel wordt gerefereerd aan vrijwillige meldingen van overheidsinstellingen en een aanbieder uit de energiesector over ransomware, waarbij vermeld dient te worden dat dit om meldingen van voor de Wannacry-uitbraak gaat. Het beeld dat in dit artikel gecreëerd is, dat bij deze incidenten sprake zou zijn van maatschappelijke ontwrichting, is onjuist. Inhoudelijk betreft dit voorvallen die geenszins qua aard en omvang als maatschappelijk ontwrichtend kunnen worden gekwalificeerd. Het zijn juist meldingen waarbij partijen de maatschappelijke verantwoordelijkheid hebben genomen om bij het NCSC voorvallen te melden zodat hier een breder beeld ontstaat van de actuele dreiging. Op basis van deze meldingen informeert en waarschuwt het NCSC waar aangewezen organisaties binnen de Rijksoverheid en de vitale infrastructuur en via de website in meer algemene zin ook andere organisaties zodat ook aldaar de dreiging van een

passend antwoord kan worden voorzien. Veelal gaat het in deze gevallen bijvoorbeeld om werkplekken van medewerkers die door ransomware worden besmet, waarna de werkgever door een back-up terug te plaatsen in staat is deze te verwijderen.

Deze incidenten en het bredere beeld dat deze opleveren vinden hun weerslag in het Cybersecuritybeeld Nederland waarover de Kamer jaarlijks wordt geïnformeerd.

Structurele aanpak
Incidenten zoals de Wannacry-casus illustreren eens te meer dat investeren in een verhoging van de digitale weerbaarheid loont. Hoewel de impact in Nederland als beperkt gekwalificeerd mag worden, kan het gebrek aan impact niet als een bevestiging gezien worden dat nationaal het weerbaarheidsniveau overeenkomt met het dreigingsniveau. Investeringen om de weerbaarheid gelijke tred te laten houden met de ontwikkeling van de dreiging zullen ook in de toekomst nodig blijven.

Aanvullend hecht ik er daarbij aan om te benadrukken dat ransomware geen nieuw fenomeen is en dat hier in de opeenvolgende aan uw Kamer aangeboden Cybersecuritybeelden Nederland (CSBN) reeds meerdere malen over is gesproken. In reactie op deze beelden is herhaaldelijk aangeven dat de dreigingen in het digitale domein, een algehele verhoging van de digitale weerbaarheid vergen. De reactie op deze dreiging is de afgelopen jaren vormgegeven aan de hand van de opeenvolgende Nationale Cyber Security Strategieën. Zo is het afgelopen jaar naar aanleiding van het CSBN 2016 additioneel geïnvesteerd in het verhogen van de cybersecurity; dit heeft onder andere geleid tot het versterken en uitbreiden van het Nationaal Detectie Netwerk. Zoals reeds aangegeven waren deze investeringen noodzakelijk en zullen deze in de komende jaren noodzakelijk blijven. Daarbij wil ik net als in het Mondeling Vragenuur d.d. 16 mei in reactie op de gepubliceerde Cyber Readiness Index onderstrepen dat we in Nederland de afgelopen jaren met bescheiden middelen in dat licht solide resultaten hebben gerealiseerd.

Het is zaak om het Nederlandse cybersecurity beleid en onze aanpak vorm te blijven geven op basis van een zo sterk mogelijk onderbouwd beeld en niet enkel op basis van incidenten. Daar waar de dreiging zich ontwikkelt, blijft het zaak om deze in een vroeg stadium te duiden en van een passend antwoord te voorzien. Vertrekpunt daarbij is het jaarlijkse CSBN. De editie van 2017 zal nog voor het zomerreces door de NCTV worden opgesteld en aan uw Kamer worden aangeboden.

Directie Cyber Security
Beleid

Datum
2 juni 2017

Ons kenmerk
2084119

De Staatssecretaris van Veiligheid en Justitie,

K.H.D.M. Dijkhoff