Ministerie van Buitenlandse Zaken

Aan de Voorzitter van de
Tweede Kamer der Staten-Generaal
Prinses Irenestraat 6
Den Haag

Directie Veiligheidsbeleid
Rijnstraat 8
2515 XP Den Haag
Postbus 20061
Nederland
www.rijksoverheid.nl

Onze Referentie
BZDOC-1235421577-13
Uw Referentie

Bijlage(n)
0

Datum 6 oktober 2021
Betreft Tegenmaatregelen *ransomware*-aanvallen

Geachte voorzitter,

In deze brief ga ik in op maatregelen die genomen kunnen worden in reactie op *ransomware*-aanvallen[1] van hackersgroepen. Daarmee kom ik tegemoet aan het verzoek in de motie van de leden Brekelmans en Mulder[2].

Beeld ransomware

Sinds enkele jaren neemt de dreiging van *ransomware*-aanvallen wereldwijd toe. Een uitgebreide duiding van deze dreiging is opgenomen in het Cybersecuritybeeld Nederland (CSBN) 2021, dat in juni met uw Kamer is gedeeld door de minister van Justitie en Veiligheid[3]. Eén van de conclusies van het CSBN 2021 is dat cybercriminaliteit de nationale veiligheid kan raken indien een aanval leidt tot omvangrijke schade, zoals door het verstoren van vitale processen. In een aantal gevallen genieten cybercriminelen bescherming van de staat van waaruit zij opereren of is er sprake van samenwerking.

Internationaalrechtelijk kader

Internationaal recht in het digitale domein
Het internationaal recht kent geen definitie van *ransomware*. Van geval tot geval zal moeten worden bekeken hoe *ransomware*-operaties kunnen worden gekwalificeerd. Allereerst dient duidelijk te zijn of er sprake is van een schending van internationaal recht en zo ja, welke juridische kwalificatie hierbij hoort. Vervolgens kan worden gekeken welke reactie gepast wordt geacht. Mede dankzij de Nederlandse inzet hebben in maart 2021 alle VN-lidstaten bevestigd dat het bestaand internationaal recht van toepassing is in het cyberdomein.

[1] *Ransomware* is het met crimineel oogmerk versleutelen van bestanden en systemen om losgeld te eisen voor het weer toegankelijk maken ervan.
[2] Kamerstuk 21501-02, nr. 2387
[3] Bijlage bij Kamerstuk 26643, nr. 767

Tegenmaatregelen
Het internationaalrechtelijk kader biedt de mogelijkheid om onder bepaalde omstandigheden tegenmaatregelen te nemen. De regering hanteert voor "tegenmaatregelen" in de cybercontext de definitie uit het staatsaansprakelijkheidsrecht. Dat wil zeggen dat tegenmaatregelen handelingen (of het nalaten van handelingen) zijn die normaliter een schending zouden opleveren van een internationaalrechtelijke verplichting, maar die geoorloofd zijn omdat zij een reactie zijn op een eerdere schending van een internationaalrechtelijke verplichting door een andere staat. Voor het volledige standpunt van de regering inzake de toepassing van internationaal recht in het digitale domein, verwijs ik u graag naar de bijlage bij de Kamerbrief inzake internationale rechtsorde in het digitale domein van 5 juli 2019[4].

Een *ransomware*-operatie wordt veelal uitgevoerd voor financieel gewin door niet-statelijke actoren. Een handeling van een niet-statelijke actor is in beginsel niet toerekenbaar aan een staat, tenzij een staat effectieve controle uitoefent over die handeling, dan wel de handeling achteraf aanvaardt als zijn eigen handeling. Dit betekent dat de niet-statelijke actor de operatie uitvoert op expliciete instructie van of onder controle van de staat. Dergelijke instructie of controle is vaak moeilijk aan te tonen. Daardoor is het juridisch toerekenen van een handeling van een niet-statelijke actor aan een staat meestal niet eenvoudig.

Zorgvuldigheidsbeginsel
In situaties waarbij toerekening in juridische zin niet mogelijk blijkt, kan het wenselijk zijn om in het kader van het staatsaansprakelijkheidsrecht te kijken naar een mogelijke schending van het zorgvuldigheidsbeginsel. Het zorgvuldigheidsbeginsel houdt in dat van staten verwacht wordt dat zij bij het uitoefenen van hun soevereiniteit rekening houden met de rechten van andere staten. Staten hebben de plicht om op te treden wanneer zij kennis hebben van het gebruik van hun grondgebied op een manier die de rechten van een derde staat schaadt. Het niet naleven van deze verplichting is een schending van een internationaalrechtelijke verplichting.

Noodzaak
Onder strikte voorwaarden is noodzaak (*necessity*) een rechtvaardigingsgrond voor handelen dat onder andere omstandigheden als internationaal onrechtmatig zou worden bestempeld, zoals bijvoorbeeld het inzetten van offensieve cybermiddelen tegen een andere staat. Noodzaak kan slechts in uitzonderlijke gevallen worden ingeroepen. Voor de precieze voorwaarden verwijs ik u graag naar de reeds genoemde bijlage van de Kamerbrief uit 2019.

Normatief kader

Normen voor verantwoord gedrag van staten in het digitale domein
Complementair aan de toepasselijkheid van het internationale recht in het digitale domein zet Nederland zich in voor de ontwikkeling van en steun voor vrijwillige, niet-bindende gedragsnormen voor staten in het cyberdomein. Nederland speelt een actieve rol in internationale onderhandelingen over deze gedragsnormen, onder andere binnen de werkgroepen van de Algemene Vergadering van de VN[5]. Daarbij

[4] Kamerstuk 33694, nr. 47
[5] Zoals de *UN Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security*, waarin van 2019-2021 een groep

zijn de consensusrapporten van de UN Group of Governmental Experts (UNGGE) 2010, 2013 en 2015[6] leidend, evenals het recent aangenomen consensusrapport van de UNGGE dat aangeboden zal worden aan de 76ste sessie van de Algemene Vergadering van de VN.

Met het eindrapport van de Open Ended Working Group (OEWG)[7], dat in maart jl. met consensus werd aangenomen, hebben alle VN-lidstaten de conclusies van het werk van de UNGGE onderschreven. Alle VN-lidstaten kunnen nu worden gehouden aan deze maatstaf van verantwoord statelijk gedrag in het digitale domein. Dit biedt mogelijkheden voor het adresseren van *ransomware*-aanvallen. Het eindrapport bevestigt immers de verontrustende trend in de toename van incidenten veroorzaakt door statelijke en niet-statelijke actoren. Daarbovenop komt dat sommige niet-statelijke actoren capaciteiten hebben ontwikkeld die eerder enkel aan staten voorbehouden waren.

Meer concreet zij gewezen op de volgende normen uit het UNGGE-rapport van 2015, zoals nu door de OEWG herbevestigd:

- Norm 13.c. houdt in dat staten hun grondgebied niet bewust mogen laten gebruiken voor internationaal onrechtmatige daden waarbij informatie- en communicatietechnologieën gebruikt worden. Nederland ziet deze norm tevens als internationaal juridische verplichting, hierover kon in VN-verband (nog) geen consensus worden bereikt.
- Norm 13.f. is er op gericht staten ervan te weerhouden ICT-activiteiten uit te voeren of bewust te ondersteunen die de kritieke infrastructuur van andere staten intentioneel beschadigen of anderszins schaden.

Nederland zal de komende tijd inzetten op handvatten voor concrete implementatie van de normen, waarbij prioriteit gegeven wordt aan het initiatief voor een "*Programme of Action to Advance Responsible State Behaviour in Cyberspace*" binnen de VN. Nederland zal hierbij bijzondere aandacht besteden aan de implementatie van normen die relevant zijn voor *ransomware*.
Eind 2020 heeft de regering uw Kamer geïnformeerd over de Nederlandse inzet op de internationale rechtsorde in het digitale domein[8].

Diplomatieke responsopties tegen ransomware

Voor de implementatie van normen in cyberspace, ook als het gaat om *ransomware*, is het van belang dat staten worden aangesproken als zij de normen overtreden. Zoals hierboven uiteengezet is het optreden tegen grensoverschrijdende criminele cyberoperaties vanaf eigen grondgebied voor veel landen in het normatieve kader van de VN een prioriteit. Als hiervan sprake is bij een *ransomware*-aanval kunnen landen daar dus ook op worden aangesproken. Dit kan bilateraal of via publieke verklaringen. En het kan gepaard gaan met maatregelen als sancties.

---

cyberexperts uit 25 VN-lidstaten, waaronder Nederland, bijeenkwam. Group of Governmental Experts – UNODA

[6] UNGGE Consensus rapport 2009/2010, A/65/201, 2012/2013, A/68/98*, 2014/2015, A/70/174.

[7] *United Nations Open Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*, opgericht in 2019 op initiatief van de Russische Federatie en bestaande uit het gehele VN-lidmaatschap. Het eindrapport is in maart 2021 met consensus aangenomen.

[8] Kamerstuk 33694, nr. 60

Dergelijke diplomatieke reacties zijn krachtiger als ze in breed coalitieverband worden vormgegeven. Binnen de EU is Nederland daarom een drijvende kracht geweest achter de *EU Cyber Diplomacy Toolbox*[9] en de aanname van het EU-cybersanctieregime in mei 2019 en zet Nederland in op de doorontwikkeling van deze instrumenten. De EU heeft hiermee goede instrumenten in handen om sneller en krachtiger te reageren op cyber-incidenten. Uit recente EU-verklaringen en sancties blijkt dat deze instrumenten tot concrete resultaten leiden. Zo heeft de EU zich uitgesproken over de *Solar Winds* hack[10] en, nog recenter, over kwaadwillende cyberoperaties vanaf Chinees grondgebied.

Het cybersanctieregime is ook al diverse malen ingezet: in 2020 legde de EU bijvoorbeeld sancties op aan een Noord-Koreaanse organisatie die de "*Wannacry*" *ransomware*-aanvallen in 2017 uitvoerde, waarbij wereldwijd honderdduizenden Microsoft-computers getroffen werden. Tot de opgelegde sancties behoren een inreisverbod en de bevriezing van financiële tegoeden. Daarnaast is het personen en entiteiten uit de EU verboden middelen ter beschikking te stellen aan personen en entiteiten waartegen sancties gelden. De sancties die onder het EU cyber-sanctieregime worden opgelegd zijn gericht tegen specifieke personen en entiteiten, niet tegen landen.

Een andere diplomatieke maatregel die kan worden ingezet tegen *ransomware* is het via diplomatieke kanalen aandringen op bilaterale medewerking van landen bij justitiële onderzoeken tegen *ransomware*. Dit kan nuttig zijn als de medewerking via de internationale justitiële kanalen onvoldoende is. Nederland kan dan via diplomatieke weg het belang dat aan medewerking wordt gehecht, kracht bijzetten.

De keuze om over te gaan tot een diplomatieke maatregel vergt integrale afweging en weloverwogen besluitvorming, in samenspraak met de betrokken departementen. Bij deze afweging spelen ernst en impact van de *ransomware*-aanval een rol. Bovendien is van belang in welke mate Nederland de *ransomware*-aanval kan toerekenen aan een actor, op basis van onderzoek door de politie of inlichtingen- en veiligheidsdiensten (I&V).

Zoals hierboven uiteengezet, streeft Nederland ernaar om diplomatieke stappen tegen normoverschrijdend gedrag in het digitale domein door staten zoveel mogelijk in coalitieverband te zetten. Om coalitievorming te bevorderen, blijft Nederland zich daarom inzetten voor gezamenlijke ontwikkeling van responsopties en kennisdeling binnen de EU, de NAVO en andere samenwerkingsverbanden met bondgenoten. Ook capaciteitsopbouw en diplomatieke contacten met derde landen die traditioneel een minder uitgesproken profiel kunnen of willen aannemen in het internationale debat over cyber is onderdeel van de Nederlandse inzet. Dit gebeurt bijvoorbeeld door middel van trainingen en andere bewustwordingsactiviteiten om cyberweerbaarheid te verhogen, onder meer via het *Global Forum on Cyber Expertise*.

[9] De EU Cyber Diplomacy Toolbox is het beleidsraamwerk voor gezamenlijke EU-respons tegen kwaadaardige cyberactiviteiten, aangenomen in 2017. De toolbox biedt mogelijkheid tot het inzetten van vijf soorten maatregelen: preventieve maatregelen; samenwerkingsmaatregelen; stabiliteitsmaatregelen; restrictieve maatregelen (zoals sancties); en het ondersteunen van rechtmatige respons van individuele lidstaten.
[10] Waarbij kwaadwillende actoren ongeautoriseerd toegang konden verkrijgen tot systemen waar bepaalde versies van SolarWinds-software op waren geïnstalleerd.

Naast de diplomatieke maatregelen die hierboven beschreven zijn, zet het kabinet in algemene zin in op een verhoging van de digitale weerbaarheid van Nederland. Om de cybersecurity van Nederland te vergroten en cybercrime tegen te gaan, neemt het kabinet diverse maatregelen in het kader van de Nationale Cyber Security Agenda (NCSA) en de integrale aanpak van cybercrime. Voorbeelden van maatregelen die worden genomen, zijn het bevorderen van veilige hard- en software, bewustwordingsactiviteiten en het versterken van de mogelijkheden voor de opsporing. De minister van Justitie en Veiligheid heeft u recent geïnformeerd over de stand van zaken van deze maatregelen in de voortgangsrapportage van de NCSA en de voortgangsrapportage van de integrale aanpak van cybercrime[11].

Bij veel succesvolle cyberaanvallen, waaronder *ransomware*, blijkt dat basismaatregelen voor *cybersecurity* onvoldoende zijn genomen. Daarbij lijken veel ondernemers, met name in het MKB, zichzelf niet als potentieel slachtoffer van *ransomware* te zien. Het *Digital Trust Center* (DTC) van het Ministerie van Economische Zaken en Klimaat zet daarom in op voorlichting over *ransomware*, onder andere door het delen van verhalen van ondernemers die slachtoffer zijn geworden van *ransomware*.

In de meeste gevallen wordt een *ransomware*-aanval gepleegd door criminele actoren en zijn statelijke actoren niet direct betrokken. In die gevallen is er meestal ook geen sprake van een dreiging voor de nationale veiligheid. Het is dan primair aan de politie en het OM om te acteren in het kader van opsporing en vervolging. Ook in gevallen waarbij mogelijk wel sprake is van betrokkenheid van staten zijn de politie en het OM in beginsel bij het onderzoek betrokken.

Indien een *ransomware*-aanval, al dan niet met een financieel oogmerk, de drempel passeert van een (zich manifesterende) dreiging voor de nationale veiligheid, bijvoorbeeld door het uitvallen van vitale sectoren, dan staan de overheid ook andere middelen ter beschikking. In dat geval kan de inzet van de I&V-diensten en de krijgsmacht in beeld komen. Zo stelt de Wiv 2017 de diensten onder meer in staat tot het verrichten van attributieonderzoek en tot handelend optreden. Een voorbeeld van het laatste is het offline (laten) halen van ICT-infrastructuur die onderdeel is van aanvalsinfrastructuur of misbruikt wordt voor digitale spionage of sabotage. Naast het optreden door I&V-diensten kan Nederland ook met de krijgsmacht reageren. Zo kan het Defensie Cyber Commando *ad ultimo* een tegenaanval uitvoeren om een vijandelijke actie af te wenden of om een essentieel belang van de staat te beschermen. Voor een tegenaanval vanuit de krijgsmacht zijn een internationale rechtsgrond, bijvoorbeeld noodzaak zoals bovenstaand beschreven, en een regeringsbesluit nodig.

Bovenstaande mogelijkheden zoals opsporing en vervolging door OM en politiediensten, de inzet van de bevoegdheden van de I&V-diensten en terugslaan door de krijgsmacht versterken het afschrikkend vermogen van Nederland. Hierbij moet worden opgemerkt dat een eventuele reactie niet domein-gebonden is, met andere woorden: ongewenste cyberactiviteiten worden niet per se beantwoord met Nederlandse cyberactiviteiten maar kunnen ook langs diplomatieke of juridische weg beantwoord worden. Andersom kan Nederland ook reageren met cybermiddelen als er dreigingen komen vanuit een ander domein.

[11] Kamerstuk 26643, nrs. 767 en 768

Directie Veiligheidsbeleid

Onze Referentie
BZDOC-1235421577-13

Tot slot

Het Cybersecuritybeeld Nederland 2021 concludeert dat een aantal cybercriminele groepen inmiddels beschikt over capaciteiten die niet onderdoen voor het niveau van statelijke actoren. Dit impliceert dat de impact van hun aanvallen een vergelijkbare dreiging kan vormen voor de nationale veiligheid door de inzet van *ransomware*. Hoewel dit zich in Nederland nog niet heeft gemanifesteerd, komt deze dreiging bovenop de al bestaande, continu toenemende, dreiging in het cyberdomein. De opsporingsdiensten, de I&V-diensten en de krijgsmacht zijn vooralsnog onvoldoende toegerust om structureel op te treden tegen actoren die door een *ransomware*-aanval een dreiging vormen voor de nationale veiligheid. Om de kosten van kwaadwillend gedrag in het digitale domein, waaronder *ransomware*-aanvallen, te verhogen en de kans op schade te verkleinen is het noodzakelijk om de aanpak van *ransomware*, zowel diplomatiek als op de andere terreinen die hierboven zijn omschreven, onder een nieuw kabinet te verstevigen.

De minister van Buitenlandse Zaken,

Ben Knapen