Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

30 821 Nationale Veiligheid

Nr. 239 **BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 27 september 2024

Met deze brief informeer ik uw Kamer over een casus waarin het Nationaal Cybersecurity Centrum (NCSC) informatie heeft gedeeld met een aantal landen. Het gaat hier om informatie over computersystemen waar een Chinese statelijke actor toegang tot heeft gekregen voor spionagedoeleinden.[1] Met deze informatie zijn deze landen in staat gesteld om maatregelen te nemen tegen deze cyberaanval. De informatie is ook gedeeld met de nationale computercrisisteams van vier niet-EU-landen: Canada, Japan, het Verenigd Koninkrijk en de Verenigde Staten. Het NCSC heeft echter geen wettelijke grondslag om dergelijke informatie met deze vier landen te delen. Daarom stel ik uw Kamer daarvan op de hoogte, gekoppeld aan de maatregelen die ik heb ingesteld om dit in de toekomst te voorkomen.

Aanleiding

U bent door de Minister van Defensie op 6 februari 2024 geïnformeerd over de onderkende Chinese spionagecampagne bij Defensie.1 Op deze datum is tevens een rapport van de Militaire Inlichtingen- en Veiligheidsdienst (MIVD), de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en het NCSC gepubliceerd over deze geavanceerde Chinese malware.[2] Deze zogenaamde COATHANGER-campagne, maakt gebruik van een kwetsbaarheid in FortiGate-systemen en is aangetroffen op een losstaand Defensie-netwerk. Op 10 juni 2024 is nogmaals aandacht gevraagd voor deze spionagecampagne met een nieuwsbericht uitgebracht door MIVD, AIVD en NCSC en is bekend gemaakt dat deze statelijke actor zowel in

[1] Kamerstuk 36 410 X, nr. 73

[2] TLP:CLEAR MIVD AIVD Advisory Coathanger | Publicatie | Nationaal Cyber Security Centrum (ncsc.nl)

kst-30821-239
ISSN 0921 - 7371
's-Gravenhage 2024

2022 als in 2023 binnen enkele maanden toegang heeft verkregen tot ten minste 20.000 FortiGate-systemen wereldwijd.[3]

De MIVD heeft op verzoek van het NCSC lijsten opgesteld met IP-adressen van FortiGate-systemen waar de statelijke actor zich (mogelijk) toegang tot verschaft heeft. Deze informatie is gedeeld met het NCSC met als doel om de slachtoffers te informeren zodat zij adequate tegenmaatregelen kunnen nemen. Het is gebruikelijk dat nationale computercrisisteams, zoals het NCSC in Nederland, elkaar informeren wanneer zij op de hoogte zijn van kwetsbare of gecompromitteerde systemen binnen hun doelgroep. Om die reden heeft het NCSC lijsten met voor deze landen gerelateerde IP-adressen gedeeld, waarbij elk land enkel de voor hen relevante IP-adressen heeft ontvangen. Naast het delen van deze informatie met landen binnen de EU waarvoor een wettelijke grondslag bestaat, is deze informatie ook gedeeld met vier landen buiten de EU waarvoor dat niet geldt.

Procedure binnen het NCSC

Voor het besluit tot het delen van (mogelijke) persoonsgegevens, zoals een IP-adres, of vertrouwelijke tot aanbieders herleidbare gegevens, hanteert het NCSC processen om dit zorgvuldig en rechtmatig te doen. Hierbij wordt gekeken of de informatie gedeeld kan worden met een specifiek belanghebbende binnen het wettelijk kader van het NCSC of door een andere partij met de juiste bevoegdheid. In het geval dat hierover twijfel bestaat of wanneer dit niet kan, maar er zwaarwegende uitzonderlijke (cyber)risico's zijn, wordt over het eventuele vervolg hierop advies gevraagd aan juristen en bestuurlijk adviseurs van NCSC en NCTV. In dit geval is deze procedure zoals boven aangegeven niet gevolgd. Dat heeft te maken met de hieronder genoemde urgentie en context waarbinnen deze informatiedeling heeft plaats gevonden.

Context bij deling informatie

De ernst van de Chinese cyberspionagecampagne is de reden geweest dat het NCSC over is gegaan tot het delen van informatie met de relevante organisaties. Deze keuze om informatie te delen bleek naderhand zonder grondslag te zijn. De doelwitten bestaan uit onder meer tientallen (Westerse) overheden, internationale organisaties en een groot aantal bedrijven binnen de defensie-industrie. De campagne was zeer omvangrijk, met meer dan twintigduizend mogelijk compromitteerde systemen wereldwijd. Ook is de gebruikte spionagesoftware zeer moeilijk te onderkennen binnen een netwerk zonder precies te weten in welk systeem deze zich bevindt. Daarom is het verstrekken van specifieke IP-adressen noodzakelijk om adequate tegenmaatregelen te kunnen nemen, zoals in dit geval is gebeurd.

Juridisch kader

Het NCSC heeft op grond van artikel 3, eerste lid, Wet beveiliging netwerk- en Informatiesystemen (Wbni) primair tot taak om vitale aanbieders en rijksoverheidsorganisaties in Nederland bijstand te verlenen, waaronder het verstrekken van dreigings- of incidentinformatie (met inbegrip van bijvoorbeeld persoonsgegevens). Ook kan het NCSC andere organisaties informeren over dreigingen en incidenten bij genoemde vitale aanbieders en rijksoverheidspartijen in Nederland. Daarnaast heeft het NCSC op grond van artikel 3, tweede lid, Wbni de taak om dreigings- en incidentin-

[3] Aanhoudende statelijke cyberspionagecampagne via kwetsbare edge devices | Nieuwsbericht | Nationaal Cyber Security Centrum (ncsc.nl)

formatie, die op systemen van andere organisaties dan de rijksoverheid of vitale aanbieders in Nederland ziet, te verstrekken aan onder de wet aangewezen (schakel)organisaties waarvan genoemde andere organisaties de achterban vormen. Aanvullend daarop geldt op grond van artikel 20, lid 2, Wbni dat bij verstrekking op basis van de in artikel 3 bedoelde taken vertrouwelijke tot aanbieders herleidbare gegevens slechts in beperkte kring kunnen worden verstrekt (CSIRTs van EU-lidstaten, inlichtingen- en veiligheidsdiensten, etc.).

In deze casus betroffen de IP-adressen, die met de computercrisisteams in niet-EU-landen zijn gedeeld, vertrouwelijke tot aanbieders herleidbare gegevens. Een IP-adres is een herleidbaar gegeven omdat het mogelijk is, via openbare informatie, te herleiden welke organisatie hieraan verbonden is. In dit geval is de informatie tevens vertrouwelijk omdat het informatie betreft over een incident. Daarnaast kan niet worden uitgesloten dat ook IP-adressen tot personen te herleiden zijn. Voor verstrekking van deze gegevens, in het geval van de computercrisisteams buiten de EU, is geen wettelijke basis, met name omdat deze niet bij of krachtens de Wbni zijn aangewezen als partijen waaraan op grond van voormelde artikelen 3 en 20 dergelijke informatie kan worden verstrekt. Conclusie is daarom dat de verstrekking van de IP-adressen aan de genoemde computercrisisteams buiten de EU zonder grondslag heeft plaatsgevonden. De gevolgtrekking van het niet uit kunnen sluiten of er sprake is van het lekken van persoonsgegevens maakt dat er sprake is van een datalek, dat gemeld is bij de Autoriteit Persoonsgegevens (AP).

Vervolg

Naar aanleiding van deze casus zijn binnen het NCSC extra waarborgen ingebouwd om te verzekeren dat de juiste procedures worden gevolgd. Dit behelst het verder aanscherpen van zowel technische als organisatorische maatregelen.

Het NCSC heeft haar werkproces voor informatiedeling aangescherpt. Ook zal het NCSC een opleidingstraject starten om de kennis van het handelings- en begrippenkader rondom informatiedeling doorlopend op peil te houden bij de verschillende organisatieonderdelen die hiermee te maken hebben tijdens werkzaamheden. Daarnaast is er een traject gestart voor het verbeteren van het proces met behulp van technische maatregelen, zoals het verbeteren van de geautomatiseerde registratie van feitelijke handelingen, het verbeteren van de vastlegging van besluitvorming en het verder structureren van overdrachtsvorming van cases tussen de verschillende functionarissen. Deze maatregelen worden geëvalueerd en zo nodig aangepast.

NIS2

Het wettelijk kader waarbinnen het NCSC opereert zal binnenkort wijzigen als gevolg van de Nederlandse implementatie van de herziene netwerk- en informatiebeveiligingsrichtlijn (NIS2-richtlijn) via het wetsvoorstel voor de Cybersecuritywet (Cbw), die voor de zomer in consultatie is geweest. De NIS2-richtlijn biedt aan lidstaten meer mogelijkheden om informatie met landen buiten de EU te delen. Het werkproces en het kader zullen door het NCSC aan de nieuwe wetgeving worden aangepast.

De Minister van Justitie en Veiligheid,
D.M. van Weel