Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 740

BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 5 februari 2021

Met deze brief wordt uw Kamer geïnformeerd over de recente ontwikkelingen rondom de hack op het Amerikaanse bedrijf SolarWinds, als gevolg waarvan een ernstige kwetsbaarheid in de software SolarWinds Orion is ontstaan. In deze brief wordt ingegaan op de gevolgen voor Nederland, en de genomen maatregelen en vervolgstappen.

Aanleiding

Het bedrijf SolarWinds biedt het product Orion aan waarmee IT-omgevingen kunnen worden gemonitord en beheerd. Door een nog onbekende methode is tussen maart en juni 2020 een versie van Orion verspreid waarin een moedwillige kwetsbaarheid blijkt te zitten. Volgens SolarWinds is de kwetsbaarheid opzettelijk gecreëerd door een actor, met als achterliggend doel om de systemen te compromitteren van de afnemers van de betreffende versie van SolarWinds Orion[1]. Op 13 december jl. verscheen dit nieuws in de internationale media. Deze kwetsbaarheid kan door kwaadwillenden worden misbruikt om toegang te krijgen tot bijvoorbeeld informatie of beheersfuncties van organisaties. SolarWinds heeft verklaard dat potentieel 18.000 klanten in verschillenden landen de kwetsbare versies in gebruik hebben genomen en dat het bedrijf deze klanten daarover benaderd heeft[2]. De VS heeft bekendgemaakt dat bij Amerikaanse overheidsinstellingen misbruik van de kwetsbaarheid is geconstateerd en dat sprake is van een ernstig incident.

Duiding

In het Cybersecurity Beeld Nederland (CSBN) 2020 (Kamerstuk 26 643, nr. 695), en in eerdere edities daarvan, wordt gewezen op de dreiging die uitgaat van het moedwillig misbruik maken van kwetsbaarheden in

[1] https://www.solarwinds.com/securityadvisory#anchor2
[2] https://www.security.nl/posting/681922/SolarWinds:+ongeveer+18_000+klanten+getroffen+door+backdoor

kst-26643-740
ISSN 0921 - 7371
's-Gravenhage 2021

producten. In het CSBN wordt onder andere in dat kader ook gewezen op de risico's die hiervan uitgaan. Zo vormen spionage en (voorbereidingen voor) sabotage van digitale diensten, processen en systemen een dreiging voor de nationale veiligheid. In het CSBN wordt daarnaast ook gemeld dat actoren nog steeds zoeken naar zwakke schakels in de leveranciersketen als opstap naar interessante doelwitten. Hier lijkt de moedwillige kwetsbaarheid in SolarWinds Orion een voorbeeld van te zijn.

Situatie in Nederland

SolarWinds levert het product Orion ook aan klanten in Nederland. Het Nationaal Cyber Security Centrum[3] doet naar aanleiding daarvan, in afstemming met andere (operationele) organisaties waaronder de AIVD, onderzoek in het kader van hun wettelijke taken. Het Nationaal Cyber Security Centrum (NCSC) heeft zijn doelgroep (Rijk en vitaal) alsmede andere schakelorganisaties binnen het Landelijk Dekkend Stelsel van cybersecurity samenwerkingsverbanden (LDS) via berichtgeving op 14, 15, 19, 22 en 24 december 2020 geïnformeerd en bijbehorend advies geboden[4]. Bij het NCSC is tot op heden op basis van meldingen gebleken dat een aantal organisaties, die onderdeel zijn van de doelgroep van het NCSC (Rijk en Vitaal), de kwetsbare versie van Orion hadden geïnstalleerd. Op basis van het actuele beeld lijkt er vooralsnog geen sprake van daadwerkelijk misbruik van de kwetsbaarheid bij deze organisaties. De betreffende organisaties hebben tevens bij het NCSC gemeld dat zij inmiddels mitigerende maatregelen hebben genomen, monitoring hebben toegepast en aanvullend onderzoek doen. Het NCSC doet nader onderzoek, staat hierover waar nodig in contact met zijn doelgroep (Rijk en Vitaal), en verleent hen bijstand indien daar aanleiding toe is.

Voor organisaties die geen deel uitmaken van de doelgroep van het NCSC, vindt informatievoorziening vanuit het NCSC plaats aan informatieknooppunten binnen het LDS – zoals het Digital Trust Center (DTC) en computercrisisteams – die tot taak hebben om die andere organisaties te informeren. Deze informatieknooppunten zijn, zoals hierboven aangegeven, geïnformeerd naar aanleiding van de kwetsbaarheid in SolarWinds Orion. Specifiek voor het niet-vitale bedrijfsleven heeft het DTC informatie en advies hierover op haar website gepubliceerd[5].

Tot slot is het belangrijk te benadrukken dat alle organisaties primair zelf verantwoordelijk zijn voor de beveiliging van hun digitale infrastructuur. Het is vanuit deze eigen verantwoordelijkheid van belang dat zij rekening houden met de beveiligingsadviezen van onder meer het NCSC en het DTC, deze adviezen waar aangewezen opvolgen en bij gebruik van de kwetsbare versie eigen onderzoek doen naar sporen van misbruik.

Het beeld ten aanzien van de rijksoverheid

De Staatssecretaris van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) meldt dat bij CIO Rijk de CISO Rijk een inventarisatie bij de rijksoverheid heeft uitgevoerd naar aanleiding van de kwestie rondom SolarWinds Orion. Uit het resultaat van de inventarisatie bij de Rijkoverheid blijkt dat enkele Rijksoverheidsorganisaties de kwetsbare software hadden geïnstalleerd. Alle systemen waarop de kwetsbare versie was geïnstalleerd, die naar voren kwamen in de inventarisatie, zijn

---

[3] Het NCSC is het Computer Emergency Response Team (CSIRT) voor de rijksoverheid en vitale aanbieders

[4] NCSC adviezen te raadplegen via: https://advisories.ncsc.nl/advisory?id=NCSC-2020–1021

[5] Te raadplegen via: https://www.digitaltrustcenter.nl/nieuws/misbruik-van-achterdeur-in-software-van-solarwinds

inmiddels gerepareerd. Aanvullend onderzoek naar daadwerkelijk misbruik van de kwetsbaarheid is uitgevoerd en tot nog toe zijn geen sporen van misbruik bekend. De bevindingen van het NCSC ten aanzien van de doelgroep rijksoverheid komen daarmee overeen met de door CISO Rijk uitgevoerde inventarisatie. Over de resultaten hiervan is goed contact geweest tussen CISO Rijk en het NCSC. In de gesprekken tussen CISO Rijk en de verschillende departementen zullen eventuele ontwikkelingen rondom deze casus besproken worden.

Naar aanleiding van de casus SolarWinds kan ik aanvullend vermelden dat ik van het Ministerie van Defensie heb vernomen, in het kader van zijn wettelijke taken in het cyberdomein, dat het geen gebruik maakt van het softwarepakket waar de kwetsbaarheid in verborgen zat.

Defensie staat in verband met haar hoofdtaken gereed om, via de geëigende kanalen en binnen de bestaande afspraken en structuren, eventuele bijstand te kunnen verlenen. Tot op heden is dat niet nodig gebleken.

Het beeld ten aanzien van de medeoverheden

Eveneens is onder verantwoordelijkheid van de Staatssecretaris van BZK een uitvraag gedaan bij de CERT's en informatieknooppunten van de medeoverheden. Dit zijn de Informatiebeveiligingsdienst (IBD) als CERT voor alle gemeenten, het CERT Watermanagement voor de waterschappen en het Centraal Informatiebeveiligingsoverleg (CIBO) van de provincies als informatieknooppunt. De respons op de uitvraag levert het beeld op dat enkele organisaties binnen de scope van deze uitvraag gebruik maakten van de kwetsbare software. Ook bij deze organisaties is vooralsnog geen misbruik bekend. Het beeld is dat zij de algemene adviezen die zijn uitgebracht door het NCSC hieromtrent opvolgen.

Vervolg

Het NCSC zal de situatie nauwlettend blijven monitoren en, indien daartoe aanleiding is, bovenbedoelde adviezen blijven actualiseren. Hierover is nauw contact met onder meer de andere overheidspartijen die deelnemen aan de samenwerking in de CIIC[6] en ook met de internationale partners.

Deze kwetsbaarheid en de impact op organisaties wereldwijd onderstrepen het belang van digitale veiligheid. De toenemende complexiteit en afhankelijkheid van derden vraagt om structurele aandacht voor en samenwerking op het gebied van cybersecurity in Nederland. Deze kwestie bevestigt eveneens hoe belangrijk onze digitale weerbaarheid is, en de noodzaak hierop te blijven inzetten. Het kabinet geeft deze inzet vorm via de Nederlandse Cyber Security Agenda (NCSA) uit 2018. Recentelijk bent u in de Kamerbrief «Verkenning wettelijke taken en bevoegdheden digitale weerbaarheid, en beleidsreacties WODC-rapporten» (Kamerstuk 26 643, nr. 738) geïnformeerd over verschillende trajecten aangaande het thema digitale weerbaarheid.

In juni van dit jaar zal de jaarlijkse voortgangsrapportage over de NCSA u toekomen.

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

---

[6] https://www.ncsc.nl/actueel/nieuws/2020/juni/18/versterkte-samenwerking-voor-een-digitaal-veilig-nederland