Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2019–2020

# 26 643 Informatie- en communicatietechnologie (ICT)

**Nr. 666**

## BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 11 februari 2020

Tijdens het mondelinge vragenuur op 1 oktober jl. gaf ik aan een analyse te laten verrichten van de gelopen risico's door de kwetsbaarheden in de virtual private network (VPN) software van het bedrijf Pulse Secure (Handelingen II 2019/20, nr. 7, item 2). Hierbij bied ik uw Kamer de conclusies van deze analyse aan.

### Kwetsbaarheden in VPN-software

Een VPN is een technische oplossing om een (beveiligde) verbinding op te zetten tussen verschillende systemen of netwerken over het internet, bijvoorbeeld om computers buiten een bedrijfsnetwerk op een veilige manier toegang te geven tot (onderdelen van) het interne bedrijfsnetwerk. In het geval van Pulse Secure zaten er kwetsbaarheden in oudere versies van de VPN-software. Kwaadwillenden kunnen via deze kwetsbaarheden toegang verkrijgen tot interne netwerksystemen van personen en organisaties die gebruik maken van deze kwetsbare software. Iedere soort software kan kwetsbaarheden bevatten die misbruikt kunnen worden.

De NCTV stelt jaarlijks een cybersecuritybeeld op om inzicht te geven in dreigingen, belangen en weerbaarheid op het gebied van cybersecurity in relatie tot de nationale veiligheid. In het Cybersecuritybeeld Nederland 2019[1] wordt geschetst dat sprake is van een toenemende digitale dreiging, met als grootste dreiging voor de nationale veiligheid, de dreiging die van statelijke actoren uitgaat. Daarnaast blijft ook de dreiging vanuit criminelen onverminderd groot. Kwetsbaarheden in software zijn niet te voorkomen. Om de weerbaarheid tegen digitale dreigingen, waaronder ook deze kwetsbaarheden, te versterken heeft het kabinet de Nederlandse Cybersecurity Agenda (NCSA)[2] en een versterkte aanpak

[1] Kamerstuk 26 643, nr. 614.
[2] Kamerstuk 26 643, nr. 536.

kst-26643-666
ISSN 0921 - 7371
's-Gravenhage 2020

cybersecurity met vier actielijnen opgesteld.[3] Belangrijk uitgangspunt is dat organisaties zelf primair verantwoordelijk zijn voor het beveiligen van hun digitale systemen, bijvoorbeeld door het regelmatig en tijdig uitvoeren van beveiligingsupdates in hun software.

**Kwetsbaarheid Pulse Secure VPN-software**

Op 24 april 2019 publiceerde de producent van VPN-software, Pulse Secure, een artikel op hun website waarin werd gemeld dat een update beschikbaar was gesteld voor een op 22 maart 2019 ontdekte kwetsbaarheid. Dit artikel is op 1 mei 2019 onder aandacht van het Nationaal Cyber Security Centrum (NCSC) gekomen. Op basis hiervan is een beveiligingsadvies opgesteld, dat op de site van het NCSC is gepubliceerd,[4] en zijn organisaties die onderdeel zijn van de rijksoverheid en vitale aanbieders (Rijk en vitaal) hierover nader geïnformeerd. Omdat er op dat moment geen «exploitcode» beschikbaar was om de kwetsbaarheid daadwerkelijk te kunnen misbruiken, werd de kwetsbaarheid op dat moment geclassificeerd als *medium/high*. Classificatie *medium/high* betekent dat de kans op misbruik gemiddeld is en de schade aan het systeem bij misbruik hoog wordt geacht. Het verschil dat een exploitcode maakt is dat zonder die code de kwetsbaarheid zelf wel bekend is, maar nog niet bekend is hoe deze misbruikt kan worden.

In augustus 2019 is er een exploitcode bekend geworden. Daarop heeft het NCSC op 21 augustus 2019 de kwetsbaarheid opnieuw beoordeeld en de classificatie verhoogd naar *high/high*, de hoogste classificatieklasse. Naast publicatie van het *high/high* beveiligingsadvies[5] door het NCSC op zijn website, zijn organisaties binnen Rijk en vitaal waarvan bekend was dat ze gebruik maakten van de betreffende software telefonisch door het NCSC geïnformeerd. Omdat het NCSC ook van kwetsbaarheden in systemen buiten Rijk en vitaal is gebleken, is deze informatie gedeeld met enkele andere organisaties waarvan bijvoorbeeld binnen hun doelgroep de software mogelijkerwijs ook in gebruik was. Op basis van later in augustus ontvangen aanvullende informatie over kwetsbare systemen in Nederland, heeft het NCSC wederom een aantal organisaties binnen Rijk en vitaal en enkele andere bovenbedoelde organisaties nader geïnformeerd. Ook na augustus heeft het NCSC steeds, indien op basis van nieuwe informatie daar aanleiding toe was, bovengenoemde organisaties geïnformeerd. Ook is in breder verband algemene informatie over de kwetsbaarheid gedeeld met andere samenwerkingspartners. Het Computer Security Incident Response Team voor digitale diensten (CSIRT-DSP, onderdeel van het Ministerie van EZK)[6] heeft naar aanleiding van de van het NCSC ontvangen informatie contact gelegd met een tiental digitale dienstverleners die mogelijk kwetsbare VPN-systemen in hun netwerk hadden staan.[7]

Ook bij onderdelen die onder het Ministerie van Justitie en Veiligheid vallen, is sprake geweest van de kwetsbaarheid in de VPN-software. Na de eerste waarschuwing van het NCSC op 1 mei 2019 zijn binnen mijn ministerie voor bijna alle onderdelen updates doorgevoerd. Toen het advies van het NCSC op 21 augustus 2019 werd omgezet in het *high/high* beveiligingsadvies bleek op aangeven van het NCSC dat nog twee

---

[3] Kamerstuk 26 643, nr. 614 en Kamerstuk 26 643, nr. 647.

[4] https://advisories.ncsc.nl/advisory?id=NCSC-2019-0353&version=1.00&format=plain.

[5] https://advisories.ncsc.nl/advisory?id=NCSC-2019-0353&version=1.01&format=plain.

[6] https://www.csirtdsp.nl.

[7] Digitale dienstverleners zijn aanbieders van clouddiensten, online zoekmachines en online marktplaatsen. Ze worden ook DSP's genoemd, oftewel Digital Service Providers. Zie ook art. 1 Wbni.

resterende onderdelen de updates op dat moment niet hadden doorgevoerd. Deze onderdelen hebben binnen enkele dagen na dit *high/high* beveiligingsadvies de kwetsbaarheid met spoed verholpen middels een update. Dit is binnen de richtlijn van een week die de Baseline Informatiebeveiliging Overheid (BIO) stelt voor dit soort beveiligingsadviezen.[8] Naar aanleiding van deze casus is met deze onderdelen gesproken en wordt nu geëvalueerd hoe in de toekomst dergelijke kwetsbaarheden sneller verholpen kunnen worden.

Het eind 2017 opgerichte Digital Trust Center (DTC; onderdeel van het Ministerie van EZK) beoogt als *one stop shop* de circa 1,8 miljoen bedrijven in Nederland die niet als vitaal zijn aangemerkt weerbaarder te maken tegen cyberdreigingen. Naar aanleiding van de verhoging van de classificatie van het beveiligingsadvies van het NCSC heeft het DTC zijn doelgroep zo breed en grootschalig mogelijk via diverse kanalen geïnformeerd.[9] Tevens heeft het DTC in de daarop volgende weken meermalig (media-)aandacht besteed aan de kwetsbaarheid en zijn doelgroep op de hoogte gehouden van de ontwikkelingen.

De AIVD en de MIVD hebben gesignaleerd dat statelijke actoren misbruik maken van de kwetsbaarheid in de Pulse Secure VPN-software. Daarom hebben de AIVD en MIVD ook bedrijven en andere organisaties geadviseerd over weerbaarheidsverhogende maatregelen.

Deze problematiek was tot slot wereldwijd aan de orde, zoals nagenoeg altijd het geval is bij digitale kwetsbaarheden. Zo hebben ook de Britse en Amerikaanse autoriteiten aandacht besteed aan deze kwetsbaarheid[10] waarbij ook is vermeld dat *advanced persistent threat*-actoren (APT's) kwetsbaarheden in VPN-software hebben misbruikt.

**Belang van versterkte aanpak cybersecurity**

In Nederland is voor zover mij bekend door deze kwetsbaarheid geen schade ontstaan bij de rijksoverheid of bij aanbieders in de vitale infrastructuur. Evenwel tonen de mogelijkheden tot misbruik van dit soort kwetsbaarheden het belang aan van alertheid en het tijdig ingrijpen door organisaties als zij door het NCSC, het DTC, het CSIRT-DSP of op andere wijze gewaarschuwd of geïnformeerd worden. Het signaleren van en het nemen van passende maatregelen ten aanzien van kwetsbaarheden, zoals die in de VPN-software van Pulse Secure, is primair de verantwoordelijkheid van iedere organisatie zelf, zowel binnen als buiten de rijksoverheid. De adviezen van bijvoorbeeld het NCSC en het DTC dragen er in belangrijke mate aan bij dat organisaties die verantwoordelijkheid kunnen nemen.

Buiten deze adviezen wordt er nog veel meer gedaan door de overheid om de digitale weerbaarheid in Nederland te verhogen. Deze casus en vergelijkbare kwetsbaarheden, zoals de kwetsbaarheid in Citrix producten waarover uw Kamer op 20 en 23 januari jl. geïnformeerd is,[11] laten zien hoe belangrijk het is om aan onze digitale weerbaarheid te blijven werken en hoe hard de kabinetsbrede investeringen en inzet op cybersecurity nodig zijn. Zoals ik in het kader van de versterkte aanpak van cyberse-

---

[8] https://bio-overheid.nl/media/1324/bio-v103.pdf, pagina 51, artikel 12.6.1.1.
[9] https://www.digitaltrustcenter.nl/actueel/nieuws/2019/09/30/index.
[10] https://www.ncsc.gov.uk/news/alert-vpn-vulnerabilities.
https://www.us-cert.gov/ncas/current-activity/2019/10/07/nsa-releases-advisory-mitigating-recent-vpn-vulnerabilities.
[11] Kamerstuk 26 643, nr. 658 en Kamerstuk 26 643, nr. 660.

curity[12] aangaf, versterk ik de regie op cybersecurity. Inzet is om de bewustwording van de risico's voor de digitale weerbaarheid te vergroten, de beheersmaatregelen en het toezicht te versterken, meer te oefenen en te testen en meer gebruik te maken van regie- en interventiemogelijkheden, dit alles om het digitale weerbaarheidsniveau structureel te verhogen. Onderdeel hiervan is bijvoorbeeld dat het NCSC afspraken maakt met de betrokken sectorale toezichthouders over het in bepaalde gevallen informeren van die toezichthouders over dreigingen en incidenten. Uw Kamer blijf ik informeren over de voortgang van de aanpak langs de ambities van de Nederlandse Cybersecurity Agenda en de in dat kader ingezette versterkte aanpak. Daarnaast ontvangt uw Kamer in dit kader in het voorjaar van 2020 de kabinetsreactie op het WRR-rapport «Voorbereiden op digitale ontwrichting» en ook de eerste bevindingen van de evaluatie in het kader van de Citrix kwetsbaarheid. Hierover en over de brede aanpak van cybersecurity blijf ik graag met uw Kamer in gesprek.

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

[12] Kamerstuk 26 643, nr. 614 en Kamerstuk 26 643, nr. 647.