Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

1539

Vragen van het lid **Rajkowski** (VVD) aan de Minister van Justitie en Veiligheid over *het bericht «Banken en overheden zetten software af uit angst voor hacks»* (ingezonden 21 december 2021).

Antwoord van Minister **Yeşilgöz-Zegerius** (Justitie en Veiligheid), Minister **Adriaansens** (Economische Zaken en Klimaat) en Staatssecretaris **Van Huffelen** (Binnenlandse Zaken en Koninkrijksrelaties) (ontvangen 2 februari 2022). Zie ook Aanhangsel Handelingen, vergaderjaar 2021–2022, nr. 1337.

Vraag 1
Bent u bekend met het bericht «Banken en overheden zetten software af uit angst voor hacks»?[1]

Antwoord 1
Ja.

Vraag 2
Kunt u een inschatting maken wat tot nu toe de schade is als gevolg van het lek bij Apache log4j? Wat is de schatting voor de komende weken?

Antwoord 2
Tot nu toe heeft het Nationaal Cybersecurity Centrum (NCSC) geen signalen ontvangen van grootschalige uitval of schade bij rijksoverheidsorganisaties of vitale aanbieders. Het NCSC acht het waarschijnlijk dat incidenten, waaruit schade kan ontstaan, over een langere tijdsperiode kunnen gaan plaatsvinden.

Vraag 3
Hoeveel gevallen zijn er al bekend waarbij criminele hackers Nederlandse organisaties aanvallen als gevolg van het lek bij Apache log4j? Met welk doel worden de betreffende organisaties aangevallen? Om welke organisaties gaat het en wat zijn de gevolgen van deze hacks?

[1] Financieel Dagblad, «Banken en overheden zetten software af uit angst voor hacks» (fd.nl/tech-en-innovatie/1423222/banken-en-overheden-zetten-software-af-uit-angst-voor-hacks-knl1ca56jOoK)

ah-tk-20212022-1539
ISSN 0921 - 7398
's-Gravenhage 2022

Antwoord 3
Op dit moment is kleinschalig misbruik van de kwetsbaarheid bij organisaties in Nederland bij het NCSC bekend. Het doel van de aanvallen is veelal financieel gewin. Verwacht wordt dat kwaadwillenden de komende tijd naar kwetsbare systemen blijven zoeken en doelgerichte aanvallen uitvoeren; de Log4J kwetsbaarheid wordt mogelijk een standaardonderdeel van aanvalsmethoden van actoren om toegang te krijgen tot systemen.
De politie heeft tot op heden geen aangiften binnengekregen van aanvallen met betrekking tot deze kwetsbaarheid.

Vraag 4
In hoeverre zijn organisaties en (vitale) bedrijven die mogelijk gebruik maken van Apache log4j van dit lek op de hoogte? Wat is de rol van het Nationaal Cyber Security Centrum (NCSC) en het Digital Trust Center (DTC) hierin? Hebben zij een regierol hier? Zo ja, wat hebben zij tot nu toe gedaan om de risico's van dit grootschalige lek te mitigeren? Hoe is de IT-informatiesessie van 15 december jl. bevallen?

Antwoord 4
Het NCSC heeft vanaf het bekend worden van deze kwetsbaarheid rijksoverheidsorganisaties, vitale aanbieders en schakelorganisaties zo veel als mogelijk proactief gewaarschuwd. Het algemene beveiligingsadvies inzake deze kwetsbaarheid is zoals gebruikelijk gepubliceerd op de website van het NCSC, zodat ook het brede publiek is geïnformeerd. Daarnaast heeft het NCSC genoemde partijen meerdere doelgroepberichten met aanvullende duiding en handelingsperspectieven verzonden. In deze zin is dus door het NCSC in zo breed mogelijke zin gewaarschuwd voor deze ernstige kwetsbaarheid.
Naast de gebruikelijke communicatiekanalen heeft het NCSC een publiek informatieplatform opgezet om technische informatie over deze kwetsbaarheid te verzamelen en te verspreiden. Dit platform, dat momenteel wereldwijd het meest compleet is, wordt nog steeds door veel partijen uit binnen- en buitenland benut.
Het Digital Trust Center (DTC) zet bij ernstige kwetsbaarheden al haar kanalen in om het niet- vitale bedrijfsleven te informeren en waarschuwen. Ook bij de Log4J kwetsbaarheid was dit het geval.
Als reactie op deze kwetsbaarheid heeft het DTC berichtgeving over Log4J inclusief handelingsperspectief breed gedeeld via de website van het DTC, DTC sociale media kanalen en de DTC community. Ook werd berichtgeving direct gedeeld met DTC samenwerkingsverbanden zodat deze de beschikbare informatie konden verspreiden bij hun achterban (de regio, sector of branche die ze vertegenwoordigen).
Het Cyber Security Incident Response Team voor digitale diensten (CSIRT-DSP) heeft een actieve rol gespeeld door het informeren van digitale dienstverleners binnen hun doelgroep over de Log4J kwetsbaarheid.
Op 15 december hebben NCSC, DTC en CSIRT-DSP gezamenlijk een informatiesessie voor IT-specialisten georganiseerd met als doel meer informatie te delen over de Log4J kwetsbaarheid, te adviseren over mogelijke acties, en vragen over de Log4J kwetsbaarheid direct te beantwoorden. Hier deden ongeveer 4000 deelnemers aan mee.

Vraag 5
In hoeverre zijn organisaties ervan op de hoogte dat er een update van Apache log4j beschikbaar is en dat ze deze update moeten uitvoeren? Hoe vaak is deze update uitgevoerd door organisaties? Welke maatregelen worden getroffen om ook de kleinere bedrijven in te lichten over het doen van deze update?

Antwoord 5
Zoals in antwoord op vraag 3 aangegeven zijn organisaties vanuit het NCSC en het DTC geïnformeerd over de kwetsbaarheid in Apache Log4J, evenals over de daartoe mogelijke beveiligingsmaatregelen, waaronder het uitvoeren van updates.
De betreffende kwetsbaarheid zit in software die vaak is ingebouwd in andere producten. De aard van de Log4J-kwetsbaarheid maakt het daarmee complex om zicht te krijgen op de mate waarin updates zijn uitgevoerd. Elke organisa-

tie blijft zelf primair verantwoordelijk voor het uitvoeren van updates en maatregelen.
Vele organisaties in Nederland maken gebruik van software waar Log4J in verwerkt zit. Zij kunnen daarom afhankelijk zijn van updates van hun softwareleverancier die op hun beurt de Apache Log4J updates dienen te verwerken in hun software. Daarnaast hebben genoemde organisaties regelmatig een externe IT-dienstverlener die bijvoorbeeld het gebruik van software binnen de organisatie beheert. Dit houdt in dat organisaties niet altijd zelf nodige updates uitvoeren of weten voor welke gebruikte software dat nodig is.
Het NCSC en DTC hebben daarom hun doelgroepen geadviseerd contact op te nemen met hun IT-dienstverlener om te bevestigen dat de juiste updates uitgevoerd worden of andere maatregelen genomen zijn.

Vraag 6
Welke overheidsorganisaties maken gebruik van Apache Log4j? Zijn er al overheidsorganisaties aangevallen door criminele hackers? Welke maatregelen neemt u om de kans zo klein mogelijk te maken dat criminele hackers succesvolle aanvallen op cruciale overheidsorganisaties kunnen uitvoeren en hen digitaal kunnen gijzelen?

Antwoord 6
Log4J is een softwaremodule die wereldwijd in velerlei software wordt gebruikt, waaronder bij de overheid. Er bestaat geen centraal overzicht van welke softwareproducten Log4J gebruiken binnen de overheid. Iedere overheidsorganisatie is primair verantwoordelijk voor zijn eigen netwerken, systemen en softwareproducten die worden gebruikt. Overheidsorganisaties scannen en inventariseren ook hun maatwerktoepassingen. Er zijn in dit verband wel overheidsbreed kaders afgesproken met eisen waaraan iedere organisatie moet voldoen, waaronder de Baseline Informatiebeveiliging Overheid (BIO). Hierin staat onder andere dat organisaties bij ernstige kwetsbaarheden binnen een week maatregelen moeten treffen. Daarnaast is het verplicht om de informatie-verwerkende omgeving te monitoren om onder meer aanvallen van criminele hackers te detecteren. Hiervoor zijn binnen de overheid Security Operations Centers (SOC's) en IT- organisaties actief. Zij hebben ook de beschikking over indicatoren die misbruik op basis van de Log4J kwetsbaarheid detecteren.
Na de ontdekking van de Log4J-kwetsbaarheid heeft BZK een crisisteam opgestart en zorg gedragen voor afstemming in het vervolg hierop met de departementen en de koepels/Computer Emergency Response Teams (CERT's) van de medeoverheden. Het crisisteam heeft er in dat verband op aangedrongen dat de benodigde maatregelen behorende bij deze kwetsbaarheid en het door het NCSC ontwikkelde stappenplan werden opgevolgd en er doorlopend onderzoek plaatsvond op mogelijk misbruik. De komende tijd zullen overheidsorganisaties extra alert blijven op aanwijzingen van mogelijk misbruik.
Op dit moment zijn er geen signalen dat overheidsorganisaties naar aanleiding van de Log4J kwetsbaarheid succesvol zijn aangevallen.

Vraag 7
Bekend is dat meerdere gemeentes hun systemen gedeeltelijk hebben afgesloten? Om hoeveel gemeentes gaat dit? Wat doen deze systemen en hoe lang gaan ze afgesloten blijven? Welke gevolgen heeft het voor de gemeentes als ze hun systemen tijdelijk gedeeltelijk moeten afsluiten?

Antwoord 7
De Vereniging Nederlandse Gemeenten (VNG) en de Informatiebeveiligingsdienst (IBD) houden geen overzicht bij van maatregelen van individuele gemeenten. Iedere situatie en iedere afweging is namelijk anders. De afwegingen om systemen gedeeltelijk/tijdelijk uit te zetten zijn door de gemeenten zelf gemaakt. Gemeenten volgen bij deze afweging het handelingskader van de IBD, zoals vermeld op hun website:[2]

[2] https://www.informatiebeveiligingsdienst.nl/nieuws/kwetsbare-log4j-applicaties-en-te-nemen-stappen/

– als een systeem kwetsbaar is
– én er is geen oplossing of aanpassing mogelijk,
– dan kàn tijdelijk uitzetten een maatregel zijn.

Dat is in sommige gevallen gebeurd en gemeenten zijn hierover transparant geweest via eigen mediakanalen naar inwoners.
Bij de afweging om systemen gedeeltelijk/tijdelijk uit te schakelen wegen aspecten mee zoals de mate waarin de systemen kwetsbaar of kritisch zijn voor de bedrijfsvoering, of direct aan het internet gekoppeld zijn (internet facing), in relatie tot continuïteit van dienstverlening. Tijdens de feestdagen van eind vorige maand is dit ook gebeurd, op momenten waarop de dienstverlening dit toeliet, zodat in deze beperkt bezette periode het aanwezige personeel niet intensief hoefde te monitoren.

Vraag 8
Naast gemeentes hebben ook organisaties in de vitale sectoren zoals banken hun systemen gedeeltelijk afgesloten. Welke gevolgen heeft dit voor de vitale sectoren? In hoeverre wordt er via het NCSC ondersteuning geboden en samengewerkt met vitale sectoren zoals de banken- en telecomsector om de schade van dit lek te beperken?

Antwoord 8
De gevolgen van het nemen van preventieve maatregelen, zoals het gedeeltelijk afsluiten van systemen is afhankelijk van de sector of organisatie. Het NCSC heeft gelet op de ernst van de kwetsbaarheid geadviseerd waar updaten niet mogelijk is, te overwegen of het mogelijk is het systeem uit te schakelen totdat een patch beschikbaar is. Het (gedeeltelijk) afsluiten van een systeem is een eigen afweging van elke organisatie.
Het NCSC heeft ten behoeve van vitale aanbieders, alsook organisaties die deel uitmaken van de rijksoverheid, de wettelijke taak te informeren en adviseren over digitale dreigingen en incidenten en bijstand te verlenen bij het treffen van maatregelen om de continuïteit van hun diensten te waarborgen of te herstellen.

Vraag 9
Hoe wordt in andere landen omgegaan met dit lek? Werkt u samen met andere landen om oplossingen te vinden voor dit lek? Kunnen lessen getrokken worden uit hoe in het buitenland om wordt gegaan met dit lek?

Antwoord 9
Het beeld van het NCSC met betrekking tot deze kwetsbaarheid wordt gedeeld met nationale CSIRT's van EU-lidstaten. Het CSIRT-netwerk, bedoeld in de EU Netwerk en Informatiebeveiligingsrichtlijn (NIB), is ook opgeschaald geweest tot alert cooperation mode op initiatief en advies van het NCSC. Dit houdt in dat er, naast het regulier delen van informatie, regelmatig overleggen tussen de CSIRTs van alle EU-lidstaten plaatsvinden om het beeld over de kwetsbaarheid actiever te kunnen delen.
Het door het NCSC opgezette en gecoördineerde publieke informatieplatform is door vele internationale partijen gebruikt om informatie over deze kwetsbaarheid te delen. Dit zien wij als een zeer geslaagde samenwerking met buitenlandse partners.

Vraag 10
Welke gevolgen heeft dit lek voor het gebruik maken van Apache log4j door de overheid? Zijn er betere alternatieven waar naar gekeken kan worden?

Antwoord 10
In geval van risico's vanwege kwetsbaarheden, zoals die betreffende Log4J, is het van belang dat patches worden uitgevoerd of aanpassingen worden gedaan. Alle software kan kwetsbaarheden bevatten, zo ook Apache Log4J. De kwetsbaarheden in Log4J zijn snel opgelost: er is geen reden om op zoek te gaan naar een alternatief en een alternatief is niet per se veiliger. Het vervangen van dit soort software is daarnaast zeer complex en daarmee een niet-realistische oplossing. Wel is er structurele aandacht nodig voor dergelijke problematiek en de Onderzoeksraad voor Veiligheid (OVV) heeft in het rapport «Kwetsbaar door software – Lessen naar aanleiding van beveiligingslekken door software van Citrix» daarvoor diverse adviezen

gegeven. Zoals aangegeven in de Kamerbrief van 16 december 2021 zal het kabinet het rapport zorgvuldig bestuderen en binnen de wettelijke reactietermijn van zes maanden schriftelijk richting de OVV reageren. Uw Kamer zal daarover worden geïnformeerd.

Vraag 11
Deelt u de mening dat het NCSC en DTC proactief lijken te communiceren? Op welke verschillende manieren proberen zij organisaties te bereiken en van informatie te voorzien? Wat kan het NCSC en DTC nog beter doen om meer mensen te bereiken, in begrijpelijke taal en welke informatie zou er nog meer gedeeld kunnen worden?

Antwoord 11
Zoals in het antwoord op vraag 4 en 5 staat vermeld staan het NCSC en het DTC hierover in nauw contact met hun respectievelijke doelgroepen en met elkaar. Eén van de grote uitdagingen bij het stimuleren van organisaties om maatregelen te nemen is het vinden van de juiste balans tussen inhoudelijk technisch advies en praktisch handelingsperspectief.
Het NCSC heeft vanaf het bekend worden van deze kwetsbaarheid rijksoverheidsorganisaties, vitale aanbieders en schakelorganisaties dan ook zo veel als mogelijk proactief gewaarschuwd én beveiligingsadviezen verzonden. Het algemene beveiligingsadvies inzake deze kwetsbaarheid is zoals gebruikelijk gepubliceerd op de website van het NCSC, zodat ook het brede publiek in die zin is geïnformeerd. Daarnaast heeft het NCSC meerdere doelgroepberichten met aanvullende duiding verzonden.
Naast de gebruikelijke communicatiekanalen heeft het NCSC een publiek informatieplatform opgezet om technische informatie over deze kwetsbaarheid te verzamelen en te verspreiden. Dit platform wordt nog steeds door veel partijen uit binnen- en buitenland benut.
Hiermee is door het NCSC dus in zo breed mogelijke zin gewaarschuwd voor deze ernstige kwetsbaarheid.
Ook het DTC streeft ernaar waar mogelijk proactief handelsperspectief te bieden voor haar doelgroep. Deze informatie wordt breed gedeeld via de DTC website, sociale media kanalen en de DTC community. Daarnaast deelt DTC beschikbare informatie ook direct met de DTC samenwerkingsverbanden, die het vervolgens binnen hun regio, sector of branche verder verspreiden. Uitgangspunt is dat het gegeven handelsperspectief voor de kleinere en minder cybervolwassen doelgroep ook te begrijpen is. Het DTC werkt op dit moment, met medewerking van het NCSC, aan een verdiepend informatieproduct voor de doelgroep van het DTC met ditzelfde uitgangspunt.
Bedrijven die geen deel uitmaken van een samenwerkingsverband maar wel de berichtgeving willen ontvangen worden door het DTC proactief uitgenodigd om zich aan te melden bij de DTC-community waar de informatie ook wordt gedeeld.[3]

Vraag 12
Deelt u de mening dat het afkondigen van een code rood, zoals het Duitse Ministerie van Binnenlandse Zaken heeft gedaan, een interessante manier kan zijn om de urgentie van deze kwetsbaarheid aan te geven, er aandacht voor te vragen en de handelingsbereidheid bij organisaties te vergroten? Zo nee, waarom niet?

Antwoord 12
In de Nederlandse context worden organisaties ook, maar op een andere manier, geattendeerd op digitale dreigingen.
Naar aanleiding van een geconstateerde dreiging wordt in de eerste plaats door het Nationaal Cyber Security Centrum een beveiligingsadvies verspreid ten behoeve van organisaties in de eigen doelgroep (vitale aanbieders, rijksoverheidsorganisaties) en schakelorganisaties zoals het DTC. Daarnaast wordt ook een algemeen beveiligingsadvies gepubliceerd op de NCSC-website. De beveiligingsadviezen worden ingeschaald op (1) de kans dat een kwetsbaarheid wordt misbruikt en (2) de ernst van de schade die optreedt

[3] www.digitaltrustcenter.nl/community

wanneer een kwetsbaarheid misbruikt wordt. Bij Log4J is een High/High advies gepubliceerd.[4]

Vraag 13
Het Belgische Ministerie van Defensie lijkt aangevallen te zijn via de log4j-kwetsbaarheid; Deelt u de mening dat deze kerstperiode voor criminelen en statelijke actoren een uitgelezen kans zou kunnen zijn om de rijksoverheid en vitale sectoren aan te vallen? Zo nee, waarom niet? Zo ja, welke voorbereidingen worden getroffen? Staan er extra cyberteams paraat en zijn alle systemen gecheckt? Is het helder wie bij een crisis de leiding neemt en hoe cyberteams van de verschillende veiligheidsdiensten zich tot elkaar verhouden? Zo nee, waarom niet? Zo ja, welke rol speelt het Defensie Cyber Commando?

Antwoord 13
Uit eerdere aanvallen in verband met andere kwetsbaarheden is gebleken dat vakantieperiodes of feestdagen vaker worden misbruikt door cybercriminelen. Een lagere bezettingsgraad kan betekenen dat organisaties mogelijk minder alert zijn of dat middelen voor herstel beperkt zijn in vergelijking met andere periodes.
Op 10 december jl. heeft het NCSC het eerste algemene beveiligingsadvies voor deze kwetsbaarheid op haar website gepubliceerd. Het NCSC waarschuwt daarin voor potentieel grote schade en adviseert organisaties daarom zich voor te bereiden op een mogelijke aanval. Daarbij is aangegeven dat het zeer waarschijnlijk is dat in de komende weken digitale (ransomware)aanvallen en datalekken plaatsvinden. Het NCSC heeft op 16 december het Nationaal Respons Netwerk (NRN) geactiveerd om aanvullende incident respons capaciteit gereed te hebben voor het kunnen verlenen van bijstand. Vanaf het bekend worden van de kwetsbaarheid heeft het NCSC de situatie doorlopend gemonitord, adviezen geactualiseerd en nauw contact onderhouden met Rijksorganisaties, vitale aanbieders en cybersecuritypartners in binnen- en buitenland. Ook het DTC communiceert de meest actuele informatie en handelingsperspectieven naar haar doelgroep.
Daarnaast kan er ook aanleiding bestaan om de nationale crisisstructuur te activeren bij een dreiging van (zeer) grote omvang. Deze nationale opschaling wordt in de praktijk gecoördineerd door het Nationaal Crisis Centrum van de NCTV. Dit is ook zo beschreven in het Nationaal Crisisplan Digitaal (NCP-D). De wijze waarop cyberteams van de verschillende veiligheidsdiensten zich tot elkaar verhouden en samenwerken staat ook in het NCP-D beschreven. Ditzelfde plan wordt ook gebruikt om met elkaar cybercrisis te oefenen. Ook de rol van het Defensie Cybercommando (DCC) is te vinden in dit plan.
De rol van het DCC was minimaal in deze casus. Zoals ook in de Kamerbrief *Tegenmaatregelen ransomware-aanvallen* van 6 okt 2021 uiteengezet door de Minister van Buitenlandse Zaken speelt het DCC de rol van het laatste digitale instrument, waarbij in een eerdere fase inzet van andere overheidsinstanties of minder vergaande instrumenten niet afdoende is gebleken.[5] Ook kan het DCC op verzoek de desbetreffende teams versterken met kennis en expertise van cyberoperators. Dat laatste is niet nodig gebleken. Wel heeft het Defensie Cyber Security Centrum (DCSC) cyberexperts geleverd uit het NRN aan het NCSC om te ondersteunen bij deze crisis. Aangezien deze casus meer toezag op cybersecurity – wat het vakgebied en de verantwoordelijkheid is van het DCSC binnen Defensie. Hiertoe is in de Log4J casus de nationale crisisstructuur tweemaal bijeengekomen op het niveau van een Interdepartementaal Afstemmingsoverleg (IAO).

[4] www.ncsc.nl/documenten/publicaties/2019/juli/02/inschalingsmatrix
[5] Tegenmaatregelen ransomware-aanvallen | Tweede Kamer der Staten-Generaal