Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2025–2026

Aanhangsel van de Handelingen

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

79

Vragen van het lid **Six Dijkstra** (Nieuw Sociaal Contract) aan de Minister van Justitie en Veiligheid over *de recente cyberaanvallen middels kwetsbaarheden in Sharepoint en Netscaler* (ingezonden 28 juli 2025).

Antwoord van Minister **Van Oosten** (Justitie en Veiligheid), mede namens de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Buitenlandse Zaken (ontvangen 22 september 2025). Zie ook Aanhangsel Handelingen, vergaderjaar 2024–2025, nr. 2842.

Vraag 1
Heeft u een voorlopig beeld van in welke mate de kwetsbaarheden in de on-premise versie van Microsoft Sharepoint Server een effect hebben gehad op de Nederlandse overheid en samenleving?[1] Kunt u in algemene zin een indicatie geven van de hoeveelheid (potentiële) slachtoffers in Nederland?

Antwoord 1
Het voorlopige beeld op dit moment is dat de kwetsbaarheden in Sharepoint slechts beperkt effect hebben gehad op de Nederlandse overheid en samenleving.
De samenwerkingsruimten bij rijksorganisaties, die zijn gebaseerd op Sharepoint, zijn destijds tijdelijk uit voorzorg door SSC-ICT geblokkeerd. Sinds vrijdag 24 juli zijn de samenwerkingsruimten weer beschikbaar voor medewerkers en externen.
Voor de medeoverheden geldt dat ze in het algemeen niet in de on-premise versie van Microsoft SharePoint Server werken omdat zij voornamelijk de cloud-variant gebruiken, waarop de kwetsbaarheid niet van toepassing is. Impact voor de medeoverheden lijkt om die reden beperkt.
Daarnaast verstrekt het Nationaal Cyber Security Centrum (NCSC) bij dergelijke kwetsbaarheden duidingsinformatie, handelingsperspectieven en beveiligingsadviezen.

[1] NCSC, 23 juli 2025, «Casus: Microsoft SharePoint Server kwetsbaarheden», https://www.ncsc.nl/actueel/nieuws/2025/07/23/casus-microsoft-sharepoint

ah-tk-20252026-79
ISSN 0921 - 7398
's-Gravenhage 2025

Vraag 2
Kunt u dit ook aangeven ten aanzien van de recente kwetsbaarheden in Citrix Netscaler?[2]

Antwoord 2
Op de impact op de strafrechtketen naar aanleiding van de offline gang van het Openbaar Ministerie (OM) heb ik uw Kamer reeds geïnformeerd.[3]
Daarnaast heeft het NCSC heeft ook ten aanzien van de kwetsbaarheid in Citrix Netscaler verschillende adviezen uitgebracht. Deze adviezen zijn gedeeld met de desbetreffende doelgroepen en betroffen aanbevelingen voor het uitvoeren van patches en het draaien van scripts.
Bij enkele rijksorganisaties zijn sporen van compromittatie aangetroffen. Mitigerende maatregelen zijn getroffen en nader onderzoek wordt verricht. Tot dusver zijn er geen aanwijzingen dat andere overheidsorganisaties zijn gecompromitteerd.

Vraag 3
Kunt u reflecteren op Microsofts attributie van de initiële cyberaanvallen waarbij gebruik is gemaakt van Sharepoint-kwetsbaarheden aan de Chinese cyber threat actors Linen Typhoon, Violet Typhoon en Storm-2603, in relatie tot de gekende Chinese digitale spionagedreiging zoals beschreven in het Dreigingsbeeld Statelijke Actoren (DBSA) 2025 (Kamerstuk 30 821, nr. 305)?[4]

Antwoord 3
De digitale spionagedreiging zoals beschreven in DBSA 2025 heeft de constante aandacht van het kabinet. Cybersecurity bedrijven zoals Microsoft onderzoeken met regelmaat de toedracht en oorsprong van cyberaanvallen. Die informatie bestudeert het kabinet met aandacht. Evenwel moet een attributie door het kabinet altijd rusten op eigenstandige informatie.

Vraag 4
In welke mate weten het Nationaal Cyber Security Center (NCSC) en de relevante doelgroepen elkaar te vinden als het gaat om het opvolgen van beveiligingsadviezen, het delen van indicators of compromise (IoC's) en het melden van compromittaties, in casussen als Sharepoint en Netscaler? Op welk vlak zijn de grootste verbeteringen nog mogelijk?

Antwoord 4
Het NCSC verzamelt en analyseert, in het kader van de uitoefening van de taken in de Wet beveiliging netwerk- en informatiesystemen (Wbni), continu informatie over dreigingen en incidenten en deelt deze informatie in datzelfde kader zo veel als mogelijk met publieke en private organisaties waarvoor die informatie relevant is, of met hun schakelorganisaties. Zo worden deze organisaties in staat gesteld zelf aanvullend onderzoek te verrichten. Via nieuws- en doelgroepberichten biedt het NCSC technische hulpmiddelen, zoals scripts en *Indicators of Compromise* (IoC's), die helpen bij het detecteren, herkennen en onderzoeken van incidenten. Ook verstrekt het NCSC onder meer duidingsinformatie, handelingsperspectieven en beveiligingsadviezen via een uitgebreid netwerk en (openbare) kanalen aan publieke en private partijen. Daarnaast onderhoudt het NCSC contact met verschillende incident response-partijen voor informatie-uitwisseling en het verstrekken van passende adviezen. Informatie-uitwisseling over cyberdreigingen- en incidenten vindt plaats via bestaande samenwerkingen en informatiekanalen. Daarnaast zijn initiatieven zoals het Cyberweerbaarheidsnetwerk en Cyclotron in ontwikkeling om deze uitwisseling verder te versterken.

Vraag 5
Zal de inwerkingtreding van de Cyberbeveiligingswet naar uw verwachting deze informatieuitwisseling versterken? Kunt u dit toelichten?

---

[2] NCSC, 22 juli 2025, «Casus: Citrix kwetsbaarheid», https://www.ncsc.nl/actueel/nieuws/2025/07/22/casus-citrix-kwetsbaarheid
[3] Kamerstuk 26 643, nr. 1379, 12 augustus 2025
[4] Microsoft, 22 juli 2025, «Disrupting active exploitation of on-premises SharePoint vulnerabilities», https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/

Antwoord 5
Na inwerkingtreding van de Cyberbeveiligingswet (Cbw) zal de uitwisseling van informatie vanuit het NCSC in ruimere zin mogelijk worden, in elk geval omdat een Computer Security Incident Response Team (CSIRT) op grond daarvan uitdrukkelijk tot taak krijgt om informatie over dreigingen, kwetsbaarheden en incidenten niet alleen aan essentiële en belangrijke entiteiten, maar ook aan alle andere relevante partijen te verstrekken. Daarbij is de tussenkomst van schakelorganisaties niet meer vereist.

Vraag 6
Wanneer verwacht u de Kamer te kunnen informeren over de omstandigheden, de schade en de consequenties van de compromittatie van systemen van het Openbaar Ministerie (OM) middels kwetsbaarheden in Netscaler, welke volgens de media waarschijnlijk door een Russische cyber threat actor uitgevoerd is?[5]

Antwoord 6
Uw Kamer is hier reeds op verschillende momenten over geïnformeerd.[6, 7, 8] Wat de exacte consequenties van de compromittatie zijn, is onderwerp van lopend onderzoek.

Vraag 7, 8, 9, 10 en 11
Bent u voornemens om die betreffende cyberaanval op het OM, indien dit met voldoende betrouwbaarheid mogelijk is, publiekelijk te attribueren aan een cyber threat actor en/of een land, net zoals het kabinet reeds gedaan heeft met de attributie van de politiehack uit 2024 aan de Russische cyber threat actor LAUNDRY BEAR?
Heeft de Nederlandse overheid een algemeen publiekelijk attributiebeleid voor cyberaanvalscampagnes?
Welk afwegingskader(s) hanteert de overheid voor het al dan niet publiekelijk attribueren van cyberaanvallen? Welk(e) bewindspersoon/-personen of welk(e) departement(en) is/zijn doorslaggevend in het besluit of dit publiekelijk gebeurt?
Zal het feit dat, zoals in het DBSA 2025 wordt gesteld, «er steeds meer landen [lijken] te zijn die in Nederland willen spioneren, met name digitaal via offensieve cyberprogramma's» van invloed zijn op het attributiebeleid of de uitvoeringspraktijk? Acht u het waarschijnlijk dat het kabinet in de komende jaren meer cyberaanvalscampagnes aan meer landen zal attribueren?
Hoe en in welke mate wegen diplomatieke afbreukrisico's mee in het al dan niet publiekelijk attribueren van een cyber threat actor aan een land?

Antwoord 7, 8, 9, 10 en 11
Zoals aangegeven in antwoord op vraag 3 heeft de digitale spionagedreiging de continue aandacht van dit kabinet. In lijn met de motie Erkens (36 410 X, nr. 46) is het de inzet van het kabinet om waar mogelijk cyberaanvallen en bijbehorende technische werkwijzen openbaar te maken. De wenselijkheid van het publiek attribueren aan een statelijke actor hangt af van een groot aantal factoren. De beoogde doelen en effecten van de publieke attributie, de technische afwegingen, diplomatieke gevolgen, eventuele gevolgen voor lopend onderzoek en het effect op de nationale veiligheid worden alle meegewogen bij besluitvorming over attributie. Ook worden gelijkgestemde partners, in het bijzonder EU-lidstaten en NAVO-bondgenoten, vooraf op de hoogte gesteld van een attributie.
Bovendien is het van belang het beoogde doel scherp te formuleren. Publieke attributie kan wat het kabinet betreft de volgende doelen dienen: het door middel van openbaarmaking van informatie verstoren van cyberoperaties, het beïnvloeden van het gedrag van kwaadwillende actoren, het informeren van internationale partners en bondgenoten en het informeren van overige derde landen die met een soortgelijke dreiging te maken hebben.

---

[5] AD, 24 juli 2025, «Sterke signalen dat Russen achter hack OM zitten, zaten mogelijk weken in systeem», https://www.ad.nl/binnenland/sterke-signalen-dat-russen-achter-hack-om-zitten-zaten-mogelijk-weken-in-systeem~a6bd3c60/
[6] Kamerstuk 26 643, nr. 1379, 12 augustus 2025
[7] Kamerstuk 26 643, nr. 1376, 12 augustus 2025
[8] Kamerstuk 26 643, nr. 1378, 4 augustus 2025

Bij deze besluitvorming zijn de Ministeries van Defensie, Justitie en Veiligheid (NCTV en NCSC), Buitenlandse Zaken, de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD), de Politie en het Openbaar Ministerie (OM) betrokken. Het uiteindelijke besluit over een attributie wordt door het kabinet, via de Raad Veiligheid en Inlichtingen, genomen.

Vraag 12
Heeft u een beeld van hoe de Cybersecurity Advisory over LAUNDRY BEAR inclusief mapping naar het MITRE ATT&CK framework over het algemeen ontvangen is bij de relevante partijen (Kamerstuk 29 628, nr. 1256)? Wordt een rapport als deze in de sector als behulpzaam beschouwd?

Antwoord 12
De Cybersecurity Advisory bevat handelingsperspectief voor publieke en private organisaties in Nederland, en wereldwijd, om hun weerbaarheid te verhogen en onderzoek mogelijk te maken naar deze cyberactor.
De relevante partijen hebben de Cybersecurity Advisory goed ontvangen. Zij zien dit rapport als behulpzaam en worden door de CSA in staat gesteld zelf onderzoek te doen.

Vraag 13
Voorziet u dat het kabinet in de toekomst vaker adviesrapporten van deze aard en omvang met classificatie TLP:CLEAR zal verstrekken? Wat zijn hierin de afwegingen?

Antwoord
De classificatie TLP:CLEAR betekent dat er, binnen de toepasselijke voorschriften en procedures voor openbaarmaking, geen beperkingen gelden voor verspreiding en dat informatie publiekelijk gedeeld mag worden.
Indien er adviesrapporten met de classificatie TLP:CLEAR beschikbaar komen worden deze door het NCSC, met inachtneming van de wettelijke kaders, verstrekt via een uitgebreid netwerk en (openbare) kanalen aan publieke en private partijen waarvoor deze informatie relevant is om zo de digitale weerbaarheid te bevorderen.