Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

Aanhangsel van de Handelingen

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

2842

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).

Mededeling van Minister **Van Weel** (Justitie en Veiligheid) (ontvangen 18 augustus 2025).

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?

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

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)?[3]

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?

---

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

[2] NCSC, 22 juli 2025, «Casus: Citrix kwetsbaarheid», https://www.ncsc.nl/actueel/nieuws/2025/07/22/casus-citrix-kwetsbaarheid

[3] 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/

ah-tk-20242025-2842
ISSN 0921 - 7398
's-Gravenhage 2025

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

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?[4]

Vraag 7
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?

Vraag 8
Heeft de Nederlandse overheid een algemeen publiekelijk attributiebeleid voor cyberaanvalscampagnes?

Vraag 9
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?

Vraag 10
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?

Vraag 11
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?

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?

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?

Mededeling

Hierbij deel ik u mede dat de schriftelijke vragen van het lid Six Dijkstra (Nieuw Sociaal Contract), van uw Kamer aan de Minister van Justitie en Veiligheid over de recente cyberaanvallen middels kwetsbaarheden in Sharepoint en Netscaler (ingezonden 28 juli 2025) niet binnen de gebruikelijke termijn kunnen worden beantwoord, aangezien nog niet alle benodigde informatie is ontvangen.
Ik streef ernaar de vragen zo spoedig mogelijk te beantwoorden.

[4] 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/