Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

TER BESLUITVORMING

Nota actief openbaar
Ja

Onze referentie
2024-0000431357

Datum
2 juli 2024

Opgesteld door
[redacted]

Samengewerkt met

Bijlage(n)
1

Aan Staatssecretaris van Digitalisering en Koninkrijksrelaties
Van DGDOO/CIO Rijk/IB&P

nota

Beantwoording Kamervragen Gemelde kwetsbaarheid Cisco Webex

Aanleiding

Op 4 juni jl. zijn vragen aan het Nationaal Cyber Security Centrum (NCSC) gesteld door een journalist die werkt aan een artikel voor Zeit Online over kwetsbaarheden in Webex Cloud. De journaliste gaf aan dat er duizenden ´overleglinkjes´ zijn gevonden met daarin metadata van Webex-overleggen van de Nederlandse Rijksoverheid. Het ging daarbij o.a. om gesprekken van verschillende bewindspersonen (MinJenV, MinIenW, MinVWS, MinFin).

Naar aanleiding van deze melding is vanuit BZK de crisisorganisatie opgestart om de impact van het incident te analyseren en handelingsperspectief uit te werken. Hierbij is tevens een gesprek met Cisco geweest, waarbij Cisco haar medewerking heeft aangeboden en de toezegging heeft gedaan om haar procedures aan te passen om een dergelijk incident in de toekomst te voorkomen.

De oorspronkelijk gevonden kwetsbaarheid is per 28 mei jl. verholpen. Dit is ook door onafhankelijke onderzoekers bevestigd. Uit onderzoek van het NCSC bleek donderdag 6 juni dat er nog een afgeleide kwetsbaarheid in oude Webex-vergaderingen zit. Het gaat hier om vergaderingen die voor 28 mei jl. zijn aangemaakt, maar nog moeten plaatvinden. Deze kwetsbaarheid is in samenwerking tussen de Belastingdienst en Cisco tevens verholpen.

Naar aanleiding van de twee Kamerbrieven[1,2] betreffende het onderwerp zijn er op 12 juni jl. schriftelijke Kamervragen gesteld. Met de onderhavige Kamerbrief worden deze vragen beantwoord.

Geadviseerd besluit

- In te stemmen met het informeren van de Kamer over de laatste stand van zaken rond het incident met Webex.
- Akkoord gaan met verzending van de beantwoording van de Kamervragen.

Kern

De afwikkeling van het incident rond Webex is klaar met het testen van de laatste reparaties die Cisco heeft uitgevoerd. De kwetsbaarheden werden gevonden in de securitytest die de Belastingdienst heeft laten uitvoeren. Hierover is uw

[1] Brief - Gemelde kwetsbaarheid Cisco WebEx (overheid.nl)
[2] Brief - Update gemelde kwetsbaarheid Cisco Webex (overheid.nl)

voorganger geïnformeerd. In de DGDOO-crisisaanpak is teruggeschaald naar de koude fase.

De beantwoording van de Kamervragen heeft in afstemming plaatsgevonden met het NCSC, de Belastingdienst, de AIVD en MinDef.

De Kamervragen zien primair toe op het soort informatie dat middels Webex behandeld kan en mag worden. Webex kan, net als bijvoorbeeld regulier telefonisch contact, gebruikt worden voor informatie tot en met 'Departementaal VERTROUWELIJK (Dep.V.)' gerubriceerd, anders niet. Defensie staat gebruik van Webex bij rubriceringen hoger dan UNCLAS niet toe.[3]

Naast het type informatie dat middels Webex besproken kan en mag worden, is de Kamer vragende naar de mate waarin men nog vertrouwen kan hebben in Cisco Webex vanwege deze kwetsbaarheid. Het ontdekken – en verhelpen – van kwetsbaarheden is een regulier IT-proces. Het onderhavige issue in kwestie was echter dat de ontdekte kwetsbaarheid niet per direct aan de Rijksoverheid gemeld werd, omdat Cisco geen verdachte activiteiten waargenomen heeft op de Rijksoverheid tenant. Hierover zijn gesprekken met Cisco gevoerd, naar aanleiding waarvan Cisco hun meldingsproces gaat herinrichten om een dergelijke kwestie in de toekomst te voorkomen. CIO Rijk is betrokken bij deze herinrichting.

Informatie die niet openbaar gemaakt kan worden
Motivering
In de openbaar gemaakte versie van deze nota zijn alle persoonsgegevens van ambtenaren geanonimiseerd.

Bijlagen

Volgnummer	Naam	Informatie
1	Kamerbrief beantwoording Kamervragen Gemelde kwetsbaarheid Cisco Webex	

[3] UNCLAS: NATO UNCLASSIFIED, informatie waarvan de toegang geen schade aan de NAVO kan toebrengen.