Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2023–2024

Aanhangsel van de Handelingen

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

2524

Vragen van de leden **Valize** (PVV), **Six Dijkstra** (Nieuw Sociaal Contract) en **Rajkowski** (VVD) aan de Ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Defensie en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over *de kabinetsbrief Gemelde kwetsbaarheid Cisco Webex vergadervoorziening* (ingezonden 12 juni 2024).

Antwoord van Staatssecretaris **Szabó** (Binnenlandse Zaken en Koninkrijksrelaties) (ontvangen 10 september 2024).

Inleiding
Naast de beantwoording van deze Kamervragen wil ik u graag mededelen dat, in opvolging van dit incident, ik nader onderzoek heb laten uitvoeren naar de beveiliging van de Rijksvideovergadervoorziening op basis van Webex. Hieruit zijn nog een aantal bevindingen naar voren gekomen, die in nauwe samenwerking tussen Cisco, de Belastingdienst en het NCSC zijn onderzocht, opgelost en opnieuw getest.

Vraag 1
Klopt de berichtgeving van Nieuwsuur dat de kwetsbaarheid in Cisco Webex bestond door de voorspelbaarheid van URLs?[1] [2] Wordt binnen de Rijksoverheid bij de implementatie van systemen standaard een controle uitgevoerd op de afwezigheid van dergelijke basale configuratiefouten?

Antwoord 1
Ja. Dit betrof geen configuratiefout van de Rijksvideodienst (Belastingdienst). De inrichting is gecheckt in samenwerking met CIO Rijk en de AIVD/NBV. Hiervoor is onder andere een BSPA[3] en DPIA[4] uitgevoerd. Wel kon er via

[1] Kamerstuk 26 643, nr. 1181
[2] NOS, 6 juni 2024, https://nos.nl/nieuwsuur/artikel/2523333-ambtenaren-gebruiken-onveilig-vergaderprogramma-data-waardevol-voor-spionnen
[3] Baseline Security Product Assessment (BSPA) | Informatiebeveiliging | AIVD
[4] DPIA: Data Protection Impact Assessment, gegevensbeschermingseffectbeoordeling. Een beoordeling van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens.

ah-tk-20232024-2524
ISSN 0921 - 7398
's-Gravenhage 2024

enumeratie[5], door een voorspelbare logische volgordelijkheid in de unieke internetadressen van websites (URL's genoemd), metadata van andere vergaderingen worden ingezien door ongeautoriseerde gebruikers. Volgens Cisco was dit mogelijk door kwetsbaarheden in specifiek de Cloud-applicaties van Cisco Webex meetings. De Rijksoverheid heeft aanbevolen veiligheidsinstellingen en werkt veelal niet met de cloud versie, maar met de client versie van Webex.

Vraag 2
Klopt de berichtgeving van de Volkskrant dat het in het verleden mogelijk was om telefonisch in te bellen op de Webex-omgeving van de Rijksoverheid? Zo ja, zouden buitenlandse inlichtingendiensten daardoor ongemerkt vertrouwelijke Nederlandse videovergaderingen kunnen hebben bijgewoond?[6]

Antwoord 2
Het is mogelijk gebleken dat ongeautoriseerde gebruikers onder bepaalde voorwaarden vertrouwelijke videovergaderingen hebben kunnen bijwonen. Cisco ondersteunt namelijk de mogelijkheid in te bellen via het Public Switched Telephone Network op Cisco Webex Meetings.
Binnen Nederland zijn echter geen gevallen bekend waarbij ongeautoriseerde gebruikers vertrouwelijke videovergaderingen van de Rijksoverheid hebben bijgewoond. Uit zowel onderzoek van Cisco als uit eigen onderzoek van het Nationaal Cyber Security Centrum (NCSC) is geen indicatie van misbruik naar voren gekomen. Dit komt mede door de standaardtoepassingen van beveiligingsmaatregelen bij het gebruik van Cisco Webex binnen de Rijksoverheid.

Vraag 3
Wilt u nader toelichten wat het concreet betekent dat Cisco Webex «niet gebruikt [mag] worden voor overleggen die als zeer vertrouwelijk zijn aangemerkt of waar staatsgeheime informatie wordt besproken»? Waar legt het kabinet de lat voor «zeer vertrouwelijk»?

Antwoord 3
Webex kan, net als bijvoorbeeld regulier telefonisch contact, gebruikt worden voor informatie tot en met «Departementaal VERTROUWELIJK (Dep.V.)» gerubriceerd, anders niet.
Informatie wordt als Dep.V. gerubriceerd indien kennisname door niet geautoriseerden schade kan toebrengen aan de belangen van één of meerdere ministeries. Informatie wordt als Staatsgeheim CONFIDENTIEEL/ GEHEIM/ZEER GEHEIM gerubriceerd indien kennisname door niet geautoriseerden respectievelijk schade/ernstige schade/zeer ernstige schade kan toebrengen aan een van de vitale belangen van de staat of zijn bondgenoten. «Zeer vertrouwelijk» valt onder de eigen beoordelingsruimte van de medewerker.

Vraag 4
Mogen er Departementaal Vertrouwelijk (Dep.V)-gerubriceerde gesprekken gevoerd worden via Cisco Webex? Zo ja, heeft het kabinet ook na dit incident nog voldoende vertrouwen in het beveiligingsniveau van Cisco Webex als product en het beveiligingsbewustzijn van Cisco als fabrikant om gesprekken op dit rubriceringsniveau te laten plaatsvinden?

Antwoord 4
Webex kan, net als bijvoorbeeld regulier telefonisch contact, gebruikt worden voor informatie tot en met «Departementaal VERTROUWELIJK (Dep.V.)» gerubriceerd, anders niet.
Door ontwikkeling van de techniek kunnen systemen die aanvankelijk veilig werden bevonden, nieuwe kwetsbaarheden bevatten. Daarnaast worden er continu nieuwe aanvalstechnieken ontwikkeld. Door het mitigeren van de

[5] Enumeratie is een proces waarbij informatie over een systeem of netwerk wordt verzameld, zoals gebruikersnamen en IP-adressen. Enumeratie wordt ingezet om toegang te krijgen tot gevoelige informatie.
[6] De Volkskrant, 6 juni 2024, https://www.volkskrant.nl/tech/lekke-vergadersoftware-toont-hoe-afhankelijk-nederlandse-overheid-is-van-amerikaanse-techbedrijven~b57bc007/

kwetsbaarheden en nemen van aanvullende maatregelen wordt een systeem weer veilig. Dit is een regulier, normaal proces waar alle IT aan onderhavig is. Het probleem in deze casus was ook niet zozeer dat er een kwetsbaarheid ontdekt was, maar dat deze 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.

Vraag 5
Zijn bewindspersonen en ambtenaren in de praktijk voldoende geëquipeerd om videogesprekken op het juiste rubriceringsniveau te voeren? Hoe wordt hierop toegezien?

Antwoord 5
Cisco Webex is geschikt voor het voeren van videogesprekken tot en met het niveau Departementaal Vertrouwelijk. Dit is ook duidelijk uitgelegd in de handleiding van Webex voor rijksambtenaren. Voor mobiele telefoongesprekken tot en met het niveau Staatsgeheim Geheim is de Sectra Tiger/S telefoon goedgekeurd door de AIVD.

Vraag 6
Kunt u illustreren wat voor soort gevoelige gesprekken wel via Cisco Webex gevoerd mogen worden, maar niet als «zeer vertrouwelijk» worden beschouwd of Stg-gerubriceerd zijn?

Antwoord 6
Een voorbeeld hiervan zouden personeels- en/of functioneringsgesprekken kunnen zijn.

Vraag 7
Mogen er via Cisco Webex gesprekken gevoerd worden waarin militair gevoelige informatie besproken wordt?

Antwoord 7
Indien de informatie tot en met «Departementaal VERTROUWELIJK (Dep.V.)» gerubriceerd is wel, anders niet.
Informatie wordt als Dep.V. gerubriceerd indien kennisname door niet geautoriseerden schade kan toebrengen aan de belangen van één of meerdere ministeries. Informatie wordt als Staatsgeheim CONFIDENTIEEL/ GEHEIM/ZEER GEHEIM gerubriceerd indien kennisname door niet geautoriseerden respectievelijk schade/ernstige schade/zeer ernstige schade kan toebrengen aan een van de vitale belangen van de staat of zijn bondgenoten.

Vraag 8
Mogen er via Cisco Webex gesprekken gevoerd worden waarin internationaal gevoelige informatie besproken wordt, zoals diplomatieke terugkoppelingen?

Antwoord 8
Zie antwoord vraag 7.

Vraag 9
Mogen er via Cisco Webex gesprekken gevoerd worden die, indien ze zouden uitlekken, de Nederlandse economische positie of economische veiligheid kunnen schaden, zoals aankomende investeringen, fusies en overnames of bedrijfsgevoelige informatie?

Antwoord 9
Zie antwoord vraag 7.

Vraag 10
Mogen er via Cisco Webex gesprekken gevoerd worden die, indien ze zouden uitlekken, de nationale veiligheid, de veiligheid van individuen of de openbare orde zouden kunnen schaden?

Antwoord 10
Zie antwoord vraag 7.

Vraag 11
Bestaat er een risico dat de vertrouwelijke identiteit van ambtenaren, waaronder medewerkers van de AIVD en MIVD, gelekt is via deze kwetsbaarheid?

Antwoord 11
Medewerkers van de Rijksoverheid maken gebruik van Webex. Bij het gebruik maken van een communicatiesysteem via het publieke internet hoort een bepaald beveiligingsniveau. Gekoppeld daaraan worden beslissingen genomen over vertrouwelijkheid.
Over de operationele werkwijzen van de inlichtingen- en veiligheidsdiensten worden in het openbaar geen uitspraken gedaan. In algemene zin houden de AIVD en MIVD altijd rekening met het beveiligingsniveau van een publieke communicatie-infrastructuur.

Vraag 12
Wat zijn de in de SLA (service level agreement) opgenomen afspraken met Cisco inzake dergelijke kwetsbaarheden en de opvolging hiervan, waaronder communicatie en afgesproken termijn voor reparatie?

Antwoord 12
Er is geen SLA met Cisco afgesloten, maar met BIS. Hierin zijn geen afspraken opgenomen omtrent kwetsbaarheden en de opvolging daarvan. Naar aanleiding van het incident wordt op korte termijn overleg met Cisco ingepland om Cisco's beleid en processen t.a.v. mogelijke toekomstig geconstateerde kwetsbaarheden/incidenten aan te passen.

Vraag 13
Hoe beoordeelt het kabinet het «coordinated vulnerability disclosure»-beleid (voor het melden van onbekende kwetsbaarheden) van Cisco en de uitvoering daarvan in de praktijk?

Antwoord 13
Het betrof kwetsbaarheden in specifiek de Cloud-applicaties van Cisco Webex meetings, waardoor het doorvoeren van updates van kwetsbare software door afnemers niet mogelijk was. Deze software is namelijk in beheer in de Cloud-omgeving van Cisco. Cisco heeft ervoor gekozen om in dit geval een andere procedure dan de coordinated vulnerability disclosure (CVD) procedure te volgen en geen kenmerken toe te kennen aan de kwetsbaarheden.
Naar aanleiding van het incident wordt op korte termijn overleg met Cisco gevoerd om Cisco's beleid en processen t.a.v. mogelijke toekomstig geconstateerde kwetsbaarheden/incidenten aan te passen.

Vraag 14
Bent u het met ons eens dat het «coordinated vulnerability disclosure»-beleid van producenten en de uitvoering daarvan in de praktijk een belangrijke afweging zou moeten zijn bij inkopen en aanbestedingen door de overheid? Hoe en in welke mate wordt dit nu door departementen meegewogen?

Antwoord 14
Het beschikken over een CVD-beleid is een concrete maatregel. In de Algemene Rijksinkoopvoorwaarden bij IT-opdrachten (ARBIT) is in art. 19 opgenomen dat wederpartij zorg draagt voor een niveau van Informatiebeveiliging dat van een redelijk handelend en bekwame IT-leverancier mag worden verwacht. Tevens moeten eventuele inbreuken zo spoedig mogelijk gemeld worden.
In Nederland is het CVD-beleid van het NCSC breed gecommuniceerd. Op de website van het Nationaal Cyber Security Centrum (NCSC) is veel informatie te vinden over Coordinated Vulnerability Disclosures (CVD). Dit betreft onder meer informatie over hoe personen een CVD-melding kunnen doen om technische kwetsbaarheden te melden bij het Nationaal Cyber Security Centrum (NCSC). Binnen de community van onderzoekers en ethische

hackers is het CVD-beleid van het Nationaal Cyber Security Centrum (NCSC) over het algemeen goed bekend. In het buitenland zijn vergelijkbare standaarden van toepassing.

Vraag 15
Bent u het met ons eens dat dit incident, in combinatie met eerdere incidenten gerelateerd aan deze fabrikant, de noodzaak benadrukt voor een hogere mate van Nederlandse digitale autonomie op het gebied van het voeren van vertrouwelijke videogesprekken? Is hier specifiek aandacht voor binnen de Nationale Cryptostrategie (NCS)?

Antwoord 15
Binnen de Nationale Cryptostrategie (NCS) worden de behoeftes van de Rijksoverheid voor informatiebeveiligingsproducten voor gerubriceerde informatie, met een focus op staatsgeheimen, besproken. Deze behoeftelijst is gerubriceerd en derhalve kunnen wij geen uitspraak doen over de inhoud hiervan.

Vraag 16
Bent u bereid om een open source alternatief voor Webex te overwegen? Zo nee, waarom niet?

Antwoord 16
De selectie van een leverancier voor het rijksbreed videoconferencing platform heeft middels een openbare aanbesteding plaatsgevonden. Geen van de inschrijvende partijen had een open source oplossing aangeboden. Uiteraard houden wij ons graag op de hoogte van de ontwikkelingen in de markt, maar we zien dat wat betreft de schaalgrootte en de complexiteit van de organisatie van de Rijksoverheid er op dit moment geen gelijkwaardige alternatieven beschikbaar zijn.