Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Nota actief openbaar
Ja

Onze referentie
2024-0000342866

Datum
4 juni 2024

Opgesteld door
[redacted]

Samengewerkt met

Bijlage(n)
0

Aan StasBZK
Van CISO Rijk

nota

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 geeft aan dat er duizenden ´overleglinkjes´ zijn gevonden met daarin metadata van Webex-overleggen van de Nederlandse Rijksoverheid. Het gaat daarbij o.a. om gesprekken van verschillende bewindspersonen (MinJenV, MinIenW, MinVWS, MinFin). Via deze nota wordt u nader geïnformeerd hierover.

Geadviseerd besluit

U wordt geadviseerd om kennis te nemen van:
1) De feiten voor zover bekend;
2) Mogelijke impact bij de Rijksoverheid;
3) Ondernomen acties tot dusver;
4) Te ondernemen acties; en
5) Vooraf genomen maatregelen

Kern

1) Feiten tot dusver bekend

- Op 4 juni jl. mailt een journaliste van *Zeit Online* naar het Nationaal Cyber Security Centrum (NCSC) over een artikel die zij schrijven over een kwetsbaarheden in Webex Cloud, waarvan zij stellen dat deze inmiddels door Cisco is opgelost.
- Zij geven aan dat zij door deze kwetsbaarheden duizenden ´overleglinkjes´ hebben gevonden met daarin data van Webex-overleggen van de Nederlandse Rijksoverheid.
- Het gaat o.a. over webex-overleggen van bewindspersonen. De namen die *Zeit Online* noemt zijn: MinJenV, MinIenW, MinVWS, MinFin .
- *Zeit Online* geeft aan dat deze informatie is verkregen via het manipuleren van de meeting informatie in de link.

- *Zeit Online* stelt dat overleggen van alle Webex-Cloud-klanten van de afgelopen 6 maanden online konden worden gevonden. Daarbij geeft zij aan dat de kwetsbaarheden door Cisco is verholpen en niet meer werkt.
- *Zeit Online* stelt vragen[1] voor de deadline van 5 juni in verband met hun aangekondigde artikel.
- In het bericht van de journalist is een relatie gelegd met de in maart jl. verschenen berichten over afgeluisterde Webex-gesprekken van het Duitse Ministerie van Defensie.
- *Security.nl* heeft een artikel geplaatst met de titel "Bugs in Cisco Webex Meetings gebruikt voor ongeautoriseerde toegang"

2) Mogelijke impact bij de Rijksoverheid

De melding wordt serieus genomen. Webex wordt breed gebruikt binnen de Rijksoverheid om digitaal te vergaderen. Het is niet wenselijk dat informatie over Webex-overleggen, van leden van het Kabinet of de Rijksoverheid, openbaar toegankelijk is. De aard van deze overleggen kan (zeer) vertrouwelijk zijn, hoewel aan gebruikers is gecommuniceerd dat de dienst niet bedoeld is voor zeer vertrouwelijke gesprekken zoals staatsgeheime informatie. Voor zover nu bekend lijkt het om informatie over de naam van de host (persoonsnaam), de meeting ID en de titel van het overleg en de start- en einddatum van het Webex-overleg te gaan.
Er zijn op moment van schrijven geen signalen dat er door ongeautoriseerde actoren interceptie heeft plaatsgevonden of overleggen zijn afgeluisterd.

3) Ondernomen acties tot dusver

- Er is overleg geweest met het NCSC en de NCTV.
- De CISO Rijk heeft de departementale CISO's geïnformeerd en de betrokken departementen gevraagd hun bewindsperso(o)n(en) te informeren in verband met de te verwachten publiciteit.
- Woordvoering BZK is direct betrokken door het NCSC.

4) Te ondernemen acties

- Vanuit CIO Rijk is contact gezocht met de Belastingdienst voor aanvullend onderzoek over misbruik van de kwetsbaarheden: hoe en in welke mate dit heeft plaats gevonden en over welke periode, en welke informatie daarbij gelekt kan zijn.
- Er wordt melding gedaan bij de Autoriteit Persoonsgegevens.
- Woordvoering BZK beantwoordt de vragen van de media.
- Vanuit CIO Rijk zal met Cisco in gesprek gegaan worden om te bespreken:
    - Hoe het incident zich voor heeft kunnen doen; en
    - Hoe dergelijke incidenten in de toekomst zoveel mogelijk voorkomen kunnen worden, en
    - Hoe het proces van incidentmeldingen verbeterd kan worden, en
    - Op welke wijze Cisco samen met de belastingdienst en het NCSC nader onderzoek kunnen doen naar de oorzaak.

5) Vooraf genomen maatregelen

[1] De vragen zijn: what is your assessment of the current security vulnerability? have you been informed about it by Cisco? Also about the extent? is there any evidence that the vulnerability has been exploited by unauthorized persons (other than us)? Or can you or Cisco rule this out? how do you proceed? Will you continue to use Webex?

Bij de ingebruikname van WebEx binnen de rijksoverheid is behalve een DPIA ook een risicoanalyse uitgevoerd voor informatiebeveiliging. De maatregelen zijn in opzet, bestaan en werking beoordeeld. De DPIA is in 2024 geactualiseerd.
Bij het uitvoeren van de analyses is afgesproken dat Cisco bewijsmateriaal aanlevert om aan te tonen dat zij voldoet aan alle gestelde eisen en dit periodiek opnieuw aanlevert. Dit betreft materiaal zoals auditrapporten, penetratietest-rapporten, SOC2 type 2 rapporten en nog meer.

Een van de geïdentificeerde risico's was dat hackers, of andere onbevoegden, kunnen proberen toegang te krijgen tot de voorziening. Om dat risico te beheersen zijn verschillende maatregelen genomen op mens, proces en technologie. Door de genomen maatregelen is het op voorhand zeer waarschijnlijk dat er geen inbreuken op de overleggen heeft plaatsgevonden.

Politieke context
Het verkrijgen van inzage door ongeautoriseerde(n) over WebEx-overleggen kan leiden tot politieke aandacht. Vanuit de coördinerende verantwoordelijkheid van BZK voor de digitale veiligheid van de overheid kan BZK hierop worden aangesproken.

Financiële/juridische overwegingen
N.v.t.

Krachtenveld
Via het CISO-netwerk zijn de departementale CISO's geïnformeerd om hun bewindspersonen te informeren die zijn genoemd door *Zeit Online*.

Strategie
Dit incident raakt ambities van het kabinet. Het raakt onder andere de ambitie om de digitale weerbaarheid van de overheid te versterken. Dit maakt onderdeel uit van de I-strategie Rijk (onder verantwoordelijkheid van BZK) en de Nederlandse Cybersecuritystrategie (onder coördinerend verantwoordelijkheid van JenV).

Uitvoering
N.v.t.

Communicatie
Woordvoering BZK is betrokken en heeft het contact met de journalist over beantwoording van de vragen en publicatie

Informatie die niet openbaar gemaakt kan worden

Motivering
In de openbaar gemaakte versie van deze nota zijn alle persoonsgegevens van ambtenaren geanonimiseerd.