Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2023–2024

26 643 Informatie- en communicatietechnologie (ICT)

32 761 Verwerking en bescherming persoonsgegevens

Nr. 1181

BRIEF VAN DE STAATSSECRETARIS VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 5 juni 2024

Op 4 juni 2024 is het Nationaal Cyber Security Centrum (NCSC) door een Duitse journalist op de hoogte gebracht van softwarekwetsbaarheden[1] die gevonden zijn in de Cisco Webex dienst. Via deze kwetsbaarheden kon een aantal metagegevens van vergaderingen van de Nederlandse rijksoverheid worden achterhaald. De zogenaamde metagegevens betroffen informatie over Webex vergaderingen, in ieder geval de titel van de meeting, de organisator/host, tijd van de vergadering en het meeting ID (een random nummer). De rijksoverheid is niet rechtstreeks door de leverancier geïnformeerd.

In het artikel dat de Duitse journalist vandaag heeft gepubliceerd, bleek dat er op basis van de gelekte gegevens bij de Duitse overheid kon worden ingelogd in vergaderingen. Gegeven de wijze waarin de Nederlandse Rijksvideo-omgeving is ingericht, is het niet waarschijnlijk dat dit ook bij ons is gebeurd; dit wordt verder uitgezocht. Ook onderzoeken wij of er gegevens zoals wachtwoorden van de vergaderingen of de inhoud van vergaderingen, chats of gedeelde bestanden inzichtelijk zijn geweest.

Er zal melding worden gemaakt bij de Autoriteit Persoonsgegevens van dit incident en ook zijn de personen waarvan we nu weten dat gegevens zichtbaar waren voor derden geïnformeerd.

Deze kwetsbaarheden zijn al begin mei 2024 gemeld aan de leverancier Cisco. Deze heeft pas gisteravond de kwetsbaarheden openbaar gemaakt[2]. De leverancier heeft ons laten weten dat de kwetsbaarheden inmiddels zijn weggenomen, waardoor het niet meer mogelijk is om van deze kwetsbaarheden gebruik te maken.

[1] Bugs in Cisco Webex Meetings gebruikt voor ongeautoriseerde toegang - Security.NL
[2] Cisco Webex Meetings Meeting Information and Metadata Issue June 2024

kst-26643-1181
ISSN 0921 - 7371
's-Gravenhage 2024

Ik vind het onacceptabel dat dit heeft kunnen gebeuren en dat deze kwetsbaarheden bij de rijksoverheid via de Duitse media tot ons zijn gekomen, in plaats van via de leverancier. Daarbij maak ik mij zorgen over het lekken van informatie op deze wijze en de late reactie van de leverancier. Bestuurders en ambtenaren moeten er te allen tijde vanuit kunnen gaan dat zij veilig kunnen overleggen. Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) neemt deze kwestie daarom zeer serieus en onderzoekt hoe dit heeft kunnen gebeuren.

Cisco Webex wordt als rijksbrede dienst voor videovergaderen aangeboden. Er zijn risicoanalyses en DPIA's gemaakt en er is technisch advies verkregen over de inrichting. Omdat de kwetsbaarheden in het systeem inmiddels verholpen zijn, heeft dit incident op dit moment geen gevolgen voor het gebruik van Webex door de rijksoverheid. We blijven dit wel nauwlettend monitoren. De dienst mag niet gebruikt worden voor overleggen die als zeer vertrouwelijk zijn aangemerkt of waar staatsgeheime informatie wordt besproken. Wij zullen in overleg treden met onze Duitse collega's van het Bundesamt für Sicherheit in der Informationstechnik (BSI) om met hen samen het onderzoek uit te voeren.

Cisco is door CIO Rijk, als opdrachtgever voor deze dienst, gevraagd om morgen nadere uitleg te geven over zowel de kwetsbaarheden en het proces van het melden van dit incident. Cisco zal tevens verzocht worden om op korte termijn een nader onderzoek naar dit incident uit te voeren.

Uw Kamer zal nader geïnformeerd worden over uitkomsten van de genoemde onderzoeken.

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
A.C. van Huffelen