AH 2447

2026Z10203

Antwoord van staatssecretaris Aerdts (Economische Zaken en Klimaat) en de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties (ontvangen 1 juli 2026)

Zie ook Aanhangsel Handelingen, vergaderjaar 2025-2026, nr. 2276

1

Bent u bekend met de bevindingen uit de twee Bloomberg-onderzoeken van 29 januari 2026 en 28 april 2026?

Antwoord

Ja.

2

Beschouwt u het als zorgwekkend dat de onderzoeker stelt dat Meta alle tekstberichten, foto's, audio- en video-opnames in onversleutelde vorm kan opslaan en bekijken en dat Meta sinds ten minste 2019 een "gelaagd machtigingssysteem" hanteert dat toegang verleent aan opdrachtnemers en een significant aantal buitenlandse medewerkers in India?

Antwoord

Ja, doorbreking van verwachte beveiliging is in algemene zin zorgwekkend. Het is wel goed om te vermelden dat berichten in WhatsApp tussen verzender en ontvanger in principe versleuteld zijn. Alleen berichten die worden verzonden naar de Meta AI middels het commando “@Meta AI” gevolgd door een vraag, zijn in te zien door Meta. De rest van de berichtenconversatie blijft volgens Meta versleuteld. WhatsApp heeft wel toegang tot zogenoemde verkeersgegevens (metagegevens).

Andere, niet zakelijk gebruikte diensten van Meta, waaronder Messenger binnen Facebook en Direct Messenger op Instagram, hebben een ander beschermingsniveau.

3

Beschouwt u de verklaringen van voormalige opdrachtnemers van Accenture dat zij en Meta-medewerkers "onbeperkte toegang" hadden tot versleutelde WhatsApp-berichten als zorgwekkend?

Antwoord

Zie antwoord op vraag 2.

4

Indien het antwoord op ten minste een van bovenstaande twee vragen bevestigend luidt, welke consequenties verbindt u hieraan voor het gebruik van WhatsApp door Nederlandse burgers, bewindspersonen en ambtenaren?

Antwoord

Het beleid en de bestaande gedragsregeling voor de digitale werkomgeving voor bewindspersonen en ambtenaren blijft op dit moment ongewijzigd. Zoals toegelicht in de beantwoording van het informatieverzoek van het lid Kathmann (GL-PvdA)[1] heeft de Rijksoverheid voor medewerkers de gedragsregeling voor de digitale werkomgeving opgesteld en geactualiseerd in oktober 2025. De gedragsregeling geeft medewerkers een kader voor het gebruik van digitale middelen zoals berichtenapps, en geeft aan dat het gebruik van berichtenapps enkel voor informeel gebruik is. Het advies luidt: app met beleid maar niet over beleid. Dit advies is ook overgenomen en herhaald in het cyberadvies Phishing via chatapps Signal en WhatsApp.[2] Deze lijn is ook onderdeel van de basisopleiding digitale weerbaarheid die verplicht is voor alle rijksmedewerkers. De gedragsregeling, in combinatie met de basisopleiding, draagt bij aan zorgvuldige omgang met communicatiemiddelen en heeft een risicoreducerend effect op het gebruik daarvan. Op dit moment ziet het kabinet geen aanleiding om de gedragsregeling te herzien en roept het alle medewerkers op deze na te leven, zodat een veilige digitale werkomgeving wordt gewaarborgd.[3] Advies aan Nederlanders die gebruik maken van chatapps, is zich bewust te zijn van mogelijke veiligheidsrisico’s. Over de privacyrisico’s van WhatsApp is informatie beschikbaar op veiliginternetten.nl. Sinds kort is er ook de mogelijkheid een check te doen op de veiligheid van apps via www.appinspector.nl.

Voor bewindspersonen is er het handboek voor bewindspersonen (het ‘Blauwe boek’).[4] Hierin staan aanwijzingen voor de omgang met digitale middelen.

5

[1] Kamerbrief d.d. 20 april 2026, Informatieverzoek lid Kathmann over phishing via chatapps, Brief - Informatieverzoek lid Kathmann over phishing via chatapps.
[2] Cyberadvies. Phishing via chatapps Signal en WhatsApp | AIVD
[3] Kamerstuk 26643 nr. 1508
[4] Handboek voor bewindspersonen | Richtlijn | Rijksoverheid.nl

Bent u bekend met de Amerikaanse CLOUD Act, op grond waarvan de Amerikaanse overheid van in de VS gevestigde bedrijven zoals Meta kan eisen dat zij toegang verlenen tot opgeslagen gebruikersdata, ook wanneer deze betrekking heeft op buitenlandse gebruikers? Zo ja, welke consequenties verbindt de regering hieraan voor het gebruik van WhatsApp door Nederlandse burgers, bewindspersonen en ambtenaren?

Antwoord

Ja, ik ben bekend met de CLOUD Act. Zoals toegelicht in de beantwoording van vraag 4 blijft het beleid en bestaande gedragsregeling voor ambtenaren voor de digitale werkomgeving ongewijzigd.

6

Acht u het mogelijk dat vertrouwelijke communicatie – ondanks de maatregelen die voortvloeien uit de Archiefwet – via Whatsapp wordt verstuurd door ambtenaren en bewindspersonen?

Antwoord

De gedragsregeling voor de digitale werkomgeving resp. het handboek voor bewindspersonen geldt voor iedereen die voor de Rijksoverheid werkzaamheden uitvoert en daarbij gebruikt maakt van de digitale werkomgeving van de Rijksoverheid. Deze regeling sluit aan op de Gedragscode Integriteit Rijk en alle ambtenaren dienen zich hieraan te houden.

7

Welke concrete maatregelen treft u op korte termijn om te voorkomen dat vertrouwelijke bestuurlijke communicatie via WhatsApp plaatsvindt, mede gelet op de ernstige twijfels over de daadwerkelijke end-to-endversleuteling?

Antwoord

De diensten hebben recent een cyberadvies gepubliceerd. Daarnaast is er binnen de Rijksoverheid veel aandacht geweest om niet over beleid te communiceren per chatapplicaties en vooral geen gerubriceerde en gevoelige gegevens te versturen via chatapplicaties.

8

Bent u bereid een onafhankelijk onderzoek in te stellen naar de vraag of WhatsApp-berichten daadwerkelijk end-to-end versleuteld zijn en niet toegankelijk zijn voor Meta, haar medewerkers, opdrachtnemers of andere derden? Zo nee, waarom niet?

Antwoord

We richten onze capaciteit en inspanningen op het realiseren van eigen, veilige digitale voorzieningen. De Rijksoverheid is bezig met een plan voor de ontwikkeling van een eigen, soevereine chatapplicatie voor communicatie tussen ambtenaren onderling. Hierbij maken we, onder andere via het Europees Consortium voor Digitale Infrastructuur (EDIC), gebruik van kennis en ervaring opgedaan door andere Europese lidstaten.

9

Zijn er op dit moment voor bewindspersonen en ambtenaren alternatieve communicatiediensten met end-to-end-versleuteling beschikbaar? Zo ja, welke, en worden deze in de praktijk gebruikt?

Antwoord

We draaien een pilot met een Europese, zakelijke berichtenapp, die voldoet aan hoge eisen op het gebied van veiligheid, privacy, datacontrole en opslag van berichten. Deze app wordt momenteel getest binnen een beperkte groep gebruikers. Op basis van die ervaringen bekijken we hoe we de kennis en ervaring kunnen onderbrengen in de eigen, soevereine chatapplicatie voor communicatie tussen ambtenaren onderling.

10

Hanteert u bij de selectie van communicatiediensten voor overheidsgebruik als criterium dat de implementatie van end-to-end-versleuteling onafhankelijk verifieerbaar moet zijn via openbare broncode, en zo nee, is de regering bereid dit criterium alsnog in te voeren?

Antwoord

De in te richten soevereine chatoplossing zal open source zijn.

11

Bent u bereid het NCSC te verzoeken een vergelijkende veiligheidsanalyse op te stellen van beschikbare open source communicatiediensten — waaronder Signal, Element/Matrix en Wire — met als specifiek doel te beoordelen welke dienst geschikt is voor vertrouwelijke bestuurlijke communicatie?

Antwoord

In 2025 heeft het CIO-beraad van de Rijksoverheid besloten tot het vergroten van soevereiniteit en autonomie via implementatie van een zelf ontwikkelde Rijkschatapplicatie op basis van Matrix/Elements. Matrix/Elements wordt tevens in andere Europese lidstaten gebruikt. In augustus wordt in het CIO-beraad het projectvoorstel voor de autonome chatvoorziening voor communicatie tussen ambtenaren onderling behandeld. Bij de implementatie hiervan wordt rekening gehouden met de noodzakelijke veiligheids- en privacy aspecten.

12

Bent u bereid een voorlichtingscampagne te starten gericht op burgers, ambtenaren en bewindspersonen, waarin wordt gewezen op de ernstige twijfels die bestaan over de vertrouwelijkheid van WhatsApp-berichten? Zo nee, waarom niet?

Antwoord

Ambtenaren en bewindspersonen worden regelmatig geïnformeerd over het gebruik van digitale diensten, zoals door het recent gepubliceerde cyberadvies van de AIVD en MIVD[5].

Inwoners worden doorlopend geïnformeerd via campagnes die erop gericht zijn om de eigen digitale weerbaarheid te vergroten. Bijvoorbeeld via campagnes als ‘Dubbel beveiligd is dubbel zo veilig’ en ‘Laat je niet interneppen’. De beweringen van de onderzoeker vormen op dit moment onvoldoende aanleiding om een dergelijke campagne te kunnen verantwoorden.

[5] Cyberadvies. Phishing via chatapps Signal en WhatsApp | AIVD