



TER BESLUITVORMING

Nota actief openbaar

Ja

Onze referentie

2023-0000152387

Datum

9 maart 2023

Opgesteld door

[Redacted]

Samengewerkt met

AIVD, DS, OIV,
interdepartementaal

Bijlage(n)

1

Aan

Staatssecretaris voor Koninkrijksrelaties en
Digitalisering
Minister van Binnenlandse Zaken en Koninkrijksrelaties

nota

Beleidsbrief over apps en antwoorden Kamervragen
inzake TikTok

Aanleiding

Op 21 maart staat de bijgevoegde beleidsbrief en beantwoording Kamervragen op de agenda van de RDINEV van 21 maart ter besluitvorming. Uw akkoord met inhoud van de brief en verzending na positieve besluitvorming wordt gevraagd.

Geadviseerd besluiten

Beleidsbesluiten

De brief bevat een tweetal beleidsbesluiten, waarmee uw akkoord wordt gevraagd:

- 1) Per direct wordt ambtenaren in dienst van de Rijksoverheid het geïnstalleerd hebben en gebruiken op hun mobiele werkapparatuur van apps van bedrijven uit landen met een offensief cyberprogramma tegen Nederland en/of Nederlandse belangen ontraden. Hiervoor zal op korte termijn communicatie worden ontwikkeld.
- 2) Het doel om te komen tot beleid waarbij mobiele apparaten uitgereikt aan ambtenaren in dienst van de rijksoverheid zo zijn ingericht dat er alleen vooraf toegestane apps, software en/of functionaliteiten kunnen worden geïnstalleerd en gebruikt (managed apparaten).

Kamerbrief

U wordt gevraagd om akkoord met verzending aan de Kamer, na een besluit hiertoe in de RDINEV van 21 maart of de daaropvolgende MR.

Kern

De nota formuleert de gevraagde beleidsbesluiten rondom apps en licht die toe. Deze zijn weergegeven in de voorgestelde Kamerbrief en antwoorden op Kamervragen.

Toelichting

Proces

Na (hoog)ambtelijk overleg de afgelopen periode (zie hierna), is de brief geagendeerd in de RDINEV van 21 maart.

Onderzoek en beleidsbesluiten voor apps

Op 1 en 6 maart heeft een tweetal verdiepende werksessies plaatsgevonden over TikTok met betrokken relevante beleidsdepartementen, de AIVD en het NCSC, om te komen tot een advies over gebruik van TikTok door Rijksambtenaren op

mobiele apparaten. Hierbij is naar TikTok gekeken, langs drie lijnen, te weten 1) dreigingen, 2) te beschermen belangen en 3) veiligheidsrisico's. De beschouwing van de AIVD van 23 februari jl. is hier ook in meegenomen.

Onze referentie
2023-0000152387
Datum
9 maart 2023

Er is door de aanwezigen geconstateerd dat feitelijk (vrijwel) alle op een mobiel apparaat geïnstalleerde apps, dus niet enkel TikTok, toegang (kunnen) krijgen tot (meta)data van gebruikers en deze zouden kunnen verzamelen. Op basis van deze gegevens zouden in het kader van spionage gerichte vervolgacties ingezet kunnen worden. Het is bekend dat er landen met een offensief cyberprogramma zijn tegen Nederland en Nederlandse belangen, waarvoor dit risico met name geldt.

Dit maakt dat er meerdere nationale veiligheidsbelangen zijn die bij gebruik van apps in den brede, voor ambtenaren in dienst van de rijksoverheid in gevaar zouden kunnen komen. Zo kunnen applicaties een spionagerisico vormen richting intellectueel eigendom, inzicht in politieke besluitvorming en processen en de gedragingen van diasporagemeenschappen in Nederland.

Als laatste is stilgestaan bij de weerbaarheid tegen bovenstaande. In de kern zijn er maatregelen mogelijk om risico's rondom apps terug te dringen. De Baseline Informatiebeveiliging Overheid (BIO), artikel 6.2, schrijft reeds voor dat er beleid en ondersteunende beveiligingsmaatregelen behoren te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren. Het gaat hier om mobiele apparaten die Rijksambtenaren krijgen uitgereikt, zogenaamde 'managed devices'. Echter ook met deze maatregelen blijft het apps mogelijk om (sommige) metadata zoals bijvoorbeeld locatie en telefooncontacten te achterhalen.

Er is in de werksessies geconstateerd dat de gesignaleerde risico's rondom digitalisering en cybersecurity in bredere zin, evenals de dreiging uit landen met een offensief cyberprogramma tegen Nederland al langere tijd onderkend zijn. Opeenvolgende Cybersecuritybeelden Nederland (CSBN) en Dreigingsbeelden Statelijke Actoren (DSA) deden deze observaties. Dit heeft onder dit kabinet en vorige kabinetten geleid tot extra investeringen en versterkte inzet hierop. Voor wat betreft de weerbaarheid biedt onder meer de BIO, maar ook bestaande Gedragsregeling Digitale Werkomgeving, handvatten aan organisaties en medewerkers die de risico's kunnen terugdringen.

Gedurende dit traject zijn ook het CIO Beraad, de CISO Raad en de CTO Raad geïnformeerd en geconsulteerd. Daarin zijn aandachtspunten in de uitwerking naar voren gekomen. Bij het toewerken naar het gewenste einddoel van de managed devices zullen zij nauw worden betrokken.

Internationaal

Gedurende totstandkoming van het beleid is er nauw internationaal contact geweest. Uit vrijwel alle landen contacten is gebleken dat landen beleid of adviezen hebben over omgang met apps. De voorgestelde meer technische aanpak van apparaatsinrichting en inzet op gedrag van ambtenaren zoals wordt voorgesteld, is in lijn met inzichten zoals opgehaald in de contacten.

Voorgestelde beleidsbesluiten

Op basis van voorgaande wordt met positief advies van de TFEV gevraagd om akkoord met de volgende twee voorgestelde besluiten/beleidslijnen:

1. Per direct wordt ambtenaren in dienst van de Rijksoverheid het geïnstalleerd hebben en gebruiken op hun mobiele werkapparatuur van apps van bedrijven uit landen met een offensief cyberprogramma tegen Nederland en/of Nederlandse belangen ontraden. Hiervoor zal op korte termijn communicatie worden ontwikkeld.
2. Het doel om te komen tot beleid waarbij mobiele apparaten uitgereikt aan ambtenaren in dienst van de rijksoverheid zo zijn ingericht dat er alleen vooraf toegestane apps, software en/of functionaliteiten kunnen worden geïnstalleerd en gebruikt (managed apparaten).

Onze referentie

2023-0000152387

Datum

9 maart 2023

Advies CZW over beleidsbesluiten:

Voor wat betreft het voorgenomen beleid, stelt CZW dat het Coördinatiebesluit organisatie, bedrijfsvoering en informatiesystemen rijksdienst 2011, specifiek artikel 2, eerste lid onder b, een grondslag biedt om tot een aanwijzing over te gaan in verband met de noodzakelijke operabiliteit of beveiliging van informatiesystemen.

In dit geval luidt de aanwijzing om het gebruik van apps uit landen met een offensief cyberprogramma tegen Nederland en/of Nederlandse belangen, op apparaten uitgereikt door het Rijk aan ambtenaren in dienst van de rijksoverheid te ontraden. De motivering om tot deze aanwijzing over te gaan, is uiteengezet onder het kopje "Onderzoek en beleidsbesluiten apps". De implementatie van en communicatie hierover wordt waar nodig verder uitgewerkt en afgestemd met de relevante gremia.

Besluit verzending Kamerbrief en meesturen AIVD-beschouwing

In de brief staan nu de besluiten geformuleerd zoals via de TFEV en interdepartementaal afgestemd. Na uw akkoord zal de brief met ook de antwoorden op de Kamervragen worden verzonden. Ook wordt u gevraagd akkoord te gaan met het meesturen van de beschouwing van de AIVD van 23 februari. [REDACTED]

Financiële overwegingen

Eventuele consequenties (financieel en qua capaciteit) van de ingezette koers bij CIO Rijk en de departementen zijn niet onderzocht. Het is wel de verwachting dat toewerken naar volledig managed devices middelen en capaciteit zal kosten.

Krachtenveld

In het Commissiedebat *Inzet algoritmes en data-ethiek binnen de Rijksoverheid* op 15 februari jl. is door enkelen partijen gevraagd of een verbod van de app TikTok voor Rijksambtenaren op zijn plaats zou zijn. De staatssecretaris heeft toen toegezegd hierop in te gaan in het antwoord op de voorliggende vragen.

Uitvoering

In toewerken naar de managed apparaten is het noodzakelijk dit met de departementen en uitvoeringsorganisaties te doen, waaronder de shared service organisaties die deze apparaten uitreiken en beheren.

Communicatie

Nationale en internationale ontwikkelingen rondom TikTok hebben aandacht van (internationale) media. Voorlichting is betrokken bij dit traject.

Onze referentie
2023-0000152387

Datum
9 maart 2023

Informatie die niet openbaar gemaakt kan worden

[Redacted text block]

Motivering

In de openbaar gemaakte versie van deze nota zijn alle persoonsgegevens van ambtenaren geanonimiseerd. Daarnaast is informatie niet openbaar gemaakt vanwege het procesbelang van de staat en de eenheid van kabinetsbeleid.

Bijlagen

Volgnummer	Naam	Informatie
1	Beslisnota Kamerbrief en antwoorden TikTok	
2	Beschouwing AIVD	
	[Redacted]	
	[Redacted]	
	[Redacted]	