gemeente Barneveld

Organisatieonderdeel: Dienstverlening
Behandelaar: V. Verhagen
Telefoonnummer: 06-11603953

Voorstelnr. 2916
Barneveld, 4 juli 2023
Portefeuillehouder: W. Oosterwijk

☒Ter kennisname naar de raad
Nummer beleidsproduct:

☐Op overzicht Bestaand beleid (website)

Onderwerp: **Gebruik van applicaties uit landen met een offensief cyberprogramma tegen Nederland**

Gevraagde beslissing:
1. In lijn met het advies van de Vereniging van Nederlandse Gemeenten (VNG), het beleid van de Rijksoverheid te volgen met betrekking tot het weren van applicaties, op mobiele werkapparatuur, uit landen die een offensief cyberprogramma tegen Nederland en/of Nederlandse belangen hanteren.
2. De communicatiekanalen die deze applicaties eventueel bieden niet in te zetten als intern of extern communicatiekanaal.
3. Het besluit ter kennisname door te sturen aan de gemeenteraad.

1. Inleiding

In de media is veel te lezen over de gevaren van applicaties afkomstig uit landen met een offensief cyberprogramma gericht tegen Nederland (verder: “de bedoelde applicaties”). Deze landen zijn, volgens de AIVD, op dit moment Rusland, China, Iran en Noord-Korea.

Op 23 februari 2023 heeft de AIVD haar beschouwing (zie bijlage “beschouwing AIVD 23-feb-23.pdf”) uitgebracht betreffende de risico’s die zijn verbonden aan het gebruik van de bedoelde applicaties.

Naar aanleiding van deze beschouwing heeft de staatssecretaris voor digitalisering op 21 maart 2023 per direct het gebruik van de bedoelde applicaties op mobiele werkapparatuur door rijksambtenaren ontraden (zie bijlage “beantwoording-kamervragen-2023z01674.pdf”).

Vervolgens heeft de VNG op 17 mei 2023 een advies uitgebracht (zie bijlage “advies VNG 17-mei-2023.pdf”) de lijn van het Rijk te volgen om de bedoelde applicaties te weren van werktelefoons en niet in te zetten als communicatiekanaal voor inwoners.

Wat zijn de bedoelde applicaties?
De belangrijkste applicatie waar het om gaat is TikTok, maar er zijn er meer (die (ook) niet worden gebruikt door Barneveld). Zie hiervoor pagina 4 onder “Chinese apps (top)” van bijlage “advies VNG 17-mei-2023.pdf”.

2. Beoogd effect

a) Meetbaar effect
Op de door Barneveld beheerde mobiele werkapparatuur zijn geen applicaties geïnstalleerd die afkomstig zijn van landen met een offensief cyberprogramma tegen Nederland en/of Nederlandse belangen.

b) Maatschappelijk effect
Inwoners en bedrijven van Barneveld kunnen zien dat de gemeente haar verantwoording neemt ten aanzien van het veilig houden van de dienstverlening die zij biedt.

3. Argumenten

Risico's bij gebruik van de bedoelde applicaties

Datadiefstal en spionage: De bedoelde applicaties kunnen worden gebruikt om gegevens te stelen en voor spionage. Dit kan leiden tot toegang tot persoonlijke gegevens en overheidsinformatie, met mogelijke schade tot gevolg.

Cyberaanvallen: Deze applicaties kunnen kwetsbaarheden bevatten die kwaadwillende actoren in staat stellen onze systemen aan te vallen, gevoelige informatie te stelen of essentiële diensten te verstoren.

Verspreiding van malware: Applicaties uit risicolanden kunnen dienen als transportmiddel voor malware, zoals virussen, wormen of spyware, wat kan leiden tot de besmetting van systemen en schade aan gegevens en functionaliteit.

Advies VNG
De risico's op het gebied van spionage zijn dermate dat de VNG adviseert de bedoelde applicaties te weren van werktelefoons en niet in te zetten als communicatiekanaal voor inwoners.

Gebruik door gemeente Barneveld
Team Communicatie geeft aan dat de gemeente op dit moment TikTok niet als communicatiekanaal gebruikt. De directe impact van het niet inzetten van TikTok is voor Barneveld dan ook verwaarloosbaar.

4. Kanttekeningen

Medewerkers die TikTok gebruiken
Een inventarisatie door I&A laat zien dat TikTok is geïnstalleerd op 33 van de 695 mobiele apparaten die de gemeente beheert.
Er zijn dus enkele medewerkers die TikTok hebben geïnstalleerd voor privédoeleinden. Dat is nu nog toegestaan omdat privégebruik van de zakelijke toestellen is toegestaan.
Het gebruik van TikTok op zakelijke toestellen is echter na het overnemen van het advies van de VNG niet meer toegestaan. De betreffende medewerkers zullen, als zij TikTok willen blijven gebruiken, een ander, niet door de organisatie verstrekt, apparaat daarvoor moeten gebruiken.

Onderhoud
Op regelmatige basis zal moeten worden gekeken of er landen moeten worden op- of afgevoerd van de lijst van landen met een offensief cyberprogramma tegen Nederland en/of Nederlandse belangen.
Ook moet op basis van die lijst van landen een lijst met te weren applicaties worden bijgehouden. Op basis van eventuele wijzigingen in de lijst met applicaties wordt het proces gestart dat leidt tot communicatie van de wijziging en de uiteindelijke verwijdering of toevoeging.

Deze werkzaamheden worden belegd bij de Chief Information Officer (CISO).

5. Financiën

De gemeente beschikt nu al over de technische middelen om specifieke applicaties van de zakelijke toestellen te verwijderen. Er zijn geen extra financiën nodig.

6. Participatie en communicatie

a) Participatie
N.v.t.

b) Communicatie
Zo spoedig mogelijk na het besluit zal via intranet aan medewerkers worden gecommuniceerd.
Voor nieuwe medewerkers zal dit worden gedaan middels aanpassing van de overeenkomst “Gebruik van in bruikleen verstrekte (ICT-)apparatuur en Communicatiemiddelen”.
Na het communiceren van het besluit via intranet zal medewerkers via email worden gevraagd de bedoelde applicaties zelf te verwijderen. Dit verzoek zal, indien nodig, nog eens worden herhaald.
Vervolgens zal worden gecommuniceerd dat de bedoelde applicaties door de ICT-beheerorganisatie worden verwijderd van de zakelijke toestellen.
Het bestaan van dit beleid zal tevens worden toegevoegd aan het overzicht met Vigerend ICT beleid.

7. Uitvoering

Planning:
Start communicatie: datum besluit + 2 weken
Verwachtte afronding (automatische verwijdering en aanpassing bruikleenovereenkomst): datum besluit + 8 weken.

Evaluatie/controle:
De CISO zal toezien op de voortgang van de implementatie van het besluit.

8. Bijlagen

1. advies VNG 17-mei-2023.pdf
2. beschouwing AIVD 23-feb-23.pdf
3. beantwoording-kamervragen-2023z01674.pdf

Advies over het gebruik van apps uit landen met een offensief cyberprogramma

Inleiding
In de media is veel te lezen over de gevaren van apps afkomstig uit onveilige landen, zoals TikTok. Begin 2023 heeft het Rijk besloten de installatie en het gebruik van apps van bedrijven uit landen met een offensief cyberprogramma tegen Nederland en/of Nederlandse belangen op mobiele werkapparatuur van ambtenaren in dienst van de Rijksoverheid te ontraden.[1] Dit op advies van de directeur van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD). De AIVD waarschuwt voor de verhoogde spionagerisico's die het gebruik van software uit dergelijke landen met zich meebrengt. De VNG sluit zich bij het beleid van het Rijk aan. In deze handreiking leest u meer over de achtergrond daarvan en hoe de gemeente hiermee praktisch aan de slag kan gaan.

Wat adviseert de AIVD en waarom?
In het geval dat een applicatie in beheer is in een land met een offensief cyberprogramma gericht tegen Nederland en Nederlandse belangen, dan is er sprake van een verhoogd spionagerisico. Applicaties hebben vaak toegang tot alle gegevens van de mobiele telefoon. Apps vragen hier veelal via de gebruikersvoorwaarden vooraf toestemming voor. De gebruiker kan ook zelf informatie toevoegen. Er kan daarbij gedacht worden aan persoonsgegevens van de gebruiker zoals contactgegevens, bestanden zoals foto’s, of contacten van de gebruiker. Maar ook aan gegevens over het specifieke apparaat en de netwerken die gebruikt worden. In specifieke gevallen worden toetsaanslagen van gebruikers onderschept. Daarom is het volgens de AIVD raadzaam een afweging te maken tussen de noodzaak van een bepaalde applicatie enerzijds en het daarbij behorende risico anderzijds. Het Rijk heeft op grond daarvan besloten het gebruik van deze apps te ontraden.

Wat adviseert de VNG aan de gemeente?
Voor gemeenten speelt de te maken afweging zich op twee gebieden af.

Enerzijds gebruiken gemeenten bepaalde apps om in contact te staan met hun inwoners en ondernemers. Gemeenten willen dichtbij hun inwoners en ondernemers staan. Daarbij maken ze gebruik van tools en platforms waar (doelgroepen onder) de inwoners ook op aanwezig zijn. Burgers moeten omgekeerd contact met de gemeente kunnen zoeken via het kanaal van hun keuze. Via Omnichannel kanaalsturing kunnen burgers naar het juiste kanaal voor het afdoen van hun vraag worden toegeleid. Om te bepalen of bepaalde social media kanalen wel of niet geschikt zijn om als communicatiemiddel te gebruiken, is door de IBD een gespreksstarter ontwikkeld.[2] De gespreksstarter voorziet gemeenten van overwegingen en praktische tips bij het nemen van een besluit over de inzet van social media als communicatiemiddel naar inwoners.
Anderzijds maken gemeenten een afweging hoe om te gaan met de installatie en het gebruik van apps op *mobile devices* van gemeentelijke medewerkers en bestuurders vanuit het

[1] Dat staat in het antwoord op de vragen van de Tweede Kamer over de app TikTok door staatssecretaris voor digitalisering van 21 maart 2023.
[2] https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2023/03/gespreksstarter-gebruik-social-media-door-gemeenten_.pdf

veiligheidsperspectief. Iedere gemeente(raad) kan zelf bepalen welk beleid het hierin hanteert, tenzij wet- en regelgeving en richtlijnen anders bepalen.

Voor apps afkomstig van bedrijven uit landen met een offensief cyberprogramma tegen Nederland en/of Nederlandse belangen geldt die afweging in principe niet: gebruik hiervan wordt ontraden. Uit het advies van de AIVD blijkt immers dat er een risico is op spionage, dat niet opweegt tegen voordelen van het gebruik van dergelijke apps. Daarom worden gemeenten geadviseerd om de lijn van het Rijk te volgen om apps afkomstig van landen met een offensief cyberprogramma tegen Nederland en/of Nederlandse belangen te weren van werktelefoons en niet in te zetten als communicatiekanaal voor inwoners.

Om welke landen en om welke apps gaat het?
Voorbeelden van landen met een offensief cyberprogramma zijn Rusland, China, Iran en Noord-Korea. Van deze landen is bekend dat inlichtingendiensten de intentie en capaciteit hebben om spionageoperaties richting Nederlandse overheden, bedrijven en personen uit te voeren. In bijlage A treft u een overzicht van veel gebruikte apps uit China.

Worden deze apps wel gebruikt door gemeentelijke medewerkers?
Het komt voor dat medewerkers van de gemeente apps afkomstig uit bovengenoemde landen op hun werktelefoon of werklaptop hebben geïnstalleerd. Soms hebben deze apps een functie omdat daarmee een bepaalde doelgroep onder inwoners kan worden bereikt. Vaker hebben deze apps hebben geen functionele toepassing, maar worden ze ter vermaak ingezet. Daarnaast gebruiken medewerkers hun werktelefoons of –laptops ook wel eens voor privédoeleinden, zoals amusement voor de kinderen. Het is in de eerste plaats is van belang dat de gemeente zich uitspreekt over de omgang hiermee. Soms zijn hierover al regels opgenomen in het personeelsbeleid, in beleid rondom *Mobile Device Management* en/of in gebruikersovereenkomsten die medewerkers moeten ondertekenen als zij een telefoon en/of laptop van de gemeente gebruiken. De VNG adviseert deze beleidsstukken waar nodig te herzien, zodat de hierin opgenomen afspraken overeenstemmen met dit advies. Indien er nog geen beleidsstukken zijn waarin dit is vastgelegd, wordt geadviseerd hier zo snel mogelijk invulling aan te geven.

Geldt het advies voor alle medewerkers van de gemeenten?
Het Rijk kiest ervoor het gebruik van apps uit landen met een offensief cyberprogramma op werkapparaten te ontraden voor alle medewerkers; op termijn moet dat afgedwongen worden door ‘managed apparaten' (zie onder). U kunt dit voorbeeld volgen of, zoals de AIVD adviseert, een risicoanalyse uit laten voeren om te bepalen waar het gebruik van applicaties een risico kan vormen voor de vertrouwelijkheid van gegevens en/of voor medewerkers of locaties. Niet alle medewerkers lopen dezelfde risico's bij het gebruik van onveilige apps. De grootste risico's worden gelopen door leden van het college van B&W, de ambtelijke topfuncties en specifieke functies die voor de (informatie)veiligheid van belang zijn. Het risico dat wordt gelopen door laag-ambtelijke en uitvoerende medewerkers is kleiner.

Hoe moet de gemeente het beleid vastleggen en uitvoeren?
Gemeenten bepalen zelf het beleid over het gebruik van werkapparaten. Dit geldt zowel voor de inzet van apps als voor de voorwaarden voor het gebruik van een werktelefoon voor privédoeleinden en/of over het gebruik van privé-apparatuur voor zakelijke doeleinden. Het college

kan besluiten het advies van de VNG op te volgen. Vervolgens moet dat worden vastgelegd in (aanvullende) voorwaarden voor het gebruik van werktelefoons. In bijlage B treft u een model daarvoor aan. Tot slot moet het beleid actief worden gecommuniceerd onder de medewerkers.

Hoe moet het beleid worden gehandhaafd?
Het is van belang het beleid te handhaven, en regelmatig te controleren of door de medewerkers aan de voorwaarden voor het gebruik van werkapparaten wordt voldaan. Het Rijk heeft besloten op korte termijn toe te werken naar een situatie 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. Het worden dan in zijn geheel zogeheten 'managed apparaten', waarvoor is bepaald welke apps daarop kunnen worden geïnstalleerd en gebruikt door de gebruiker. De gemeente kan overwegen dit voorbeeld te volgen.

Hoe moet er worden omgegaan met het gebruik van privé toestellen?
Medewerkers die hun privé toestellen gebruiken voor werkdoeleinden moeten erop gewezen worden dat het gebruik van apps uit onveilige landen voor eenieder risico's met zich meeneemt. Als zij het advies negeren voor wat betreft het gebruik op hun privé toestel, is het des te belangrijker is dat dit toestel niet wordt gebruikt voor zakelijke doeleinden. Daarover kunnen afspraken met medewerkers worden gemaakt.

Hoe moet de communicatie met burgers en ondernemers vorm krijgen?
Bepaalde onveilige apps zijn populaire informatiekanalen bij specifieke doelgroepen, bijvoorbeeld jeugdigen. Door geen gebruik meer te maken van deze kanalen moet een andere kanaalstrategie worden bepaald om de doelgroep te bereiken. Het is van belang om inwoners en ondernemers duidelijk te maken waarom de gemeente ervoor kiest niet via alle apps digitaal te communiceren. Langs deze weg kan ook het publiek bewust worden gemaakt van de risico's die zij lopen voor privacy en informatieveiligheid.
De inzet van bepaalde social media kanalen die niet afkomstig zijn van bedrijven uit landen met een offensief cyberprogramma tegen Nederland en/of Nederlandse belangen ten behoeve van communicatie met inwoners is in principe geoorloofd, mits daarvoor de juiste afwegingen zijn gemaakt. Hiervoor verwijzen we nogmaals naar de gespreksstarter voor gebruik social media door gemeenten.[3]

[3] https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2023/03/gespreksstarter-gebruik-social-media-door-gemeenten_.pdf

Bijlage A

Chinese apps (top)
• **TikTok** — Bytedance
• **Lemon8** — Bytedance
• **CapCut** — Bytedance
• **Pinduoduo** — PDD Holdings
• **Temu** — PDD Holdings
• **CamScanner** — Intsig Information
• **Shein** — Roadget Business
• **TurboVPN** — Innovative Connecting
• **WeChat** — Tencent
• **UC Browser** — Alibaba Group
• **SHAREit** — SHAREit Technologies

Bron: https://www.komando.com/security-privacy/china-based-apps/883845/

Chinese a**pps** (overig)
• **LIKE**
• **CM Browser**
• **Xender**
• **TurboVPN**
• **Viva Video**
• **Beauty Plus**
• **Vault-Hide**
• **NewsDog**
• **Virus Cleaner**
• **SHEIN**
• **Vigo Video**
• **Weibo**
• **Bigo Live**
• **UC News**
• **ClubFactory**
• **Helo**
• **Kwai**
• **ROMWE**
• **Photo Wonder**
• **APUS Browser**

• **Perfect Corp**
• **Mi Community**
• **DU recorder**
• **YouCam Makeup**
• **Mi Store**
• **360 Security**
• **DU Browser**
• **DU Battery Saver**
• **DU Cleaner**
• **DU Privacy**
• **Clean Master – Cheetah**
• **CacheClear DU apps studio**
• **Baidu Map**
• **Baidu Translate**
• **Wonder Camera**
• **ES File Explorer**
• **QQ International**
• **QQ Launcher**
• **QQ Player**
• **QQ Security Centre**
• **QQ Music**
• **QQ Mail**
• **QQ NewsFeed**
• **WeSync**
• **SelfieCity**
• **Parallel Space**
• **Mi Video call – Xiaomi**
• **Mail Master**
• **Clash of Kings**

Bron: https://www.itechfever.com/suspicious-chinese-apps-and-alternatives/

Bijlage B

Door de verantwoordelijkheden op het gebied van informatiebeveiliging in het arbeidscontract van werknemers, de arbeidsovereenkomst met externen en het personeelsreglement[1] vast te leggen, worden enerzijds de verwachtingen duidelijk vastgelegd en anderzijds kan men bij eventuele incidenten terugvallen op deze overeenkomsten. Het maakt hierbij niet uit of men direct voor de gemeente werkt, via een uitzendorganisatie/detacheringbureau, of via uitbesteding. In het vervolg wordt zowel het arbeidscontract als de arbeidsovereenkomst aangeduid als contract.

Neem regels met betrekking tot ‘goed gedrag’ op in het contract dat de werkrelatie regelt. Onder ‘goed gedrag’ wordt onder andere verstaan het eerbiedigen van relevante wet- en regelgeving, maar ook de omgang met de middelen van de gemeente die ter beschikking gesteld zijn en het gebruik van informatiesystemen. Verder valt het signaleren van zwakke plekken in de verdediging onder dit gedrag (het ‘bewijzen’ van zwakke plekken is echter niet toegestaan).

Neem verder in het contract op dat het deze regels ten opzichte van ‘goed gedrag’ ook van kracht zijn buiten het terrein van de werkgever en buiten de kantoortijden, zodra een relatie met de gemeente herkenbaar is. Bijvoorbeeld internet, e-mail en sociaal mediagedrag.

Aandachtspunten met betrekking tot contracten:

- Eisen ten aanzien van informatiebeveiliging moeten in de functiebeschrijving opgenomen zijn. De diverse functies zijn beschreven, inclusief de gevoelige informatie waartoe men toegang heeft.
- Als er gebruik gemaakt wordt van een personeelsreglement maakt dit deel uit van het arbeidscontract. Hierin kunnen extra eisen ten aanzien van informatiebeveiliging zijn opgenomen.

Aandachtspunten met betrekking tot geheimhoudings- en een integriteitsverklaring:

- In contracten met werknemers moet een clausule opgenomen worden waarin geheimhoudingsplicht wordt benoemd en afspraken hierover worden gemaakt. Medewerkers moeten een geheimhoudingsverklaring met boetebeding (sancties)[4] tekenen zolang er nog geen ambtseed is afgelegd.
- In contracten met externe bedrijven (bijvoorbeeld ICT-leveranciers, uitzend- en detacheringbureaus[5]) moet een clausule opgenomen worden waarin geheimhoudingsplicht wordt benoemd en afspraken hierover worden gemaakt. Het gaat hierbij om een geheimhoudings- en een integriteitsverklaring met boetebeding (sancties).
- De geheimhoudings- en een integriteitsverklaring behoren individueel te zijn. Wanneer er sprake is van een collectief contract, dan moet daarin beschreven zijn, dat er aparte individuele geheimhoudingsverklaringen gebruikt worden.
- Maak duidelijk, dat de geheimhouding zowel tijdens de contractperiode als na afloop van het contract geldt.

- De geheimhoudings- en een integriteitsverklaring worden actueel gehouden door de Human Resource (HR) / Personeel en Organisatie (P&O)-adviseur en zijn in lijn met het informatiebeveiligingsbeleid.[6]
- De direct leidinggevende is verantwoordelijk voor de controle op naleving van de afspraken die in de clausule met betrekking tot de geheimhoudingsplicht zijn opgenomen. De leidinggevende dient incidenten te bespreken met de betrokken medewerker en de mogelijke consequenties (disciplinaire maatregelen) kenbaar te maken.

Aandachtspunten met betrekking tot apparatuur en software in personeelsreglement:

- Beschrijf in het personeelsreglement het toegestane en het verboden gedrag van medewerkers met betrekking tot apparatuur en software die door het bedrijf ter beschikking gesteld zijn. Door dit op te nemen in het personeelsreglement, wordt het een onderdeel van het arbeidscontract. Bij medewerkers die niet onderworpen zijn aan het personeelsreglement geldt, dat de omgang met apparatuur en software in het contract opgenomen behoort te zijn.
- Beschrijf in het personeelsreglement het toegestane en het verboden gedrag van medewerkers op het internet, bij het interne en externe e-mailverkeer en bij het gebruik van sociale media, zoals LinkedIn, Facebook, Twitter of bijvoorbeeld Instagram. Door deze aandachtspunten op te nemen in het personeelsreglement, wordt het een onderdeel van het arbeidscontract. Bij medewerkers die niet onderworpen zijn aan het personeelsreglement geldt, dat bovenstaande aandachtspunten onderdeel van het contract behoren te zijn.

Zie voor meer informatie:

Handreiking Mobile Device Management BIO:
https://www.informatiebeveiligingsdienst.nl/product/mobile-device-management/

Handreiking Personeelsbeleid gemeente BIO:
https://www.informatiebeveiligingsdienst.nl/product/personeelsbeleid/

[1] Het personeelsreglement wordt ook wel personeelshandboek, personeelsregeling of arbeidsvoorwaardenreglement genoemd en is een aanvulling op de cao en/of arbeidsovereenkomst, waarin de arbeidsvoorwaarden (nader) zijn uitgewerkt. Het bevat belangrijke procedures, regelingen en overige voorwaarden ten behoeve van u en uw werknemers. Voorbeelden hiervan zijn: verzuimreglement, verlof et cetera. Het personeelsreglement maakt onderdeel uit van de arbeidsovereenkomst. De werknemer is daarom gehouden om de voorschriften en regels in het reglement na te leven, want deze heeft immers zijn/haar handtekening gezet onder de arbeidsovereenkomst.

[2] https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/basisregistraties-en-afsprakenstelsels/inhoud-basisregistraties/

[3] De voorwaarden met betrekking tot de basisregistatries zijn vastgelegd in de aansluitvoorwaarden op basisregistraties. Het niet voldoen aan de aansluitvoorwaarden kan leiden tot afsluiting van de basisregistratie zoals de Basisregistratie Personen (BRP), waardoor primaire bedrijfsvoering in gevaar komt.

[4] Zie hiervoor ook het operationele product ‘Handreiking Geheimhoudingsverklaringen’

[5] Aan de uitzendbureaus is de verplichting opgelegd om de uitzendkrachten een geheimhoudings- en een integriteitsverklaring te laten ondertekenen. Check of dit ook daadwerkelijk is gebeurd en en vraag altijd om een kopie van de verklaring.

[6] Zie hiervoor ook het operationele product ‘Voorbeeld Informatiebeveiligingsbeleid van de gemeente’.

Algemene Inlichtingen- en
Veiligheidsdienst
*Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties*

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
T.a.v. de Rijks CISO
Turfmarkt 147
2511 DP DEN HAAG

Postadres
Postbus 20010
2500 EA Den Haag

Contact

Ons kenmerk

Uw kenmerk

Bijlagen
0

Datum 23 februari 2023
Betreft Beschouwing risico's gebruik applicaties uit landen met een offensief cyberprogramma gericht tegen Nederland

Geachte

In reactie op uw schriftelijke verzoek d.d. 23 februari 2023 komt de AIVD tot een beschouwing van de risico's van het gebruik van applicaties uit landen met een offensief cyberprogramma gericht tegen Nederland en Nederlandse belangen door (rijks)ambtenaren. Dit document gaat in algemene zin in op de risico's van dergelijke applicaties. Een actueel voorbeeld waarop onderstaande beschouwing van toepassing is, is TikTok.

De AIVD benadrukt dat het gebruik en de aanwezigheid van mobiele telefoons en de daarop geïnstalleerde applicaties te allen tijde een inherent spionagerisico vormen. In dit kader wijzen we u ook op onze hand-out 'Uw digitale veiligheid' voor rijksambtenaren en onze informatiefolder 'Op reis naar het buitenland'. De verzameling en opslag van gegevens door applicaties maakt gebruikers kwetsbaar voor spionageactiviteiten. Dit is in het bijzonder het geval wanneer applicaties door bedrijven en organisaties buiten Europa in beheer zijn.

Statelijke actoren investeren in mogelijkheden om toegang te krijgen tot grote datastromen die voortkomen uit het gebruik van mobiele apparatuur. Bij dergelijke datastromen is te denken aan telecommunicatie en de bijbehorende metadata, maar ook telemetriedata vormt in dit kader een voorstelbare interesse van statelijke actoren. Deze datastromen bevatten doorgaans persoonsgegevens die gebruikers aan de fabrikant afstaan door gebruik te maken van de betreffende applicatie. Hieruit kunnen statelijke actoren gevoelige informatie verwerven en personen van belang identificeren, profileren en lokaliseren.

In het geval dat een applicatie in beheer is in een land met een offensief cyberprogramma gericht tegen Nederland en Nederlandse belangen, dan is er sprake van een verhoogd spionagerisico. Voorbeelden van landen met een dergelijk offensief cyberprogramma zijn Rusland, China, Iran en Noord-Korea. Van deze landen is bekend dat inlichtingendiensten de intentie en capaciteit hebben om spionageoperaties richting Nederlandse overheden, bedrijven en personen uit te voeren. Dergelijke spionageoperaties vinden veelvuldig plaats. Vaak hebben statelijke actoren uit landen met een offensief cyberprogramma verregaande mogelijkheden om toegang te verkrijgen tot gegevens die in beheer zijn bij bedrijven uit dat land.

Zo kunnen veel offensieve inlichtingendiensten organisaties en datacentra verplichten hun gebruikersgegevens te delen, of in bepaalde gevallen fabrikanten zelfs verzoeken om technische voorzieningen in de software aan te brengen die toegang of meekijken voor statelijke actoren mogelijk maken.

Gezien de interesse van statelijke actoren met een offensief cyberprogramma gericht tegen Nederland en Nederlandse belangen in de verwerving van persoonsgegevens, alsook de verregaande technische en wetgevende mogelijkheden van deze statelijke actoren om dergelijke persoonsgegevens te vergaren, waarschuwt de AIVD voor de verhoogde spionagerisico's die het gebruik van software uit deze landen met zich meebrengt. Applicaties hebben vaak toegang tot alle gegevens van de mobiele telefoon en daarom is het raadzaam een grondige afweging plaats te laten vinden tussen de noodzaak van een bepaalde applicatie enerzijds en het daarbij behorende risico anderzijds. U kunt een risicoanalyse uit laten voeren om te bepalen waar het gebruik van applicaties een risico kan vormen voor de vertrouwelijkheid van gegevens en/of voor medewerkers of locaties. Het centraal beheren van mobiele telefoons door middel van bijvoorbeeld *Enterprise Mobility Management*, waarbij door de beheerder geschikt bevonden applicaties centraal toegestaan kunnen worden, kan daarbij een oplossing bieden.

Hoogachtend,
De directeur-generaal van de Algemene Inlichtingen- en Veiligheidsdienst,
namens deze.

Directeur Inlichtingen

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA Den Haag

www.rijksoverheid.nl
www.facebook.com/minbzk
www.twitter.com/minbzk
www.linkedin.com/company/ministerie-van-bzk

Kenmerk
2023-0000159485

Uw kenmerk
2023Z01674

Datum	21 maart 2023
Betreft	Beantwoording Kamervragen (2023Z01674) en maatregelen inzake het weren van apps op mobiele devices van rijksambtenaren

Op 2 februari 2023 zijn er schriftelijke vragen gesteld, met kenmerk 2023Z01674, door het lid Dekker-Abdulaziz (D66) over de mogelijkheid om de Chinese applicatie TikTok te weren op mobiele devices van medewerkers van de Rijksoverheid. In het debat *Inzet algoritmes en data-ethiek binnen de Rijksoverheid* op 15 februari jl. heb ik toegezegd nader onderzoek te doen. Er is in dat debat ook door enkele partijen gevraagd of Nederland niet net als de Verenigde Staten een verbod voor gebruik door ambtenaren moet instellen vanwege het potentieel hoge veiligheidsrisico. Sinds het debat hebben de Europese Commissie, Raad van de Europese Unie, en het Europees Parlement het gebruik van TikTok opgeschort. In deze brief zal ik ingaan op het uitgevoerde onderzoek, en aangeven welk beleid ik hierop ga volgen. Ook zijn de antwoorden op de schriftelijke vragen bijgevoegd, mede namens de minister van Binnenlandse Zaken en Koninkrijksrelaties.

Onderzoek veiligheidsrisico's
Op basis van de vragen van de Kamer is aan de AIVD gevraagd een advies te geven. De conclusie daarvan is dat het gebruik en de aanwezigheid van mobiele telefoons en de daarop geïnstalleerde applicaties te allen tijde een inherent spionagerisico vormen. Het is daarom raadzaam altijd een grondige afweging plaats te laten vinden tussen de noodzaak van het installeren van een bepaalde applicatie enerzijds en het daarbij behorende risico anderzijds. Gebruik van apps van bedrijven uit landen met een offensief cyberprogramma door ambtenaren in dienst van de rijksoverheid[1] verhoogt dit risico. Voorbeelden van landen met een dergelijk offensief cyberprogramma zijn Rusland, China, Iran en Noord-Korea. Het overgaan op apparaten die door de werkgever beheerd worden is een meer structurele oplossing voor dit risico. De beschouwing van de AIVD, die de basis was voor verder interdepartementaal onderzoek, is ter informatie toegevoegd als bijlage bij deze brief.

[1] Dit zijn alle ambtenaren in dienst bij de departementen en daaronder vallende agentschappen en andere uitvoeringsorganisaties.

In algemene zin hebben applicaties vaak toegang tot alle gegevens van de mobiele telefoon. Apps vragen hier veelal via de gebruikersvoorwaarden vooraf toestemming voor. De gebruiker kan ook zelf informatie toevoegen. Er kan daarbij gedacht worden aan persoonsgegevens van de gebruiker zoals contactgegevens, bestanden zoals foto's, of contacten van de gebruiker. Maar ook aan gegevens over het specifieke apparaat en de netwerken die gebruikt worden. In specifieke gevallen worden toetsaanslagen van gebruikers onderschept.

Er is in mijn onderzoek ook nauw contact geweest met een aantal partnerlanden in de EU en de Europese Commissie, over hun inschattingen en hun beleidskeuzes voor wat betreft apps op mobiele apparaten in gebruik door hun overheidsambtenaren. Hieruit komt het beeld naar voren dat landen verschillende keuzes maken, maar dat veel landen maatregelen hebben genomen ter beveiliging van telefoons van hun ambtenaren. Enkele landen hebben gekozen voor een specifiek verbod op TikTok, een aantal landen ontraadt of verbiedt in meer generieke zin het gebruik van apps van bedrijven uit bepaalde landen vanwege de inherente risico's. Een aantal landen heeft aangegeven dat zij ervoor gekozen hebben hun mobiele apparaten zo in te richten, dat enkel vooraf toegestane apps geïnstalleerd en gebruikt kunnen worden. We volgen ook de ontwikkelingen buiten de Europese Unie. Daarbij hebben we kennis genomen van het verbod dat het Verenigd Koninkrijk als voorzorgsmaatregel heeft ingesteld voor TikTok op overheidsapparatuur, toewerkend naar een versterking van het beleid rondom apps van derde partijen. Ook worden de maatregelen en stappen die de Verenigde Staten zetten gevolgd, waar bijgevoegde vragen ook al aan refereren.

Beleid voor de rijksoverheid
In het licht van de hierboven genoemde risico's en de beschouwing van de AIVD acht ik het nodig om aanvullende stappen op het gebied van veiligheid van mobiele apparaten bij de Rijksoverheid te zetten. De eerste stap is het per direct aan ambtenaren in dienst van de Rijksoverheid ontraden om apps geïnstalleerd te hebben en te gebruiken op hun mobiele werkapparatuur van bedrijven uit landen met een offensief cyberprogramma tegen Nederland en/of Nederlandse belangen. Om ambtenaren in dienst van de rijksoverheid hierover goed te informeren zal op korte termijn communicatie worden ontwikkeld.

Tegelijk zal op korte termijn worden toegewerkt naar een situatie 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. Het worden dan in zijn geheel zogeheten '*managed apparaten*', waarvoor is bepaald welke apps daarop kunnen worden geïnstalleerd en gebruikt door de gebruiker. Apps van bedrijven uit landen met een offensief cyberprogramma tegen Nederland en/of Nederlandse belangen zullen dan niet toegestaan worden. Ik wil dit beleid zo snel als mogelijk ingericht hebben, in samenwerking met de *'shared service organisaties'* (SSO's) die deze mobiele apparaten beheren. Daarbij bezie ik ook het *bring your own device* beleid dat door onderdelen van de rijksoverheid wordt gehanteerd.
Uitzondering op de bovenstaande maatregelen geldt wanneer een dergelijke applicatie nodig is of kan zijn voor het uitoefenen van een primaire taak van een

rijksorganisatie. Hierbij kan worden gedacht aan inspectie en toezicht, opsporingsonderzoek of inlichtingenbelang. Deze uitzondering zal in samenwerking met de departementen de komende periode verder worden uitgewerkt.

Appgebruik in de samenleving
Deze brief heeft zich tot nu gericht op risico's voor de rijksoverheid. Apps worden ook door andere overheden en vooral ook door burgers, waaronder kinderen, gebruikt. Het is belangrijk om het bewustzijn over gegevensverwerking door dit soort apps te verhogen. Daarom gaat het kabinet hier de komende periode op inzetten. Voor de zomer komen wij hier bij uw Kamer op terug.

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties
Digitalisering en Koninkrijksrelaties

Alexandra C. van Huffelen

Vraag 1
Deelt u de mening dat het onduidelijk is in hoeverre de gegevensbescherming van TikTok voldoet en dat de Chinese applicatie daarmee een potentieel hoog veiligheidsrisico heeft?

In de begeleidende brief bij deze antwoorden, ben ik nader ingegaan op risico's voor de Rijksoverheid, en de stappen die ik in reactie daarop ga nemen.

Als het gaat om het voldoen van TikTok aan de geldende regels, doet op dit moment de Ierse privacytoezichthouder (de zogenaamde *Data Protection Commission*), als leidende EU-privacytoezichthouder, onderzoek naar de wijze waarop TikTok persoonsgegevens verwerkt. Het onderzoek van de Ierse toezichthouder richt zich onder andere op rechtmatigheid van de overdracht door TikTok van persoonsgegevens naar derde landen waaronder China en de naleving van de vereisten van de Algemene verordening gegevensbescherming (AVG) voor deze overdrachten.

De minister voor Rechtsbescherming heeft de Autoriteit Persoonsgegevens (AP) gevraagd om bij haar Ierse collega te vragen naar de stand van zaken van dit onderzoek. Uit deze navraag blijkt dat de onderzoeksresultaten in de eerste helft van 2023 worden verwacht. Uit dit onderzoek zal blijken in hoeverre de gegevensbescherming van TikTok voldoet aan de geldende wet- en regelgeving.

Vraag 2
Hoe kijkt u naar de ontwikkeling in de Verenigde Staten waar het besloten is om publieke vertegenwoordigers te verbieden TikTok op hun mobiele werkdevice te hebben en zou u dit ook aan Nederlandse volksvertegenwoordigers adviseren? [1]

Zoals aangegeven in de begeleidende brief, is in het traject de afgelopen weken nauw contact geweest met Europese partners, en hun beleid rondom mobiele apparaten bij de overheid en TikTok. Deze contacten hebben daarmee bijgedragen aan de in de brief genoemde besluiten.

De risico's die naar voren zijn gekomen, gelden niet alleen voor de rijksoverheid, maar kunnen ook breder gelden. Ik adviseer het Nederlandse parlement dan ook om kennis te nemen van de brief, en met inachtneming van zijn eigen onafhankelijke positie, te besluiten over eventuele extra veiligheidsmaatregelen.

Vraag 3
Bent u bereid medewerkers van de Rijksoverheid en andere overheidsambtenaren te verbieden de applicatie TikTok op hun mobiele werkdevice te hebben, om op die manier potentiële risico's te verkleinen?

Voor het antwoord op deze vraag verwijs ik naar het beleid zoals geformuleerd in de begeleidende brief bij deze antwoorden.