Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties
Mw. drs. A.C. van Huffelen,
Staatssecretaris
Postbus 20011
2500 EA 'S-GRAVENHAGE

Datum
17 mei 2023
Kenmerk
TPW/U202300365
Telefoon
070 373 8393
Bijlage(n)
1

Onderwerp
Het ontraden van appgebruik uit landen met een offensief cyberprogramma voor ambtenaren

Geachte mevrouw Van Huffelen,

Uw brief d.d. 6 april jongstleden ter zake het gebruik van apps uit landen met een offensief cyberprogramma is in goede orde ontvangen.

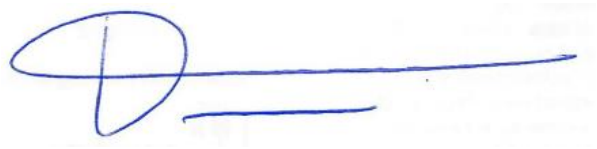
Gemeenten en gemeenschappelijke regelingen bepalen zelf het beleid over de omgang met werkapparaten en het gebruik van social media. Daarbij vindt een afweging plaats tussen het belang met inwoners te communiceren via de kanalen die zij gebruiken en het belang van informatieveiligheid. Verschillende apps uit landen met een offensief cyberprogramma zijn populair, met name onder de jeugd. Het advies van de AIVD is echter zwaarwegend. Wij hebben onze leden in een handreiking geadviseerd uw lijn te volgen en het gebruik van apps uit dergelijke landen op werkapparaten voor medewerkers te ontraden. Deze handreiking treft u hierbij aan. Daarbij zien we de suggestie van de AIVD om een risicoanalyse uit te voeren als een valide alternatief. De risico's die door medewerkers van gemeenten met uiteenlopende verantwoordelijkheden worden gelopen, zijn immers van verschillende grootte.

U geeft in uw brief aan op de korte termijn tot managed werkapparaten te willen komen. Wij vinden dit een belangrijke ontwikkeling, mede in verband met vraagstukken over archivering. We zien ook een relatie met het voorstel van de regeringscommissaris voor de informatiehuishouding om te komen tot moderne werkplekken. Aangezien er geen gemeenschappelijk beleid is in het lokaal domein over werkapparaten kan dat voorbeeld niet door alle gemeenten direct en gelijktijdig worden gevolgd. Onze leden kunnen daarvoor opteren.

Vereniging van Nederlandse Gemeenten
Nassaulaan 12 Den Haag | Postbus 30435 | 2500 GK Den Haag
070 - 373 83 93 | info@vng.nl

Wij wisselen gaarne met u van gedachten over de problematiek en wachten uw uitnodiging daartoe af.

Met vriendelijke groet,
Vereniging van Nederlandse Gemeenten



mr L.K. Geluk
Algemeen directeur

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 apps (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’.