NSM

Vår saksbehandler
Torgeir Pande Braathen

Vår dato
20.03.2023

Vår referanse
B-23/00356-2

Deres dato

Deres referanse
3/1268 - ROB

Antall vedlegg

Til
Justis- og beredskapsdepartementet
Postboks 8005 Dep
0030 OSLO
Annette Tjaberg

Vurdering av særskilte råd, retningslinjer og informasjonstiltak

Vi viser til brev fra Justis- og beredskapsdepartementet datert 3. mars 2023 og vil med dette fremme anbefalinger og titak knyttet til TikTok og Telegram.

NSM vurderer at det medfører høy risiko dersom applikasjonene TikTok og Telegram installeres på tjenesteenheter som

a) har tilgang til virksomhetens interne digitale infrastruktur eller tjenester, eller
b) som brukes til kommunikasjon eller behandling av slik virksomhetsrelatert informasjon som er unntatt offentlighet eller underlagt taushetsplikt
c) enheter og programvare som benyttes til tale som er gradert BEGRENSET iht. sikkerhetsloven

NSM vurderer at TikTok eller Telegram ikke bør installeres på tjenesteenheter. Dersom det er tjenstlig behov for TikTok eller Telegram, anbefaler NSM at applikasjonen installeres og benyttes på en separat enhet forbeholdt denne typen formål og at denne enheten ikke får tilgang til virksomhetens interne digitale infrastruktur eller tjenester.

Applikasjonene TikTok eller Telegram bør heller ikke installeres på private enheter som får tilgang til virksomhetens interne digitale infrastruktur eller tjenester.

Tiltakene omtalt her bør rettes mot ansatte i offentlig sektor. I tillegg bør tiltakene rettes mot ansatte i de virksomheter i privat sektor som ifølge sikkerhetsloven § 1-3 første ledd helt eller delvis er underlagt sikkerhetsloven. Det kan være hensiktsmessig å prioritere iverksetting av tiltak rettet mot statsansatte.

Anbefalingene vil også kunne rettes mot personer med beskyttelsesbehov, for eksempel personer med adressesperre kode 6 eller kode 7.

TikTok, Telegram og andre applikasjoner kan brukes på mobiltelefoner, nettbrett og personlige datamaskiner. I anbefalingene bruker vi derfor begrepet «tjenesteenheter» i stedet for kun tjenestetelefoner ettersom dette begrepet dekker flere typer enheter.

Vi legger til grunn at tjenesteenheter er utstyr og abonnementer som er betalt av arbeidsgiver for å dekke tjenstlig behov. Mobiltelefoner som arbeidsgiver låner ut til ansatte på tjenestereise til høyrisikoland er også tjenesteenheter. Vi vil understreke at tjenstlig behov kan omfatte bruk av de nevnte applikasjoner. Det er derfor nødvendig å utforme tiltak som skiller mellom forskjellige typer tjenesteenheter.

Generelle anbefalinger og tiltak for sikkerhet på private- og tjenesteenheter

NSMs hovedbekymring er ikke nødvendigvis én enkelt applikasjon, men summen av ulike applikasjoner som samlet sett kan utgjøre en risiko via mobile enheter. Vi vil derfor også fremme noen generelle forhåndsregler som gjør seg gjeldende uavhengig av hvilken applikasjon det er snakk om.

På generelt grunnlag anbefaler NSM å separere jobb- og privatliv på enheter. Skulle det foreligge tjenstlige behov for å bruke sosiale medier og meldingstjenester, bør dette foregå på en adskilt enhet. Det er virksomhetens ansvar å foreta en risikovurdering basert på de verdiene man forvalter i form av sensitive data, og dermed også å foreta de nødvendige tiltakene som anskaffelse av separate enheter.

På tjenesteenheter bør det utvises forsiktighet og tilbakeholdenhet ved installasjon av applikasjoner og bruk av sosiale medier og meldingstjenester. Virksomheter har ansvaret for å gi ansatte tilstrekkelig og tydelig veiledning og instruks når det gjelder både installasjon og bruk av tjenesteenheter. Hver ekstra applikasjon som installeres på enheten kan potensielt redusere sikkerheten på enheten, få tilgang til data, forårsake datalekkasjer mot internett, svekke personvernet til brukeren og øke faren for misbruk av enhetens mikrofon og kamera til avlytting og «avtitting» av brukerens omgivelser. Sluttbrukere bør derfor kun installere applikasjoner som er strengt nødvendige og da applikasjoner fra kjente og tiltrodde kilder.

NSM understreker også at NSMs 13 råd om sikkerhet på mobile enheter som et minimum er et godt utgangspunkt for å redusere risikoen for å bli utsatt for sikkerhetstruende virksomhet gjennom mobile enheter. Disse anbefalingene er like gjeldende for både private- og tjenesteenheter. Men merk at de 13 rådene skal revideres for å tydeliggjøre at for tjenesteenheter så er det først og fremst virksomhetens risikovurdering, veiledning og instruks som skal følges.

NSM har også utviklet en veileder (C-04) som beskriver et teknisk sikkerhetskonsept for oppsett av mobile klienter (iOS-enheter) og inkluderer vedlegg som omhandler brukertiltak og vurdering av applikasjoner. Denne kan deles på forespørsel.

Bakgrunnsinformasjon

Vi viser til Etterretningstjenestens trusselvurdering i Fokus 2023 som fremhever at Russland og Kina er de fremste trusselaktørene mot norske sikkerhetsinteresser. Vi har derfor i denne besvarelsen avgrenset oss til å vurdere applikasjonene TikTok og Telegram som har tilknytning til disse landene. Dette betyr ikke at andre applikasjoner ikke kan utgjøre en tilsvarende risiko.

Blant annet vet vi at kinesiske myndigheter har ifølge deres etterretningslov utstrakt anledning til å pålegge kinesiske virksomheter og enkeltpersoner å samarbeide med og utlevere informasjon til kinesisk etterretning. NSM legger til grunn at en stor del av kinesiskprodusert teknologi vil kunne benyttes som en plattform for innhenting av ulovlig etterretning til fordel for Kina.[1]

[1] Nasjonal sikkerhetsmyndighet - Risiko 2022

I tråd med blant annet Center for Cybersikkerhed i Danmark, EU-kommisjonen, Rådet for Den europeiske union og amerikanske myndigheter ("No TikTok on Government Devices Act") deler NSM deres bekymring vedrørende TikToks utstrakte og inngripende innhenting av data. NSMs egne tekniske undersøkelser understøtter observasjoner fra relevante tredjeparter.

Det tas forbehold om at Telegram ikke er analysert av NSM og vi har ingen solide kilder, analyser eller observasjoner som særskilt utpeker Telegram som meldingstjeneste i negativ retning ut ifra et teknisk perspektiv. Vurderingene er i hovedsak støttet på informasjon fra tredjeparts åpne kilder. Likevel er det viktig å påpeke at applikasjonen ikke bruker ende-til-ende-kryptering som standard, og den bør dermed betraktes som en hvilken som helst meldingstjeneste. Brukere bes på generelt grunnlag om å utvise forsiktighet og tilbakeholdenhet rundt alle meldingstjenester og applikasjoner. Sikkerhetsbrudd kan forekomme for alle applikasjoner.

Med hilsen

Sofie Nystrøm
direktør

Dette dokumentet er elektronisk godkjent hos Nasjonal sikkerhetsmyndighet og sendes uten signatur.