NSM

2024

Temarapport

Mobilapplikasjoner på tjenesteenheter

Mobilapplikasjoner og beste praksis

I 2023 ble 257 milliarder applikasjoner lastet ned globalt. [1] Alle applikasjoner som lastes ned på mobil eller nettbrett, kan bringe med seg et bredt utvalg sikkerhetsutfordringer for enhetene.

Mobiltelefoner er allemannseie. Det handler ikke lenger om hvorvidt vi har mobil, men i hvilken alder vi får det. Stadig flere bruker jobbtelefon, og slik blir skillet mellom privatliv og arbeidsliv stadig mindre.

Arbeidshverdagen foregår heller ikke lenger bare på kontoret. Når ansatte beveger seg ut av virksomhetens fysiske miljø, må virksomhetens verdier beskyttes med nye metoder. Sikring av mobile enheter er komplekst og utfordrende fordi det er et felt som stadig er i endring.

Det er en økende trend at applikasjoner fører til sikkerhetshendelser på tjenesteenheter. Dette er utstyr og abonnementer som er betalt av arbeidsgiver for å dekke tjenstlig behov. Angrep mot virksomheters mobile enheter rammer både systemer, personvern og kundedata. [2]

Tjenesteenheter er en integrert del av organisasjonens digitale infrastruktur med samme behov for sikring som eksempelvis stasjonære eller bærbare datamaskiner. NSM anbefaler sterkt at norske virksomheter ikke overlater til den enkelte ansatte å vurdere hvilke applikasjoner som kan lastes ned på tjenesteenheter. NSM har derfor samlet en rekke råd og anbefalinger knyttet til mobilapplikasjoner for norske virksomheter å benytte i sikkerhetsarbeidet for tjenesteenheter.

Denne rapporten deler beste praksis for applikasjoner og utfyller NSMs 13 råd for bedre sikkerhet på mobile enheter. [3] I rapporten kommer NSM med forslag til hvordan norske virksomheter, private og offentlige, kan forbedre sikkerheten på tjenesteenheter ved å tilpasse tiltak til ulike brukergrupper og situasjoner. NSM deler anbefalinger inn i ulike kategorier fra generelle retningslinjer for alle ansatte med tjenestetelefon, ansatte som bør ta ekstra forholdsregler, og anbefalinger for særskilte situasjoner hvor det er høy risiko for at tjenesteenheten kan bli utsatt for ondsinnet aktivitet fra trusselaktører. Videre forklarer rapporten hva virksomheter bør være oppmerksomme på når de vurderer ulike applikasjoner og funksjonalitet, og ikke minst hvorfor.

Generelt bør alle ha et bevisst forhold til applikasjonene som til enhver tid er tilgjengelig på telefonen, enten det er en tjenesteenhet eller privat. Et generelt råd til alle med smarttelefon og nettbrett er å være kritiske til hvilke tillatelser og informasjon de gir den enkelte applikasjon. Gi kun midlertidige tillatelser der dette er mulig.

Anbefalingene i rapporten gjelder ikke tjenesteenheter som kan motta gradert informasjon. For skjermingsverdige og sikkerhetsgraderte informasjonssystemer etter sikkerhetsloven gjelder egne krav som ikke omfattes eller påvirkes av denne anbefalingen.

Anbefalinger og råd for virksomheter

En mobil enhet som blir brukt i jobbsammenheng er en integrert del av organisasjonens digitale infrastruktur med det samme behovet for sikring. NSM anbefaler at vurderinger rundt tjenesteenheter og applikasjoner er en del av organisasjonens IKT-sikkerhetspolicy.

Virksomheter bør sentralt administrere og sikre mobile enheter. NSM anbefaler flåtestyring på mobile enheter for virksomheter.

Flåtestyring, også kjent som *Mobile Device Management* (MDM), er et verktøy for å kunne administrere mobile enheter fra sentralt hold. Verktøyet gjør det mulig å håndheve retningslinjer der det som et minimum er begrensninger på hvilke applikasjoner som kan installeres, og fjernsletting om enheter blir mistet eller stjålet. I tillegg er det mulighet til å sentralisere logging, påkreve *Virtual Private Network* (VPN) og generelt låse ned enheten av sikkerhetshensyn.

Alle virksomheter, uavhengig av om de har flåtestyring eller ikke, anbefales sterkt å gjøre en overordnet risikovurdering. Denne bør være førende for hvordan virksomheten både bruker mobile enheter og beskytter egne digitale verdier. Virksomhetene må kartlegge hvilken og hvordan sensitiv informasjonen forvaltes, enten det er på egne eller tredjeparts vegne. Det er virksomhetens ansvar å ha kjennskap til trusselbildet mot egen organisasjon og hva som er akseptabel risiko.

NSM har utformet et sett med anbefalinger og råd spesifikt rettet mot applikasjoner og mobile enheter for å hjelpe virksomheter med mulige praktiske tiltak som kan avbøte eventuelle risikoer avdekket i virksomhetenes kartlegging.

Det er viktig å merke seg at anbefalingene ikke er uttømmende, og at hver virksomhet må gjøre egne tilpasninger. Anbefalingene i tabellene på de neste sidene er kategorisert på tre nivåer: Det er anbefalinger som kan gjelde alle ansatte med tjenesteenhet, for ansatte som bør ta ekstra forholdsregler og for særskilte situasjoner. Det er virksomhetene selv som vurderer hvilken kategori deres ansatte passer inn i og hvilke tiltak som passer ved særskilte tilfeller. Ikke alle tiltak er nødvendigvis permanente, men knytter seg til eksempelvis rolle, oppgaver, tilganger eller reisevirksomhet.

Tjenesteenheter er mobile enheter som mobiltelefoner, nettbrett eller datamaskiner som er betalt av arbeidsgiver og tilknyttet virksomhetens interne digitale infrastruktur.

Anbefalte retningslinjer ved lav risiko

Retningslinjene er generelle og bør gjelde alle ansatte i virksomheten med tjenesteenheter.

Anbefalinger	**Kommentar**
Vær kritisk til hvilke applikasjoner som lastes ned og installeres, hvilke tillatelser hver enkelt applikasjon gis og hvilken informasjon applikasjonen får tilgang til. **Vær særlig oppmerksom på tillatelser til bruk av kamera og mikrofon.**	Enheter leveres ofte med mange forhåndsinstallerte applikasjoner. Avinstaller unødvendige applikasjoner, eller deaktiver dem hvis avinstallering ikke er mulig.
Bruk stedstjenester kun når høyst nødvendig.	Stedstjenester kan brukes til å overvåke geografiske bevegelser. Vær selektiv i bruken av tjenestene, og vurder bruksområdet.
Vær kritisk til bruk av *Near-Field Communication* (NFC), Bluetooth og wifi.	Trådløse teknologier deler ofte mye informasjon og vil kunne avsløre både posisjon og i enkelte tilfeller unik id for enheten selv når den er avslått. Vurder derfor å slå av tjenestene når de ikke er i bruk. Husk å skru av Bluetooth i *Innstillinger,* ikke kun i *Kontrollsenter.* Vær klar over at Bluetooth automatisk blir aktivert etter omstart.
Vurder å benytte løsninger for kryptert kommunikasjon.	All sensitiv informasjon bør kommuniseres via løsninger for kryptert kommunikasjon for å beskytte mot dataavlytting.

Anbefalte retningslinjer ved middels risiko

Retningslinjene er for ansatte som bør ta ekstra forholdsregler. Virksomheter kan eksempelvis vurdere i hvilken grad de ansatte har sensitiv informasjon lagret på enheten, og hva konsekvensen er om informasjonen skulle komme på avveie.

Anbefalinger	**Kommentar**
Vurder nødvendigheten av hver applikasjon. Gi kun absolutt nødvendige tillatelser til nødvendige applikasjoner. Bruk fiktive opplysninger der det er mulig. **Vær særlig oppmerksom på tillatelser til bruk av kamera og mikrofon.**	Tiltakene vil redusere sårbarheten overfor en eventuell trusselaktør, samt redusere risiko for at sensitive data utilsiktet kommer på avveie.
Bruk stedstjenester kun når høyst nødvendig.	Stedstjenester kan brukes til å overvåke geografiske bevegelser. Vær selektiv i bruken av tjenestene og vurder bruksområdet.
Omstart enheten ved jevne mellomrom.	Å slå enheten helt av før du starter den igjen gjør det vanskeligere for eventuell spionvare å forbli på enheten.
Sikker sletting av hele enheten etter bruk.	En ufullstendig slettet enhet er en risiko. Med «etter bruk» menes ved for eksempel eierskifte eller anskaffelse av ny enhet.
Vær kritisk til bruk av *Near-Field Communication* (NFC), Bluetooth og wifi. Benyttes kun når det er absolutt nødvendig.	Trådløse teknologier deler ofte mye informasjon og vil kunne avsløre både posisjon og i enkelte tilfeller unik id for enheten selv når den er avslått. Slå derfor av funksjonene når de ikke er i bruk. Husk å skru av Bluetooth i *Innstillinger,* ikke kun i *Kontrollsenter.* Vær klar over at Bluetooth automatisk blir aktivert etter omstart.
Bruk ende-til-ende-kryptert kommunikasjon (E2E).	All sensitiv informasjon bør kommuniseres via E2E for å beskytte mot dataavlytting.

Anbefalte retningslinjer ved høy risiko

Retningslinjer for særskilte situasjoner hvor det er høy risiko for at tjenesteenheten kan bli utsatt for ondsinnet aktivitet fra trusselaktører – og sannsynligheten for en uønsket hendelse er stor. Dette gjelder for nøkkelpersonell og ledelse, i tilfeller hvor mye eller høy grad av sensitiv informasjon er lagret på enheten, og ved reiser til land som utgjør en risiko eller tilsvarende.

Anbefalinger	**Kommentar**
Ikke installer applikasjoner på tjenesteenheter.	Hvis man må installere applikasjoner, bør de være begrenset til dem som er forhåndsgodkjente av virksomheten. Godkjente applikasjoner bør låses ned til et minimum av tillatelser via flåtestyring (*Mobile Device Management*).
Bruk *burner phone* (telefon til engangsbruk) til usikre applikasjoner.	Ta også forholdsregler for å sikre en *burner phone* fysisk.
Ikke aktiver stedtjenester.	Stedstjenester kan brukes til å overvåke geografiske bevegelser.
Omstart enheten en gang i døgnet.	Å slå enheten helt av før du starter den igjen gjør det vanskeligere for eventuell spionvare å forbli på enheten.
Sikker sletting av hele enheten etter bruk.	En ufullstendig slettet enhet er en risiko. Med «etter bruk» menes ved for eksempel eierskifte eller anskaffelse av ny enhet.
Vær svært restriktiv ved bruk av *Near-Field Communication* (NFC), Bluetooth og wifi. Unngå funksjonene så langt det lar seg gjøre.	Trådløse teknologier deler ofte mye informasjon og vil kunne avsløre både posisjon og i enkelte tilfeller unik id for enheten selv når den er avslått. Funksjonene skal være avslått når ikke i bruk. Husk å skru av Bluetooth i *Innstillinger,* ikke kun i *Kontrollsenter.* Vær klar over at Bluetooth automatisk blir aktivert etter omstart.
Bruk kun ende-til-ende-kryptert kommunikasjon (E2E).	All sensitiv informasjon bør kommuniseres via E2E for å beskytte mot dataavlytting.
Vurder å aktivere restriktive innstillinger som telefonen har mulighet til, som eksempelvis *lockdown*-modus på iOS.	*Lockdown*-modus reduserer klart risikoen for å bli infisert av sofistikert spionvare, men på bekostning av svært redusert funksjonalitet.

Fra retningslinjer til tiltak

NSMs inndeling i tre ulike kategorier sørger for en god balanse mellom funksjonalitet, risiko og sikkerhet. Virksomhetens egne risikovurdering må ligge til grunn for bruk av anbefalinger og iverksetting av tiltak. Det er virksomhetene som må sørge for at virksomhetens retningslinjer er tilstrekkelige og blir fulgt.

Et tiltak kan være å veilede ansatte i bevisst mobilbruk og gi innføring i virksomhetens retningslinjer for sikrere bruk av mobile enheter. Et godt råd kan være at ansatte sjekker innstillingene på applikasjonen de laster ned. Kontrollspørsmål kan være om den enkelte applikasjonen trenger tilgang til eksempelvis kamera, lyd, kontaktliste eller stedstjenester for å fungere? Kan nødvendige tillatelser begrenses til kun når applikasjonen er i bruk? Kontaktinformasjon som telefonnummer, bilder, meldinger og e-post er eksempler på informasjon som kan være sensitiv.

Det er en klar anbefaling at applikasjoner burde få midlertidige tillatelser der det lar seg gjøre, eksempelvis at navigasjonsapplikasjoner kun har tilgang til stedstjenester når applikasjonen er i bruk. Tilsvarende bør Bluetooth være avskrudd når den ikke er i bruk. Bluetooth er nødvendig for å kunne bruke trådløs telefon i bil, smartklokke eller trådløse øretelefoner. Dersom Bluetooth alltid er påskrudd, kan den medføre en sporingsrisiko fordi den til enhver vil tid annonsere sin tilstedeværelse. Den vil kunne koble seg opp til ukjente enheter og dele informasjon utilsiktet. Det er i mange tilfeller også mulig å bytte ut trådløse teknologier med andre alternativ, som hodetelefoner med kabel.

Ved installasjon av applikasjoner kan det i flere tilfeller være nyttig å benytte seg av fiktive opplysninger for å minimere hvor mye informasjon som deles. Det er tenkelig at en applikasjon laget for ett formål som en årlig konferanse, har noe lavere standard hva gjelder sikkerhetsløsninger. I slike situasjoner hvor sikkerhetsløsningen og kanskje utvikler er ukjent, kan det være fordelaktig med fiktive opplysninger. De ansatte kan for eksempel opprette en anonym e-postadresse som ikke er direkte knyttet opp til den ansatte selv eller virksomheten. Det kan også være mulig å kun oppgi forbokstav i navnet sitt, i stedet for fullt fornavn og etternavn.

Informasjon er en handelsvare

Informasjon er en handelsvare for alle fra kommersielle aktører til kriminelle. Data videreselges, lekkes og brukes til identitetstyveri, utpressing eller til etterretningsformål av statlige aktører.

Ulike aktører samler systematisk informasjon om flere ulike forhold, eksempelvis knyttet til politiske prosesser, industri, finans, forsvar og forskning. Trusselaktører opererer både opportunistisk og målrettet, ofte i en kombinasjon av begge fremgangsmåter. Et svakt passord hos en bruker langt nede i et system kan være et første skritt på veien til et bestemt mål med langt høyere verdi. Derfor må virksomheter ha en helhetlig tilnæring til sikkerhet, inkludert installering og bruk av applikasjoner på tjenesteenheter.

Trusselaktører er ofte spesielt interessert i personer med tilgang til informasjon eller i en autoritetsposisjon som kan utnyttes. Det kan være en IT-administrator med tilgang til hele organisasjonens systemer, eller ledere oppover i virksomheten. Kompromittering av disse brukerne gir trusselaktør mulighet til å utnytte brukerens rettigheter til å utføre handlinger i systemene. *Spearphishing* er et kjent eksempel, hvor aktører bruker *phishing* mot enkeltindivider høyere opp i organisasjoner eller bedrifter. Aktør kan da overvåke korrespondanse over tid for å innhente informasjon om virksomheten for å bruke i et annet angrep.

Desto mer sensitiv informasjon brukeren har tilgang til, desto større er risikoen hvis denne faller i feil hender. I flere bransjer er det nødvendig å skille mellom private enheter og tjenesteenheter, fordi konsekvensene av en lekkasje av høysensitiv informasjon kan være svært kritisk. Trusselaktører interesserer seg for norske teknologibedrifter, forsknings- og utviklingsmiljøer og offentlige forvaltningsorganer. [4] I tillegg er energi- og våpenindustrien, menneskerettighetsorganisasjoner, journalister og politikere av særskilt interesse for enkelte trusselaktører, ifølge ENISA. [5]

NSM har de siste årene observert en økning i ondsinnet aktivitet mot norske virksomheter. De er mål for både statssponsede aktører og opportunistiske vinningskriminelle. [4] Det er nødvendig med en mer trusselbasert «føre var»-tilnærming for å hindre at uønskede aktører får fotfeste i Norge. Tar vi ikke inn over oss de økte verdiene og komplekse sårbarhetene i cyberdomenet, øker risikoen for at land som Kina, Russland og andre trusselaktører skaffer seg tilganger til systemer tilknyttet grunnleggende nasjonale funksjoner uten at samfunnet er klar over det. [6]

Russlands invasjon av Ukraina i februar 2022 førte til et sikkerhetspolitisk paradigmeskifte. Det har ført til en økt bevissthet rundt digitale leverandørkjeder. Trusselaktører velger ofte minste motstands vei, og digitale leverandørkjeder er ofte det svakeste punktet i en kjede av både verdier og leverandører. [4] I NSMs sikkerhetsfaglige råd fra 2023 påpekes det at data i økende grad blir behandlet på mobile enheter. Dette kan være sensitiv og kritisk informasjon og informasjonssystemer som ikke er tilstrekkelig beskyttet. [6]

Dette gjelder ikke bare i Norge. Det er derfor viktig å gjøre gode sikkerhetsmessige vurderinger også for reiser, spesielt til utsatte områder. Det gjelder både sikring av sensitiv informasjon og fysisk sikring av ansatte på reise, fordi det kan ha forsterkende konsekvenser for hverandre.

Er virksomheten og de ansatte i risikogruppen?

«Ingen er vel interessert i akkurat meg? Jeg har ingenting av verdi.»

Det er ikke alltid lett for den enkelte ansatte å se hvilke verdier hen besitter. Men nettopp fordi informasjon er handelsvare og trusselaktørene opererer langs flere flater, er det nødvendig for virksomheter å ha en helhetlig IKT-sikkerhetspolicy som inkluderer applikasjoner på tjenesteenheter.

På en mobil enhet er det en mengde informasjon med ulike grader av sensitivitet. Det kan være både lagret informasjon, og informasjon som passerer enheten den ene eller andre veien. Informasjon som isolert sett kan synes å være uvesentlig, kan ha stor verdi for en trusselaktør. Tilgang til en e-postadresse kan være nok til at en angriper kan utlede mye informasjon. Når denne sammenstilles med annen informasjon fra åpne kilder, sitter trusselaktører med informasjon som samlet sett kan være sensitiv. Applikasjoner ønsker ofte å innhente en mengde data for å skreddersy innhold til hver enkelt bruker. Dette sammenfaller ofte med interessene til en eventuell trusselaktør.

Som i de fleste andre tilfeller av risikovurdering er det viktig at virksomheter vet hva som skal beskyttes. Og ikke minst; hva vil være ytterste konsekvens hvis denne informasjonen kommer på avveie? Det er et annet risikobilde for representanter for organisasjoner, bedrifter eller i offentlige verv enn for privatpersoner.

Kontrollspørsmål i virksomheten kan være:

- Hva slags informasjon trenger beskyttelse?
- Hvor mye informasjon er nødvendig å ha på en tjenesteenhet for at den ansatte skal kunne utføre arbeidet sitt?
- Hva er ytterste konsekvens av at informasjonen kommer på avveie?

Vurdering av mobilapplikasjoner

Applikasjoner er på sett og vis ferskvare. Det gjør det vanskelig for NSM å vurdere eller godkjenne hver enkelt applikasjon som dukker opp i markedet og som kan være nyttig for norske virksomheter. Derfor finner NSM det mest hensiktsmessig å dele generelle råd. Hovedbekymringen er ikke nødvendigvis én applikasjon, men summen av ulike applikasjoner som samlet sett kan utgjøre en risiko via mobile enheter. Noen applikasjoner ber om unødvendig mye informasjon. Dårlige sikkerhetsløsninger eller uforholdsmessige krav til informasjonsdeling er en utfordring fordi det kan utnyttes av trusselaktører.

Applikasjoner kan misbrukes

Til klimatoppmøtet COP27 i Egypt i desember 2022 ble det laget en egen applikasjon for møtedeltakere. Klimatoppmøtet samlet nærmere 35.000 mennesker fra nær alle land i verden, deriblant en rekke statsledere og ministre. NSM analyserte COP27-applikasjonen på bakgrunn av bekymring for personvern, men også potensiell overvåkning. Denne bekymringen ble delt av flere, inkludert Amnesty International og Human Rights Watch. Applikasjonen var i utgangspunktet obligatorisk for alle deltakerne på konferansen.

De tekniske funnene til NSM ga indikatorer på at applikasjonen inneholdt funksjonalitet som *potensielt* kunne utnyttes til overvåkning av brukerne. Det mest urovekkende funnet var applikasjonens utvidede tillatelser til kamera og mikrofon og funksjonalitet til å spore brukere både innen- og utendørs. For en potensiell trusselaktør vil dette, koblet sammen med eksempelvis passinformasjon og personalia, utgjøre svært verdifull informasjon. NSM formidlet dette til sikkerhetsansvarlige for den norske delegasjonen slik at de kunne gjøre hensiktsmessige sikkerhetsvurderinger på vegne av de norske delegatene. [7]

Skadevare eller spionvare?

Det finnes en rekke programvarer som er laget for å overvåke, spore og lagre brukers aktivitet i omfattende grad. Det spenner fra applikasjoner hvor foreldre følger med på egne barns bevegelser med beskyttelse som formål til det som er rendyrket «ondsinnet» overvåkning. I stor grad er det hensikt og tillit som avgjør hvordan disse kan skilles fra hverandre. En applikasjon som er laget for å beskytte, kan også brukes til illegitime formål. Applikasjoner kan potensielt bli brukt som et første ledd i en operasjon hvor personer av interesse blir kartlagt, for deretter å bli gjenstand for målrettet infeksjon av avansert spionvare.

Skadevare har mange kallenavn blant annet virus, trojaner og spionvare. Det er en samlebetegnelse «[...] på programkode som uten brukerens tillatelse utfører handlinger med brukerens systemer eller informasjon». [21]

Spionvare er i denne rapporten definert som programvare brukt til å samle inn forskjellige typer informasjon om en bruker på en måte som er mot målets viten og vilje, og som sannsynlig bryter brukers rett til personvern.

Pegasus er en svært avansert spionvare og er nok den mest kjente og omtalte spionvaren rettet mot mobile enheter. Pegasus har mulighet til å infisere enheter uten at målet gjør noe aktivt og uten at bruker vil merke at det skjer. Spionvaren selges som en komplett løsning som mobilapplikasjon og bakenforliggende infrastruktur.

NSO Group har utviklet systemet og selger det angivelig kun til nasjonalstater. Spionvaren har blitt rapportert brukt til å overvåke blant andre statsoverhoder, næringslivsledere, politikere, ikke-statlige organisasjoner, regimedissidenter, journalister, studenter, og andre politisk engasjerte personer. [8] Det har ført til økt oppmerksomhet for NSO Group i vestlige medier.

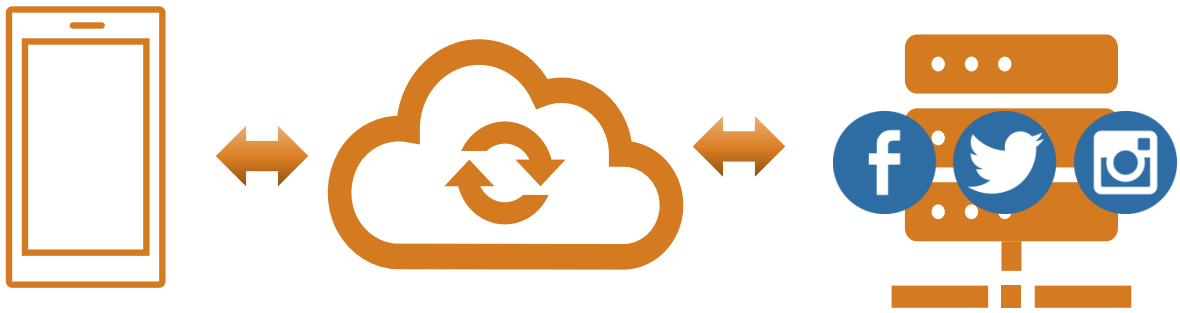
I januar 2022 gikk det finske utenriksdepartementet ut med at de var blitt utsatt for målrettet spionasje via Pegasus og i april samme år ble det rapportert funn ved den britiske statsministerens kontor. [9]

Det som skiller NSO Group fra andre aktører innen kommersiell spionvare, er den sofistikerte utnyttelsen av underliggende sårbarheter i operativsystem eller populære applikasjoner. Applikasjoner som WhatsApp, iMessage og WebKit/Safari har blitt utnyttet med Pegasus. [10] [11] De relativt mange sikkerhetsoppdateringene som har blitt sluppet for Apple-produkter i de siste årene er en indikasjon på sårbarheter og utnyttelse av disse.

Apple har på iOS introdusert *lockdown*-modus som et mottiltak overfor sofistikerte cyberangrep som Pegasus. [12]

Et digitalt økosystem

Når en applikasjon installeres på en mobil enhet, er det et samspill mellom enheten og applikasjonen, nettverket det kobler til og måten data blir lagret, behandlet og videreformidlet på. Hvordan data blir sikret i hele denne kjeden har betydning for hvilken risiko dataforflytting utgjør.



De fleste mobilapplikasjoner er tilknyttet en webtjeneste for lagring og prosessering av data. Illustrasjon: NSM

Hvor sikker er bruk av mobilen?

Mobilen eller nettbrettet kan være sårbar i flere lag. Enheten kan bli fysisk overtatt, inneha sårbarheter i maskinvare eller operativsystem, eller ha fått installert sårbare applikasjoner. En eller flere av disse faktorene kan gjensidig bidra til at data kommer på avveie.

Hvorfor bør man oppdatere operativsystemet?

Sikkerheten for mobile enheter har blitt betraktelig bedret de siste årene. [13] [14] Ny teknologi og bedre sikkerhet har blitt tatt i bruk både i operativsystemer og maskinvare. Det er derfor avgjørende å bruke enheter som fremdeles mottar sikkerhetsoppdateringer for å minimere risikoen for utnyttelse av sårbarheter. Selv om enheten mottar sikkerhetsoppdateringer i programvare, kan den fremdeles være sårbar på grunn av mangler eller sårbarheter i fysisk maskinvare. [15] Dette gjelder for både Apple-produkter som iPhone, iPad og de ulike enhetene som kjører Android. Hver har egne særegenheter og utfordringer.

Er data kryptert fra ende-til-ende og er eier av nettverket til å stole på?

Data må transporteres mellom sender og mottaker. Det er viktig å kunne stole på at transporten er beskyttet hele veien. Internett er et nettverk av en mengde noder som data må traversere. Åpne, ukrypterte nettverk på flyplasser, hoteller, kafeer og liknende kan utgjøre en risiko. Noen har en landingsside (*captive portal)*, som sender brukerne videre etter en form for autentisering. Disse kan forfalskes av trusselaktører. Dette kan inkludere bruk av åpne wifi-nettverk, både ukrypterte eller krypterte med kjente passord. Til tross for at mye nettverkstrafikk foregår kryptert er det fremdeles mange servere og tjenester som bruker ukryptert webtrafikk. [16] [17] Det er enkelt for trusselaktører å sette opp falske wifi-nettverk som utgir seg for å være kjente og legitime.

Er data lagret og sikret på en god måte?

Data som transporteres via et nettverk, vil i de fleste tilfeller nå en bakenforliggende infrastruktur. Her lagres, prosesseres og sendes data tilbake til enheten. Det er blitt svært vanlig at mobilapplikasjoner bruker tredjepartsbiblioteker og rammeverk for ekstern lagring. Dette gjør utviklingsjobben ofte enklere for leverandør, men kan også medføre sikkerhetsutfordringer på grunn av overflødig funksjonalitet og manglende sikring av standardkonfigurasjon. [18] [19]

Mange store datalekkasjer skjer fordi bakenforliggende servere og tjenester ikke har vært forsvarlig sikret. NSM har sett en tydelig trend mot at trusselaktører bruker underleverandører og tredjeparter som angrepsvektor. [20]

Vedlegg

Utfyllende informasjon om rådene finner du her:

- *nsm.no/mobilrad*
- *nsm.no/sosialemedier*

Kilder

[1] Statista Inc, «Number of mobile app downloads worldwide from 2016 to 2023», 2024. [Internett]. Nettadresse: https://www.statista.com/statistics/271644/worldwide-free-and-paid-mobile-app-store-downloads/

[2] Zimperium, Inc., «2022 Global Mobile Threat Report», 2022. [Internett]. Nettadresse: https://get.zimperium.com/2022-global-mobile-threat-report/

[3] NSM, «13 råd om sikkerhet på mobile enheter», 2023. [Internett]. Nettadresse: https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/13-rad-for-bedre-sikkerhet-for-mobile-enheter.

[4] NSM, «Nasjonalt digitalt risikobilde 2022», 2022. [Internett]. Nettadresse: https://nsm.no/regelverk-og-hjelp/rapporter/nasjonalt-digitalt-risikobilde-2022

[5] European Union Agency for Cybersecurity, «ENISA Threat Landscape 2022», 2022. [Internett]. Nettadresse: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

[6] NSM, «Sikkerhetsfaglig råd», 2023. [Internett]. Nettadresse: https://nsm.no/regelverk-og-hjelp/rapporter/sikkerhetsfaglig-rad-et-motstandsdyktig-norge

[7] «The New Arab», 2022. [Internett]. Nettadresse: https://english.alaraby.co.uk/news/egypt-using-unethical-online-surveillance-cop27-app

[8] S. Kirchgaessner, «Israeli spyware company NSO Group placed on US blacklist», 2021. [Internett]. Nettadresse: https://www.theguardian.com/us-news/2021/nov/03/nso-group-pegasus-spyware-us-blacklist

[9] S. Kirchgaessner, «The Guardian | No 10 suspected of being target of NSO spyware attack, Boris Johnson 'told'», 2022. [Internett]. Nettadresse: https://www.theguardian.com/politics/2022/apr/18/no-10-suspected-of-being-target-of-nso-spyware-attack-boris-johnson

[10] Apple Inc., «Apple sues NSO Group to curb the abuse of state-sponsored spyware», 2023. [Internett]. Nettadresse: https://www.apple.com/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware/

[11] S. Groß, «Project Zero: A Look at iMessage in iOS 14» 2021. [Internett]. Nettadresse: https://googleprojectzero.blogspot.com/2021/01/a-look-at-imessage-in-ios-14.html

[12] Apple Inc., «Om Lockdown-modus» 2022. [Internett]. Nettadresse: https://support.apple.com/no-no/HT212650

[13] Android Open Source Project, «Design for Safety». [Internett]. Nettadresse: https://developer.android.com/design-for-safety

[14] Apple Inc., «Apple styrker sikkerheten for brukerne med ny, kraftig databeskyttelse», 2023. [Internett]. Nettadresse: https://www.apple.com/no/newsroom/2023/01/apple-advances-user-security-with-powerful-new-data-protections/

[15] D. Goodin, «Ars Technica | Developer of Checkm8 explains why iDevice jailbreak exploit is a game changer», 2019. [Internett]. Nettadresse: https://arstechnica.com/information-technology/2019/09/developer-of-checkm8-explains-why-idevice-jailbreak-exploit-is-a-game-changer/

[16] Google Inc, «HTTPS encryption on the web – Google Transparency Report». [Internett]. Nettadresse: https://transparencyreport.google.com/https/overview

[17] W3Techs, «Usage Statistics of Default protocol https for Websites», January 2023. [Internett]. Nettadresse: https://w3techs.com/technologies/details/ce-httpsdefault

[18] Kotlin Foundation, «The Six Most Popular Cross-Platform App Development Frameworks | Kotlin», 2023. [Internett]. Nettadresse: https://kotlinlang.org/docs/cross-platform-frameworks.html

[19] T. Karasavvas, «Why Flutter is the most popular cross-platform mobile SDK», 2022. [Internett]. Nettadresse: https://stackoverflow.blog/2022/02/21/why-flutter-is-the-most-popular-cross-platform-mobile-sdk/

[20] Håkon Styri, NSM, «Like sikkert på innsiden som på utsiden». Debattinnlegg i Finansavisen, 2021. [Internett]. Nettadresse: https://www.finansavisen.no/nyheter/debattinnlegg/2021/04/11/7653409/like-sikkert-pa-innsiden-som-pa-utsiden

[21] T. H. Nätt, «Store norske leksikon | Skadevare», 2022. [Internett]. Nettadresse: http://snl.no/skadevare.