NSM

Temarapport

Nasjonal kontroll av IKT-tjenester

Temarapporten beskriver mulige internasjonale avhengigheter for IKT-tjenester, og er relevant for virksomheter med tjenester de enten drifter helt selv eller har i noen grad tjenesteutsatt til leverandør i Norge eller utlandet.

Oktober 2023

Nasjonal sikkerhetsmyndighet (NSM) er Norges direktorat for forebyggende nasjonal sikkerhet.

Nasjonalt cybersikkerhetssenter (NCSC) er en del av NSM, og ble etablert 2019. Senteret bidrar til å beskytte grunnleggende nasjonale funksjoner, offentlig forvaltning og næringsliv mot cyberangrep.

NSMs temarapporter inneholder råd og anbefalinger til bruk for norske virksomheter. De er ment å belyse temaer, bygge kompetanse og bistå norske virksomheter i forebyggende sikkerhetsarbeid.

Innhold

1 Introduksjon

1.1 Oppsummering

Denne temarapporten beskriver faktorer som kan skape internasjonale avhengigheter i forbindelse med IKT-tjenester. Det drøftes hvordan slike avhengigheter kan forstås for så å oppnå bedre nasjonal kontroll på en IKT-tjeneste. Tematikken er relevant for virksomheter som drifter en tjeneste helt selv, eller når den helt eller delvis tjenesteutsettes til leverandør i Norge eller utland.

Slike avhengigheter kan bestå av flere faktorer, eksempelvis *1)* geografisk plassering av datasenter, *2)* geografisk plassering av personell som drifter og støtter de ulike delene av systemene og *3)* eierskap i verdikjedene. Det kan også være viktig å forstå avhengigheter i forbindelse med *4)* krisespekteret (fred, krise, væpnet konflikt).

1.2 Bakgrunn

NSM får stadig spørsmål fra norske virksomheter om bruk av utenlandske skytjenester. Mange lurer på hvilke råd NSM og andre myndigheter har. Denne rapporten søker å konkretisere dette gjennom faktorer som kan være relevante å vurdere. Det kan være hensiktsmessig at både kunder og leverandører har en klar forståelse av faktorer som er relevante ved vurdering av nasjonal kontroll.

Regjeringen [1] mener det er viktig å «*å ivareta Norges suverenitet, territorielle integritet og politiske handlefrihet. Målet sikres gjennom et bredt sett av politiske, militære, folkerettslige, diplomatiske, teknologiske og økonomiske virkemidler»*. NSM er bekymret for at suverenitet og politisk handlefrihet kan bli utfordret dersom norske virksomheter ikke forbedrer den nasjonale kontrollen av viktige norske IKT-tjenester.

Det er en del misforståelser knyttet til bruk av skytjenester. Det kan være mange fordeler med bruk av utenlandske skytjenester, men samtidig kan slik bruk være vanskelig å forene med behovet for nasjonal kontroll. Flere misforståelser er nevnt i kapittel 4.1 - ytterligere informasjon.

For å oppnå nasjonal kontroll tror en del virksomheter at det er tilstrekkelig at serveren, med sin tjeneste, er plassert i Norge og at virksomheten selv står for applikasjonsdrift. De glemmer imidlertid ofte at plattformlagene «under» applikasjonen ofte driftes fra flere andre land. Tilsvarende gjelder for eksempel brukerdatabasene (inneholder brukerkontoer for sluttbrukere samt for de som drifter systemet). Virksomheter og personell som drifter disse underliggende lagene har teknisk tilgang til data og har teknisk kontroll på tjenesten selv om serveren er plassert i Norge - uansett valg av kryptering (forklart nærmere i kapittel 4). Mange virksomheter i både offentlig og privat sektor har misforstått dette og tror deres tjeneste er under norsk teknisk kontroll.

Ta hensyn til krisespekteret. Norge er avhengig av en del tjenester og systemer gjennom hele krisespekteret (fred, krise, væpnet konflikt). Hvis slike tjenester helt eller delvis leveres fra utlandet, eller helt eller delvis driftes fra utlandet, er tjenesten utenfor norsk kontroll. Da kan vi som samfunn være sårbare.

Andre europeiske land har tilsvarende bekymringer. Flere land har etablert, eller er i ferd med å etablere, egne nasjonale skytjenester. Utfordringer med å få IKT-tjenester under nasjonal kontroll er ikke en særnorsk problemstilling og blir fremhevet både internt i andre land og i europeisk sammenheng [2].

1.3 Avgrensing

Rapporten presenterer noen av de viktigste faktorene som gjelder internasjonale avhengigheter for norske virksomheters *IKT-tjenester* (egne og kjøpte). Vi fokuserer også på *IKT-produkter (maskinvare og programvare)* der disse benyttes til å bygge opp slike IKT-tjenester.

Tematikken kan være relevant for alle IKT-tjenester som benyttes i Norge, enten de leveres av en utenlandsk leverandør, norsk leverandør eller av virksomheten selv.

Rapporten har en generell tilnærming og går ikke nærmere inn på hvilke typer tjenester og data som bør være under nasjonal kontroll.

Rapporten søker å være uavhengig av spesifikke lover. Den offentlige debatten rundt bruk av utenlandske skytjenester har hovedsakelig fokusert på personvernlovgivning, men tematikken kan også være relevant i forhold til andre regelverk. Rapporten unngår å knytte tematikken til et bestemt regelverk, men peker generelt på en rekke internasjonale avhengigheter for IKT-tjenester.

Rapporten søker å være mest mulig uavhengig av utviklingen innen teknologi, lovgivning og internasjonal politikk. Rapporten bør leses uten at man kobler den for mye til dagens teknologi, dagens lovgivning og dagens internasjonale sikkerhetspolitiske situasjon. Rapporten søker å ta hensyn til at fremtiden alltid er uviss, og at enkelte av Norges mer prinsipielle valg rundt IKT-tjenester bør være robuste i et langsiktig perspektiv.

1.4 Målgruppe

Alle virksomheter kan ha nytte av denne rapporten. Den kan bidra til bevisstgjøring om avhengigheter utenfor Norge ved valg av IKT-tjenester og IKT-produkter.

Rapporten har et teknologifokus, men også ikke-teknologer vil ha nytte av den.

2 Hva betyr nasjonal kontroll for din virksomhet?

2.1 Hva menes med nasjonal kontroll?

Begrepet “nasjonal kontroll” er omtalt i stortingsmeldingen “Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet” [3].

Hvorfor er nasjonal kontroll av IKT-tjenester viktig for Norge?
Nasjonal kontroll av IKT-tjenester er viktig for å beskytte data og tjenester i norske virksomheter og for å hindre at Norge kommer i et for stort avhengighetsforhold til andre land. Slike vurderinger foregår ikke bare i Norge. Også på nasjonalt nivå i flere europeiske land, og sentralt på EU-nivå, står denne og beslektede problemstillinger høyt på agendaen [2].

Nasjonal kontroll for IKT-tjenester i praksis
En rekke IKT-tjenester er viktige for myndighetsutøvelse og for å ivareta viktige funksjoner i samfunnet. Disse IKT-tjenestene bør i større grad være under nasjonal kontroll. Nasjonal kontroll for IKT-tjenester innebærer at:

- utvalgte norske data og tjenester er underlagt *reell norsk teknisk og juridisk kontroll* og at man med høy grad av sannsynlighet kan utelukke at utenlandske selskaper og andre land har teknisk tilgang til norske data og tjenester. Dette innebærer at det ikke skal være teknisk mulig for noen utenfor Norge (inkludert utenlandske leverandører og andre lands myndigheter) å lese, manipulere eller sabotere norske data og tjenester.
- data og tjenester skal *fungere godt i hele krisespekteret* uten å komme i konflikt med forrige punkt.

Beslektede begreper: Digital suverenitet og autonomi
Utenfor Norge benyttes begrepet *«digital suverenitet»* om tilsvarende utfordringer. Dette gjelder både i EU [2] og de enkelte medlemsland. Begrepet «digital suverenitet» har ofte en bredere betydning enn «nasjonal kontroll». Blant annet brukes begrepet digital suverenitet også i at Europa bør bli mer selvforsynt på utvikling og produksjon av programvare og maskinvare. Dette er ikke en sentral del av denne rapporten. Det kan også nevnes at man i flere land benytter begrepet «sovereign cloud» i omtale av ulike prosjekter for nasjonale skytjenester.

I en del sammenhenger benyttes også begrepet «autonomi». Dette omfatter et systems evne til å være uavhengig av andre systemer. I praksis vil det si at et autonomt system skal fungere selv om forbindelsen til omverden brytes. Man kan for eksempel ha lokal, regional eller nasjonal autonomi. Et eksempel på regional autonomi er at man kan kommunisere internt i Nord-Norge selv om en sentral enhet på Østlandet feiler. Denne rapporten fokuserer i så henseende på nasjonal autonomi. Eksempelvis at systemer i Norge skal virke selv om landets utenlandsforbindelser skulle bli brutt for en kortere eller lengre periode.

Forholdet mellom nasjonal kontroll og andre varianter av geografisk kontroll

Det er ikke alltid det er hensiktsmessig at data og tjenester er under nasjonal kontroll. I noen tilfeller vil slike begrensninger også kunne være i strid med konkurransemessige hensyn og hensynet til fri fly av varer og tjenester i EUs indre marked.

Rapporten omtaler mest behovet for nasjonal kontroll i forbindelse med en IKT-tjeneste. Rent teoretisk (dvs. uavhengig av nåværende nasjonale og internasjonale regelverk) bør man likevel være oppmerksom på flere varianter:

- Med *«nasjonal kontroll»*, så har man ideelt sett ingen digitale avhengigheter utenfor *Norge*.
- Med *«nordisk kontroll»*, så har man ideelt sett ingen digitale avhengigheter utenfor *Norden*.
- Med *«europeisk kontroll»*, så har man ideelt sett ingen digitale avhengigheter utenfor *Europa*.
- Med *«vestlig kontroll»*, så har man ideelt sett ingen digitale avhengigheter utenfor *vestlige land*, primært NATO-land i tillegg til noen andre land.

Det er i dag flere regelverk som systemeiere må være oppmerksom på. Et relevant eksempel er *europeisk* regelverk som kan hindre krav om utelukkende nasjonale leverandører. Alle europeiske leverandører skal da kunne levere et tilbud i forbindelse med IKT-anskaffelser. Slike regelverk er avhengig av hva slags data og tjenester det dreier seg om. Det kan da være relevant for noen å lese denne rapporten slik at man i alle fall bør sikre at IKT-tjenesten er under *europeisk kontroll*, dvs. ideelt sett ikke har avhengigheter utenfor Europa.

2.2 Utenlandske avhengigheter kan ikke unngås

Det sies at Norge ikke kan bli hundre prosent selvforsynt på matvarer. Det samme gjelder også IKT-produkter og IKT-tjenester. Det er ikke realistisk at Norge selv kan produsere nok maskinvare og programvare. Det er heller ikke realistisk at Norge blir hundre prosent selvforsynt på IKT-tjenester. Det er heller ikke alltid at det er hensiktsmessig.

Det kan bli krevende å oppnå stordriftsfordeler, tilgang til kompetanse og tjenester, ny innovasjon, og samtidig ha nasjonal kontroll.

Ideelt sett, med hensyn til nasjonal kontroll, kan det være ønskelig at datasenter er lokalisert i Norge, all drift og support foregår i Norge, selskap, materiell og rettigheter er norskeid, all maskinvare og programvare er utviklet og produsert i Norge, osv. Dette idealet er naturligvis ikke realistisk.

Det er derfor nødvendig å foreta en del valg som kan bidra til reduksjon av risiko. Man bør etterstrebe en hensiktsmessig balanse av nasjonal kontroll, funksjonalitet og økonomi.

Virksomheter må gjøre en risikovurdering av hvilke land man har avhengigheter til og hvilke land man kan tillate seg å ha avhengigheter til. Det bør gjøres en vurdering ut i fra en rekke forhold som er beskrevet i NSMs temarapport om landvurderinger [4]. Som en tommelfingerregel kan det antas at land i Norges politiske nærhet i utgangspunktet har lavest risiko. Landvurdering er relevant i forbindelse med vurdering av eierskap, plassering av datasentre, plassering av personell samt ved import av maskinvare og programvare.

2.3 Forslag til ulike nivåer av nasjonal kontroll

Virksomheter, systemer, og verdier er ulike og er underlagt ulike regelverk. Det kan være hensiktsmessig å ha ulike nivåer for nasjonal kontroll. Dette kan både være mer kostnadseffektivt og gi tilstrekkelig fleksibilitet og valgmulighet.

Man kan se for seg at en IKT-tjeneste kan ha en av følgende:

- *lav* grad av nasjonal kontroll
- *middels* grad av nasjonal kontroll
- *høy* grad av nasjonal kontroll

Et fjerde nivå kan gjelde graderte systemer underlagt sikkerhetsloven.

De ulike nivåene kan inneholde ulik bruk av de ulike vurderingsfaktorene som nevnes i kapittel 3.

2.4 Har din IKT-tjeneste behov for nasjonal kontroll?

Ikke alle IKT-tjenester i norske virksomheter trenger økt grad av nasjonal kontroll. I mange tilfeller kan internasjonale avhengigheter ha liten betydning, og nytteverdien av å fritt kunne benytte løsninger fra utenlandske leverandører kan være stor.

Utgangspunktet bør være at man vurderer tjenesten i lys av hvilken funksjon tjenesten har og hvor viktig funksjonen er for virksomheten og de som bruker tjenesten. Følgende kan være nyttig ved en slik vurdering:

a) Vurdere relevant gjeldende regelverk, men forsøk å ha et langt tidsperspektiv. Regelverk er ikke alltid oppdatert til den teknologiske utvikling og den internasjonale sikkerhetspolitiske situasjon.

b) Vurderingene bør omfatte både data, metadata og selve tjenesten mht. konfidensialitet, integritet og tilgjengelighet.

c) Vurderingene bør inkludere hele krisespekteret.

d) Ta også hensyn til at tjenester ofte bygges opp av flere underliggende tjenester, som kan ha uklare internasjonale forgreninger.

e) Vurder også om det for eksempel er tilstrekkelig med «europeisk kontroll», ref. kapittel 2.1.

2.5 Hvor bør en virksomhet begynne?

Rapporten tar frem flere faktorer for nasjonal kontroll av en tjeneste. Disse kan være krevende å vurdere for den enkelte virksomhet. Hvis virksomheten vurderer at det er behov for økt nasjonal kontroll av en tjeneste, bør man i første omgang se på følgende:

- **Faktor nr.1:** Bør tjenestene kun benytte datasentre i Norge?
- **Faktor nr.2:** Bør alle lag driftes og støttes (support) av personell som er i Norge?
- **Faktor nr.3:** Har man tilstrekkelig beredskap for hele krisespekteret? Hvordan blir andre virksomheter eller samfunnet påvirket hvis min virksomhets tjenester bortfaller midlertidig eller for alltid.

Dersom overnevnte faktorer ikke er vurdert, er det fare for at virksomheten har en iboende sårbarhet som må håndteres. En slik sårbarhet kan bli både en virksomhetsmessig og en nasjonal sårbarhet. I så fall bør virksomheten ta tak i disse utfordringene.

3 Faktorer for nasjonal kontroll av IKT-tjenester

Det finnes ulike faktorer som påvirker graden av nasjonal kontroll av tjenester for Norge. Disse er oppsummert her:

> ***Viktige faktorer for nasjonal kontroll***
>
> *1: Plassering av **datasenter***
>
> *2: Plassering av **personell for drift og støtte** (support) av programvare og maskinvare*
>
> *3: Nødvendig **beredskap** for både fredstid, krise og væpnet konflikt*
>
> *4: Kontroll på **eierskap** og nasjonalitet i alle ledd av leverandørkjedene*
>
> *5: Tillit til **programvare** og **maskinvare** (IKT-produkter)*
>
> *6: Tilstrekkelig **sikkerhetsskille** mellom ulike kunder på samme infrastruktur*

Disse faktorene drøftes nærmere i avsnittene under. Disse faktorene er relevante enten man drifter selv eller om man tjenesteutsetter.

Merk at slike faktorer for nasjonal kontroll har mindre effekt hvis man likevel ikke har **god IKT-sikkerhet**. Derfor bør alle aktivt benytte et sikkerhetsrammeverk som NSMs grunnprinsipper for IKT-sikkerhet [9], ISO/IEC 27000-serien eller lignende. Dette gjelder både egen IKT-infrastruktur og ved tjenestekjøp. IKT-arkitekturen bør følge moderne prinsipper som beskrevet i [10] og i [9, kategori 2].

3.1 Plassering av datasenter

Et datasenter består av et eller flere datarom som leverer strøm, kjøling, dataforbindelse og fysisk sikring til datamaskiner (servere) og nettverksutstyr. Datamaskinene og nettverksutstyret, sammen med en del annet utstyr, produserer selve datatjenestene. Datasentre kan være små og store, noen produserer tjenester for mange kunder (herunder skytjenester), mens andre produserer tjenester utelukkende for en enkelt virksomhet. Datasentre kan være plassert i Norge og i utlandet.

Mange norske tjenester benytter datasentre i utlandet. Ofte er dette uproblematisk, men dersom det er et behov eller krav om nasjonal kontroll i forhold til tilgjengelighet, integritet og konfidensialitet på en tjeneste, så er dette ikke mulig å oppnå dersom tjenesten produseres i et datasenter utenfor Norge.

Risikoreduserende tiltak

- Generelt bør tjenester som har behov for nasjonal kontroll benytte datasentre i Norge. NSM har skrevet en egen rapport om dette tema, med noen anbefalinger [5].

3.2 Plassering av personell for drift og støtte (support)

Drift

Selv om et datasenter befinner seg i Norge, kan programvaren og maskinvaren som kjører/plasseres i datasenteret være driftet fra utlandet.

Eksempler på drift kan være: sikkerhetskopiering, installasjon, avinstallasjon, oppdatering, konfigurasjon, tilgangsstyring, brukeradministrasjon, nettverksdrift, systemovervåkning, hendelseshåndtering, avhending, mm.

Drift omfatter både maskinvare og programvare. For å forstå hva slags maskinvare og programvare det siktes til, se lister i kapittel 3.5.

Drift vil innebære stor grad av automatisering, men driftspersonell vil likevel ha tilgang.

Det er generelt teknisk mulig for driftspersonell å lese data, endre data, opprette ny data, slette data eller stoppe tjenesten hvis et annet lands myndighet skulle beordre dem til det. Driftspersonell utenfor Norge er underlagt sitt lands lovgivning, ikke norsk lovgivning. Disse *kan* aksessere norsk data hvis de pålegges det (hverken tilgangskontroll eller kryptering med egne nøkler hjelper mot slik beordret aksess, se kapittel sist i rapporten). Eksempelvis vil ofte det nederste programvarelaget, infrastrukturlaget (bl.a. virtualiserings-programvaren) som regel driftes fra utlandet.

Hvis deler av driften utføres fra utlandet, har man ikke reel teknisk nasjonal kontroll over tjenesten eller data.

Støtte (support)

Begrepet «brukerstøtte» er mest kjent som hjelp til sluttbrukere, mens «support» eller generell «støtte» er et bredere begrep som bl.a. også omfatter støtte til de som drifter systemet.

Personell som utfører støtte og har adgang til tjenesten kan ha 1) leserrettigheter til data, 2) skriverettigheter til data og 3) systemrettigheter (administrative eller privilegerte rettigheter). Sistnevnte er i praksis rettighetsmessig tilsvarende som systemdrift, selv om mange selskaper omtaler slikt som støtte. Merk at da er det først og fremst støtte til kundens driftspersonell.

Det er ofte krevende å finne nok personell i Norge for slike oppgaver. I tillegg er det ofte billigere å kjøpe slike tjenester fra utland.

Risikoreduserende tiltak

- Hvis man trenger nasjonal kontroll av en IKT-tjeneste så må **drift** av *alle lag* utføres av personell som arbeider i Norge. Det er *ikke* tilstrekkelig at maskinene står i Norge. Også brukerdatabaser bør plasseres i og driftes fra Norge.
- All **støtte** som innebærer les-, skriv- eller systemrettighet bør utføres av personell som er plassert i Norge. Dersom dette ikke er mulig, er systemrettigheter viktigere enn skriverettigheter, som er viktigere enn leserettigheter. Hvis ikke støtte kan utføres i Norge, vurder hvilke land som gir minst risiko, se kapittel 2.2. Påse at tilstrekkelig logging utføres, og at i alle fall logging er under nasjonal kontroll. Som minimum bør uansett støtte med systemrettigheter utføres fra Norge.

Se kapittel 4 for mer utfyllende om støtte.

Merk at det ikke nødvendigvis er et problem at IKT-tjenesten *brukes* fra en datamaskin eller mobiltelefon (klient) som er utenfor Norge. Tilstrekkelig IKT-sikkerhet er en forutsetning, slik at tjenesten ikke kan hackes på grunn av en for dårlig sikret klient.

3.3 Nødvendig beredskap for fred, kriser og væpnet konflikt

Mange av dagens IKT-kjøp baserer seg på en antagelse om at en normaltilstand alltid vedvarer. Noen virksomheter bør vurdere beredskapstiltak for å beskytte IKT-systemer mot enkelte uvanlige/dramatiske hendelser. Alle slike hendelser *kan ramme Norge både indirekte eller mer direkte*. Noen eksempler på slike hendelser kan være:

- *Menneskelige eller teknisk svikt:* Alvorlige hendelser behøver ikke være villede, men komme som resultat av menneskelige eller tekniske feil som i noen tilfeller kan ende opp med å ramme kundene. Det kan gjelde både telekominfrastrukturen og skytjenester. Eksempelvis stoppet en skytjeneste opp i februar 2023 [6], som rammet et stort antall kunder i mange land. Heldigvis ble dette løst etter ca. 1-2 døgn. Ved fremtidige globale tjenesteutfall er det ikke nødvendigvis slik at norske kunder vil bli prioritert.
- *Naturkatastrofer*: Orkaner, flommer, tørke, mm. kan påvirke elektrisitetsforsyning, datasentre eller telekominfrastruktur. Klimaendringer kan øke hyppighet av slike hendelser.
- *Sabotasje*: internasjonal og nasjonal telekominfrastruktur kan for eksempel bli ødelagt (eller avlest). Norges og Sveriges plassering på en halvøy er en utfordring, da alle internasjonale dataforbindelser må via havbunnen eller broer. Satellittforbindelser kan være et supplement, men kan ha begrenset kapasitet og kan også introdusere andre sårbarheter.
- *Overbelastninger* kan føre til at norske virksomheter blir nedprioritert i forhold til virksomheter i andre land.
- *Væpnet konflikt* i eller i nærheten av Norge. I verste fall kan Norge bli helt eller delvis okkupert. I dag er det liten fare for slikt, men kan oppstå i et lengre perspektiv.
- *Sanksjoner*: Akkurat som mat og energi, kan også IKT-tjenester bli brukt som et politisk virkemiddel mot et land, eksempelvis [7]. Slike avhengigheter kan benyttes for å redusere Norges handlefrihet i en krise eller en væpnet konflikt. Sanksjoner (eller trusler om sanksjoner) *kan* også forekomme i fredstid, et eksempel er fra 1993, se [8].

Noen eksempler på mulige konsekvenser:

- Tjenesten man er avhengig av blir utilgjengelig. Det kan bli alvorlig hvis dette rammer sektorer som kraftproduksjon, helse, telekom, politi, finans, forsvar, mm.
- Man kan ikke logge inn på sine maskiner og tjenester på grunn av at identitetstjenester (Identity-as-a-service) blir utilgjengelige.
- Norske folkevalgte politikere kan miste handlefrihet i utøvelse av sin politikk. Det vil si at de får færre valgmuligheter når de skal velge Norges kurs i for eksempel en krise.
- Norske virksomheter kan miste råderetten på egne eller andres data.
- Data og tjenester kan bli lest og misbrukt av annen stat ved militær overtagelse av et norsk datasenter. Enkelte bør derfor etablere evnen til *raskt å slette visse data i visse datasentre*.

- Data og tjenester kan gå permanent tapt ved helt eller delvis militær okkupasjon av Norge. Enkelte bør derfor etablere evne til *raskt å flytte data og tjenester til alternative lokasjoner* i Norge, norsk territorium utenfor fastlands-Norge eller lokasjoner i utlandet. Merk at dette kan gjøres på flere måter uten å miste nasjonal kontroll over tjenesten, det er ikke nødvendig å bruke utenlandske selskaper.

Disse eksemplene kan virke lite sannsynlig i dag. Imidlertid vil det oppstå endringer i den internasjonale sikkerhetspolitiske situasjon over tid. Utfordringen er å forutse *hva* disse endringene kan innebære, og *hvor alvorlige* de blir. Norske IKT-kjøp bør ikke baseres på forutsetninger om at slike scenarier aldri kan forekomme og at dagens internasjonale orden vil være uendret over IKT-systemenes levetid.

Risikoreduserende tiltak

Noen virksomheter bør etablere beredskapsplaner for IKT for hele krisespekteret, bruk gjerne scenarieeksemplene over.

For å planlegge slikt må man vurdere de ulike typer data og tjenester og deres beskyttelsesbehov.

3.4 Kontroll på eierskap og nasjonalitet i alle ledd

Eierskap og nasjonalitet ifm. IKT-tjenester kan gjelde blant annet:

- Eiere av skytjenesteleverandøren
- Eiere av underleverandører til skytjenesteleverandøren
- Eiere av selskaper eller underleverandører som utvikler eller distribuerer programvare og maskinvare (se liste i kapittel 3.5)
- Eiere av for eksempel serverne i et datasenter
- Eiere av datasentre. I tillegg bør man vurdere eiere av underleverandører som vaktselskapet, elektrikere, og andre entreprenører/underleverandører.

Slike eiere kan være underlagt andre lands lover. Når hele eller deler av verdikjeden er underlagt andre lands lovverk har man en situasjon hvor norsk regelverk kan bli «satt til side». Norske myndigheter har da mistet deler av sin myndighetsutøvelse, for eksempel det å verne om innbyggernes interesser. Man får en situasjon hvor norske og andre lands lover og interesser kommer i motsetning til hverandre.

Eierskap kompliseres av oppkjøp slik at eierskap og eieres nasjonale tilknytning endres. Eierskap består også av komplekse verdikjeder av ulike tjenester og «undertjenester» som en hovedleverandør bygger inn i sin tjeneste, men som kunden ofte ikke er oppmerksom på.

Denne tematikken drøftes delvis i Stortingsmelding 9-2022 om nasjonal kontroll [3].

Risikoreduserende tiltak

Det kan være vanskelig for kunder å få oversikt over eierforhold. Noen sikkerhetsmessige kompromisser med hensyn til eierskap må man nok leve med.

- Kartlegg leverandørkjedene til de ulike produktene og tjenestene som skal benyttes, i den grad det er mulig og hensiktsmessig.
- Vurder hvilke land som gir minst risiko, ref. kapittel 2.2. Det kan hjelpe i de tilfellene leverandørenes opprinnelsesland og nasjonale tilknytning er oversiktlig.
- Det kan være mange ulike eiere i et selskap. Det mest praktiske er ofte å ta utgangspunkt i plasseringen til hovedkontoret.

3.5 Tillit til programvare og maskinvare (IKT-produkter)

Følgende er eksempler på programvare *brukt i moderne IKT-tjenester:* virtualisering-plattformer, verktøy for plattform-orkestrering, operativsystemer, kontainer-plattformer, database-plattformer, verktøy for systemovervåkning, verktøy for håndtering av brukere og rettigheter samt andre driftsverktøy. Disse produktene består av kode/algoritmer.

Følgende er eksempler på maskinvare *brukt i moderne IKT-tjenester:* serverskap, servere, lagringssystemer, nettverksutstyr, kabler, mm. Disse produktene inneholder blant annet kretslogikk, mikrokode, UEFI-kode, radiosendere, mm.

Overnevnte programvare og maskinvare benyttes både i systemene til store skytjenesteleverandører, andre tjeneste-leverandører og i vanlige IT-avdelinger.

Programvare og maskinvare omtales videre samlet som I*KT-produkter*.

Nesten ingen av disse IKT-produktene har norsk opprinnelse. Det er ikke realistisk at Norge kan bli selvforsynt med slike produkter.

Med *tillit* til IKT-produkter så menes det at *i)* man bør ha en trygghet i at det ikke er skjult funksjonalitet i produktene som kan misbrukes og som kan skade norske interesser. Det er også viktig å ha tillit til at *ii)* produktene blir støttet og videreutviklet mht. til å lukke sårbarheter, og at reservedeler er tilgjengelige. Til slutt *iii)* så må en kunde ha en tillit til at algoritmer produserer rett svar uten bias mm. slik at man tar avgjørelser basert på korrekt grunnlag.

IKT-produkter og IKT-tjenester *kan* ha det som kalles bakdører. Som alle andre stater må også norske myndigheter ta slike muligheter med i betraktning. Se kapittel sist i rapporten for nærmere forklaring på hva som menes med bakdører.

Risikoreduserende tiltak

Tilliten til IKT-produkter kan være vanskelig for kunder å ha oversikt over. Deres opphav likeså. Man kan ikke regne med å oppnå 100% tillit til IKT-produkter.

- Noen sikkerhetsmessige kompromisser må man leve med. Vurder hvilke land som gir minst risiko, se kapittel 2.2.
- Som et minimum kan det være en realistisk målsetning å unngå *kundespesifikke* bakdører. For maskinvare kan det da være hensiktsmessig å blant annet være diskret med å opplyse distributør/leverandør om bruken og formålet når man bestiller et produkt. Og ikke la produktet bli stående for lenge på distributørs og eget lager (potensielt ubevoktet) før det tas i bruk. For programvare (inkludert oppdateringer) kan det også være hensiktsmessig å være diskret mht. bruken av programvaren. Ytterlig forbedret tillit kan oppnås hvis det kan etablere

felles krav til leverandører og distributører. Det kan være krevende uten et koordinert samarbeide på nasjonalt, nordisk eller europeisk nivå.

3.6 Tilstrekkelig sikkerhetsskille mellom ulike kunder

Dagens skytjenester leveres som regel fra fysiske servere og lagringsmedier som deles mellom mange ulike kunder fra ulike sektorer/bransjer, slik bruk av delte ressurser kalles gjerne «flerbruk» eller «multitenancy». Også virtuelle nett kan bli delt mellom ulike kunder.

Alle IKT-produkter (både maskinvare og programvare) har sårbarheter. Noen sårbarheter er kjente mens andre ikke er oppdaget eller offentliggjort enda. Noen av sårbarhetene kan svekke skillet mellom ulike kunders tjenester og data. Noen momenter her:

- Ulike kunder kan ha ulik nasjonalitet. Ved alvorlige sårbarheter kan det bli utført angrep fra en kunde til en annen kunde. Da kan den nasjonale kontrollen svekkes.
- Ulike kunder av samme nasjonalitet kan ha svært ulik risikovillighet med ulik IKT-sikkerhet. Kunder som er mindre nøye mht. IKT-sikkerhet kan bli hacket og kan da bli en trussel mot både leverandøren eller mot de kundene som er mer opptatt av sikkerhet.
- På sektor/bransje-nivå vil for eksempel sannsynligvis kunder i offentlig sektor eller i finansbransjen ikke ønske å dele kritiske ressurser med kunder i bransjer som er mindre opptatt av sikkerhet. Det er sannsynligvis større forskjeller på ønsket risikoeksponering mellom ulike sektorer/bransjer.

Risikoreduserende tiltak

- Undersøk om en leverandør har et tilfredsstillende sikkerhetsskille mellom de ulike kundene. Finn ut hvordan ressurser som nettverk, server, lagring, brukerhåndtering mm. fungerer på tvers av kundene.
- Grupper av kunder kan gå sammen og bestille egne, dedikerte fysiske ressurser fra en tjenesteleverandør. Det kan for eksempel være et samarbeid mellom flere virksomheter i offentlig sektor. For private selskaper kan koordinering utført av bransjeforeninger være en god tilnærming.

3.7 Andre faktorer

Det finnes andre faktorer som også er relevant når man vurderer grad av nasjonal kontroll. Samtidig så er det er ikke nødvendigvis slik at alle faktorene som er nevnt er like relevant i alle scenarier og for alle virksomheter. Faktorene som er nevnt er en slags fellesnevner som kan være relevante for de fleste.

4 Ytterlig informasjon og referanser

4.1 Ytterlig informasjon

Dette kapittelet underbygger rapporten med kompetanse som NSM ønsker å dele ut over det som allerede er skrevet i rapporten.

Kort om lagdelingen i alle moderne datasentre

Moderne sky-plattformer og kundenes egne moderne datasentre kan forenkles etter følgende generelle lag-oppdeling:

- *Lag 6 - Programvare:* Selve tjenestene (applikasjonene)
- *Lag 5 - Programvare:* Kontainertjenester, databasetjenester, mm.
- *Lag 4 - Programvare:* Virtuelle datamaskiner og/eller kontainere, mm.
- *Lag 3 - Programvare:* Hypervisorer, kontainer-plattform, mm.
- *Lag 2 - Maskinvare:* Fysiske servere, fysisk nettverk og fysisk lagring
- *Lag 1 - Datarom:* Rom med tilgang til strøm, nett, kjøling, mm.

Modellen med lagene over er gyldig for alle moderne datasentre, både leverandørers datasentre og virksomheters egne datasentre.

Begrepene *IaaS, PaaS og SaaS* er godt kjent. Litt forenklet kan man si at lag 1-3 representerer det som tilbys av en IaaS-tjeneste (hvis kunden utfører det meste selv med hensyn til de virtuelle maskinene i lag 4), lag 1-5 representerer det som tilbys av en PaaS-tjeneste og lag 1-6 representere det som tilbys av en SaaS-tjeneste. Det kan det være variasjon i hvordan leverandører tilbyr dette eller hvordan deres kunder benytter de ulike tilbudene.

Vanlige misforståelser om skytjenester

Det er flere vanlige misforståelser i forbindelse med dagens populære skytjenester, disse har relevans enten for nasjonal kontroll og for vanlig IKT-sikkerhet:

- Det medfører ikke riktighet at man har norsk kontroll på data bare fordi det leveres fra et datasenter i Norge. Man har heller ikke norsk kontroll fordi applikasjonslaget driftes av noen i Norge. Ved de fleste skytjenester vil i praksis noe av driften foregå i ulike land. Dette gjelder for eksempel programvaren i lag 3 og 4 i modellen over. Et annet eksempel er systemovervåkning. Da er norsk data og metadata teknisk sett kontrollert og tilgjengeliggjort av en eller flere utenlandske selskaper som må følge andre lands lover, inkludert andre lands etterretnings-lover.

- Mange tror at kryptering av data med egne kundenøkler kan løse utfordringen med forrige punkt. Dette er en utbredt misforståelse. Med dagens teknologier er det dessverre umulig å teknisk sett hindre skytjenesteleverandør innsyn i kundedata, uansett hva slags kryptering som benyttes. Les mer om dette på [11]. En ofte spissformulert «definisjon» av skytjenester er at «sky kun er noen andres datamaskiner». I andres datamaskiner er det umulig å følge med på alt som skjer. Det betyr at det ikke er realistisk at en kunde kan oppdage slik uønsket avlesning av data.

- Det er riktig at en del sårbarheter fjernes av skytjenesteleverandøren når man flytter til en skytjeneste. Ikke minst er profesjonelle leverandører raskere på å innføre sikkerhetsoppdatering av programvare. Men *vesentlig* sikkerhetsgevinst oppnås ved å fjerne sårbarheter som for eksempel *i)* lett gjettbare passord til bruk og drift, *ii)* svak styring og manglende segmentering av nettverk, *iii)* svak styring av systemrettigheter, *iv)* med mer. Dette vil i mange tilfeller fortsatt være en del av kundenes oppgaver. De mest vanlige dataangrep kommer gjerne via «toppen» av infrastrukturen (se lagdeling tidligere i teksten). Hvis ikke nevnte og andre sårbarheter også fjernes/reduseres, da kan sikkerhetsgevinsten ved å flytte til en skytjeneste i mange tilfeller bli marginal. God sikkerhet er fremdeles også avhengig av kundens eget sikkerhetsarbeid.

Kort om ulike trusler mot IKT-tjenester

Man bør vurdere ulike trussel scenarier. Disse truslene kan gjelde både egne tjenester i egne datasentre og innkjøpte skytjenester (nr. 5 er kun relevant for innkjøpte skytjenester). Det kan være

- *Trussel scenario 1 - datakriminalitet*: dataangrep fra individer og kriminelle som for eksempel skader (digital utpressing - løsepengeangrep) og stjeler konfidensiell informasjon.
- *Trussel scenario 2 – avtapping:* faren for at uvedkommende kan lese innholdet av data som transporteres blant annet mellom kundens og skytjenesteleverandørens datasenter.
- *Trussel scenario 3 - insider*: faren for utro tjenere i alle deler av leverandørkjedene i skytjenestene.
- *Trussel scenario 4 - etterretning1:* etterretning fra stater som ikke også er hjemlandet til skytjenesteleverandøren.
- *Trussel scenario 5 - etterretning2:* etterretning fra samme stat som også er skytjenesteleverandørens hjemland (for eksempel Schrems 2 – scenariet).
- *Trussel scenario 6 - krisespekteret*: manglende sikkerhet/beredskap i ulike deler av krisespekteret.
- *Trussel scenario 7 – konfigurasjons-utnyttelse*: manglende/svak sikkerhetskonfigurasjon av tjenesten gir angripere ekstra muligheter.
- *Trussel scenario 8 – verdikjede*: angripere utnytter svakheter hos underleverandører av skyleverandør eller svakheter i leveransekjeder av tjenester. Dette kan også være relevant for underleverandør benyttet til egne tjenester driftet selv i eget datasenter.

Utfyllende om støtte (support)

Vær oppmerksom på at:

- Å gi *systemrettigheter* til personell utenfor Norge gir størst risiko. De som har slike rettigheter kan beordres til å lese data, endre data, opprette ny data, slette data eller stoppe tjenesten. Rettighetsmessig er dette i praksis drift. Støtten er primært for de som skal drifte tjenesten.
- Å gi *skriverettigheter til data* til personell utenfor Norge gir også risiko. De som har slike rettigheter kan beordres til å lese data, endre data, opprette ny data eller slette data.
- Å gi *leserettigheter til data* til personell utenfor Norge kan og gi risiko. De som har slike rettigheter, kan beordres til å lese data.

Den tekniske muligheten for slike operasjoner (som er ulovlig etter norsk lov, men ikke nødvendigvis etter andre lands lover) kan redusere tillit til den norske tjenesten.

Merk også at uavhengig av både mulig beordring og geografi, så kan personell med rettighetene i listen over naturligvis også bli hacket/kompromittert.

Hvis man likevel velger å benytte personell i andre land til støttetjenester, så bør man sikre seg god sporbarhet mht. hva personell har utført. Sporbarhet kan etableres ved bruk av *logging* av transaksjoner. Slik logging må naturligvis ikke kunne manipuleres av noen utenfor norsk kontroll. Med transaksjoner menes alle operasjonene på tjenesten (drift og alle operasjoner på data eller metadata). Loggingen må regelmessig inspiseres (automatisert, med manuell oppfølging av varsler) av personell i Norge for å kontrollere at det ikke er utført uønsket brudd på behovet for norsk kontroll av tjenesten.

Norsk støttepersonell må gjerne *dele skjerm* i digitale møter med støttepersonell utenfor Norge. Sistnevnte får da selv ikke tilgang til data eller system, men kan veilede personell i Norge. Personell i Norge er ansvarlig for at sensitive data ikke vises. Bruk gjerne norsk møteprogramvare (de utenfor Norge trenger vanligvis ikke samme programvare – de kan gjennomføre møtet i en nettleser). Opptak bør deaktiveres eller være under kontroll av personell i Norge.

Kort om mulige bakdører i maskinvare, programvare eller IKT-tjenester

NSM viser her kun til offentlig kjent informasjon. Følgende er en generell/akademisk gjennomgang.

«Bakdører» er et begrep som angir en «bakvei» inn for uvedkommende, og som er ukjent for kundene. Bakdører kan være *a)* i maskinvare, programvare eller tjenester, *b)* være beordring av leverandør eller uten kjennskap fra leverandøren (for eksempel sårbarhetsutnyttelse), *c)* innføres i ulike deler av leverandørkjeden (utvikling, produksjon, transport, oppbevaring, bruk), *d)* være permanent til stede siden produksjon eller temporære (ved tjenester med hyppige oppdateringer) og *e)* ramme alle kundene eller være kundespesifikke. Sist, men ikke minst så er det *f)* det er lite sannsynlig at virksomheter kan selv oppdage slikt, det blir eventuelt ved (sjeldne) publiserte lekkasjer/varslinger at slikt blir kjent.

Sårbarhetsutnyttelse: all IKT (maskinvare, programvare og tjenester) har nesten uten unntak sårbarheter. Med rett kompetanse, kursing i avansert penetrasjonstesting, god økonomi og litt tålmodighet så finner man gjerne til slutt de sårbarhetene man trenger for å finne og utnytte en bakdør. Det er sannsynlig at noen land har gode fagmiljøer på slike oppgaver. Slikt arbeid er antagelig relevant i forbindelse med populære IKT-produkter (maskinvare og programvare) som benyttes i datasentre, skytjenester, IT-avdelinger, mm.

Det blir ofte en spekulasjon om man kan regne med eller ikke regne med slike bakdører. Som de fleste nasjonalstater må også norske myndigheter likevel ta slike muligheter med i betraktning for å best mulig beskytte både nasjonalstaten og innbyggernes rettigheter.

Kort om mulighet for etterretning i forbindelse med IKT-tjenester

NSM viser her kun til offentlig kjent informasjon. Følgende er en generell/akademisk gjennomgang.

Rent akademisk kan etterretning forekomme *flere steder* ifm. IKT-tjenester. Disse stedene kan være: *1)* Brukerens terminal, *2)* kundens eget datasenter, *3)* ved landegrenser med statspålagt overvåkning, *4)* kommunikasjonskabler (på land og under vann), *5)* kommunikasjons-hubber og *6)* datasenter til tjenesteleverandør.

Rent akademisk, f*or alle disse 6 stedene kan gjelde*: *a)* Både masseinnhenting eller mer målrettet innhenting, *b)* både innhenting ved beordring av leverandør eller uten kjennskap fra leverandør (sårbarhetsutnyttelse), *c)* både avlesning av data og avlesning av metadata, *d)* både kapasitet for dataavlesning, kapasitet for dataforfalskning og kapasitet for sabotasje av tjenesten, og *e)* etterretning utført både av vennligsinnede og ikke så vennligsinnede stater.

Man kan se for seg ulike kombinasjoner med disse to listene. Det finnes en rekke offentliggjorte eksempler, så dette er ikke teoretisk.

Det blir ofte en spekulasjon om man kan regne med eller ikke regne med etterretning i forbindelse med IKT-tjenester. Som alle stater må også norske myndigheter likevel ta slike muligheter med i betraktning for å best mulig beskytte både nasjonalstaten og innbyggernes rettigheter.

4.2 Referanser

[1] Sikkerhetspolitikk, Regjeringen, https://www.regjeringen.no/no/tema/utenrikssaker/sikkerhetspolitikk/id1111/

[2] Digital sovereignty for Europe, European Parlament, 2020, https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

[3] Stortingsmelding 9-2022, Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet, https://www.regjeringen.no/no/dokumenter/meld.-st.-9-20222023/id2950130/

[4] Landvurdering ved tjenesteutsetting av IKT-tjenester, https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/landvurdering-ved-tjenesteutsetting-av-ikt-tjenester

[5] Norske datasentre og digital autonomi, NSM, 2022. www.nsm.no/sky

[6] Microsoft Outlook Service Goes Down Worldwide on Feb. 6, https://redmondmag.com/articles/2023/02/07/microsoft-outlook-service-goes-down-worldwide-on-feb-6.aspx

[7] Microsoft suspends new sales in Russia, https://blogs.microsoft.com/on-the-issues/2022/03/04/microsoft-suspends-russia-sales-ukraine-conflict/

[8] Norway threatened with sanctions over whales, New Scientist, 1993, https://www.newscientist.com/article/mg13918880-300-norway-threatened-with-sanctions-over-whales/

[9] NSMs grunnprinsipper for IKT-sikkerhet, NSM, 2020, www.nsm.no/gp-ikt

[10] Statens muligheter for IT-modernisering og digital transformasjon (VIRT-1902), NSM, 2021. www.nsm.no/sky

[11] Ofte stilte spørsmål om sky og tjenesteutsetting, NSM, www.nsm.no/sky/oss