Sikkerhetsfaglige anbefalinger ved bruk av tjenesteutsetting og skytjenester

Hensikten med denne temarapporten er å bistå offentlige og private virksomheter med overordnede sikkerhetsfaglige anbefalinger ved tjenesteutsetting av IKT-tjenester herunder bruk av skytjenester. Anbefalingene er relevante for offentlige og private virksomheter som vurderer å tjenesteutsette basisdrift, applikasjonsdrift eller applikasjonsforvaltning til en ekstern tjenesteleverandør.

Bakgrunn

Det er en økende trend at private og offentlige virksomheter velger å tjenesteutsette hele eller deler av sin IKT-portefølje. Ifølge Statistisk sentralbyrå (SSB) benytter 85,4 % av kommunene seg av skytjenester[1]. Private virksomheter med ti eller flere ansatte benytter 51 % seg av en eller flere skytjenester. Internasjonalt er trenden den samme.

Tjenesteutsetting, inkludert skytjenester, er av de mest betydningsfulle trendene innen digitaliseringen av samfunnet. Digitalisering av samfunnet kan sammenlignes med øvrig samfunnsutvikling som strøm, jernbane og vann. Vellykket digitalisering er en viktig driver for innovasjon og for effektivisering av samfunnets tjenester. Virksomhetene benytter tjenesteutsetting som ett av virkemidlene for å holde følge med teknologiutviklingen og digitaliseringen, og ofte skjer dette ut av landet.

Økende bruk av tjenesteutsetting gjelder også for virksomheter som understøtter samfunnets beredskap og krisehåndtering. Dette er leveranser som bør være mer robuste og tilgjengelige enn vanlige kommersielle løsninger, fordi de skal fungere i situasjoner hvor mye annet er utilgjengelig. Dette må tas hensyn til når tjenesteutsetting vurderes.

Det blir stadig mer krevende å ha oversikt over allerede komplekse verdikjeder ved økende digitalisering av samfunnet. Tjenesteutsetting bidrar til å øke risikoen ved ytterligere å øke kompleksiteten i verdikjeden.

Erfaringer fra NSMs operative virksomhet og andre statlige tilsynsorganer viser at det er lav bevissthet rundt krav til og oppfølging av informasjonssikkerhet ved tjenesteutsetting av IKT-tjenester. Risikovurderinger og konsekvensutredninger som utføres ved tjenesteutsetting er ofte mangelfulle. NSM er bekymret for at samfunnskritiske IKT-tjenester tjenesteutsettes uten tilstrekkelige risikovurderinger og sikringstiltak, og at data flyttes til utlandet uten tilstrekkelige sikkerhetsfaglige vurderinger.

Hensikten med temarapporten er å bistå offentlige og private virksomheter med overordnede sikkerhetsfaglige anbefalinger om hva som bør ivaretas ved tjenesteutsetting av basisdrift, applikasjonsdrift eller applikasjonsforvaltning. Anbefalingene er relevante for offentlige og private virksomheter. Rapporten bør leses i sammenheng med *NSMs grunnprinsipper for IKT-sikkerhet*.

[1] Statistisk sentralbyrå, «Digitalisering i kommunene», 2019

Kontaktpunkt for kommentarer er ikt-radgivning@nsm.no. Vennligst bruk rapportens navn som emne. Kommentarer og innspill mottas med takk.

Sikkerhetsfaglige anbefalinger for tjenesteutsetting

Tjenesteutsetting av IKT-tjenester til profesjonelle aktører kan gi bedre sikkerhet og mer stabile og tilgjengelige tjenester. Tilgang til ekspertkompetanse og verktøy man ikke selv besitter kan bedres, kostnader kan bli lavere og mer forutsigbare og det kan i større grad bidra til bedre fokus på virksomhetens kjerneaktivitet. Samtidig må virksomheter være bevisst hvilken risiko en tjenesteutsetting medfører. Tilsvarende eller høyere nivå på både tjenestekvalitet og IKT-sikkerhet bør være en målsetning ved tjenesteutsetting.

En tjenesteutsetting stiller store krav til egen virksomhet og krever annen kompetanse enn om tjenesten leveres av egen organisasjon. Før det foretas en strategisk beslutning om bruk av tjenesteutsetting, bør virksomheten vurdere om den er «rigget» for å håndtere alle faser i en tjenesteutsettingsprosess. Virksomheten må også kartlegge hvilke lover, krav og regler som gjelder både nasjonalt og internasjonalt. Eksempelvis gir både sikkerhetsloven og personopplysningsloven med forskrifter føringer ved tjenesteutsetting. Noen sektorer har også regulert hvilke muligheter virksomheten har til å tjenesteutsette.

For å ivareta IKT-sikkerheten ved tjenesteutsetting, anbefaler NSM at virksomheten er bevisst behovet for:

1. **God bestillerkompetanse**
2. **Oversikt og kontroll på hele livsløpet**
3. **Gode risikovurderinger for å kunne ta riktig beslutning**
4. **Riktige og gode krav til IKT-tjenesten og til leverandør**
5. **Riktig beslutning på riktig nivå**

1. God bestillerkompetanse

En vellykket tjenesteutsetting fordrer at virksomheten har god bestillerkompetanse. Svak bestillerkompetanse kan medføre at virksomheten anskaffer IKT-tjenester uten tilstrekkelig kartlegging av behov, og kan gi utfordringer med å stille gode krav til blant annet IKT-sikkerhet ovenfor leverandør. Det kan resultere i at tjenesteutsettingen gjennomføres uten at det er vurdert hva som skal ivaretas gjennom livsløpet til tjenesteutsettingen, fra forberedende aktiviteter til opphør av avtalen.

NSM anbefaler at virksomheten 1) ivaretar behovet for bestillerkompetanse gjennom hele livsløpet til tjenesteutsettingen, og 2) som et minimum har følgende kompetanseområder ved en tjenesteutsetting:

Virksomhets-kompetanse	**Sikkerhets-kompetanse**	**Integrasjons-kompetanse**	**Kompetanse om anskaffelser**	**Juridisk kompetanse**
- For å kunne definere behov og stille nødvendige krav.	*- For å kunne vurdere risiko og stille riktige sikkerhetskrav. Dette gjelder alle områder av sikkerhet dvs. fysisk, personell-*	*- For å kunne forstå hvordan tjenestene kan integreres i virksomheten på best mulig måte.*	*- Slik at anskaffelsen kan gjennomføres på en måte som støtter virksomhetens forretnings-messige og*	*- Slik at virksomhetens juridiske krav og behov ivaretas og at kontrakten kan oppfylles i produksjonen.*

	og informasjons-sikkerhet.		*funksjonelle behov på best måte.*	

Grunnleggende IKT-kompetanse er en forutsetning for kvalitet i kompetanseområdene beskrevet over.

2. Oversikt og kontroll på hele livsløpet

Når en virksomhet har besluttet å ta i bruk tjenesteutsetting som en del av sin IKT-strategi, må man sørge for å etablere oversikt og kontroll på hele livsløpet ved tjenesteutsettingen. Livsløpet kan inndeles i fire hovedfaser (forberedende, anskaffelse, forvaltning og opphør), hvor hver fase inkluderer et sett med behov og krav som må følges opp. **NSM anbefaler at kontrakten for tjenesteutsettingen må omhandle alle fasene.**

Figur 1: Tjenesteutsettingens livsløp kan deles i fire hovedfaser. I hver fase er det et sett med aktiviteter som virksomheten må ha oversikt og kontroll over.

Forberedende: I denne fasen utarbeides detaljerte forutsetninger for tjenesteutsettingen, samt at det gjøres nødvendige vurderinger av om tjenesteutsettingen kan gjennomføres og eventuelt hvordan. En viktig vurdering her er hvordan tjenesten som settes ut skal integreres med virksomhetens øvrige IKT-systemer, slik at nødvendig sikkerhetsnivå ivaretas.

Anskaffelse: Med basis i forutsetningene og vurderingene i den forberedende fasen, starter arbeidet med valg av leverandør og inngåelse av kontrakt. Innholdet i kontrakten er svært viktig fordi kontrakten regulerer forholdet mellom virksomhet og leverandør, herunder leveransekvalitet, rapportering, endringsprosesser, revisjon og møtearenaer. Utvetydige prosedyrer for verifisering og oppfølging av kontraktens leveransekrav bør være på plass før kontraktsinngåelse og iverksetting av tjenesteutsettingen.

Forvaltning: Fasen innebærer etablering, integrering og eventuell transisjon av tjenesten som settes ut. Den må videre regulere hvordan virksomheten skal følge opp leverandøren og leveransene, slik at kontraktsforpliktelsene samt virksomhetens endringsbehov ivaretas i kontraktsperioden. Forvaltning innebærer at avvik fra leveransekravene vurderes med hensyn til iverksetting av tiltak.

Opphør: Dette er perioden når virksomheten skal avslutte tjenesteutsettingen. Det kan være tilsiktede og utilsiktede grunner til at en virksomhet avslutter kontrakten. Det kan eksempelvis være kontraktsbrudd eller endrede uakseptable forhold ved vertslandet og/eller leverandør. Ved opphør må virksomheten være særlig forberedt på to aktiviteter:

1. Tilbakeføring og/eller overføring: Iverksette plan for å tilbakeføre tjenesten til virksomheten, eller overføre tjenesten til en annen leverandør.
2. Sletting: Iverksette plan for at data tilhørende virksomheten blir forsvarlig slettet av leverandøren.

3. Gode risikovurderinger for å kunne ta riktig beslutning

En beslutning om tjenesteutsetting bør tas basert på risikovurderinger som beskriver de faktiske risikoene tjenesteutsettingen medfører. *NSMs erfaringer tilsier at det i altfor stor grad er et primærfokus på kostnader og at det kun vurderes økonomisk risiko eller risiko ved gjennomføring av selve tjenesteutsettingen (prosjektrisiko).* **NSM anbefaler å tydeliggjøre hva en risikovurdering som omhandler en tjenesteutsetting av IKT-tjenester skal inneholde og at hele livsløpet til tjenesteutsettingen risikovurderes.**

Eksempler på faktorer som vil kunne påvirke risikobildet er redusert kontroll på stadig mer komplekse verdikjeder, tap av intern kompetanse og avhengigheter til eksterne tjenesteleverandør for å kunne levere virksomhetens tjenester. Risikovurderingen bør også inkludere risiko knyttet til selve leverandøren, eksempelvis leveranseevne og muligheten til å vedlikeholde ønsket sikkerhetstilstand.

Utsetting av en eller flere tjenester vil endre konfigurasjonen og sammensetningen på virksomhetens IKT-portefølje og arkitektur. Tjenestene skal i de fleste tilfeller integreres i eksisterende infrastruktur og tjenesteportefølje. Tjenesteutsetting til en profesjonell aktør kan i mange tilfeller gi bedret sikkerhet, men nye sårbarheter kan også introduseres. Samtidig er virksomheten avhengig av at leverandøren iverksetter nødvendige kompenserende tiltak, noe som kan være utfordrende å kontrollere. En virksomhet som tjenesteutsetter må derfor ha et aktivt forhold til hvordan leverandøren iverksetter tiltak og reduserer risiko slik at risikovurderingene i egen virksomhet beskriver den faktiske risikoen virksomheten tar.

Eksempler på områder som bør risikovurderes er:

- Geografisk og fysisk lokalisering av utstyr og driftspersonale.
- Hvem som har innsyn i virksomhetens informasjon.
- Hvor og hvordan informasjon behandles og lagres, samt hvordan informasjonen er adskilt fra andre kunder.
- Tilgangsstyring, inkludert kryptering, aktivitetslogging og fysisk og logisk sikkerhet.
- Rutiner for hendelseshåndtering og avviks- og sikkerhetsrapportering.
- Krise- og beredskapsplaner som skal harmonisere med virksomhetens egne planer.
- Bruk av underleverandører.
- Fremtidige endringer i leverandøren og underleverandørers eierskapsstruktur.
- Mulighet for terminering av kontrakten og overføring (transittering) av tjenester og data til ny leverandør.

Hvis tjenesten skal leveres fra utlandet, anbefaler NSM, i tillegg til å vurdere tjenestetilbyderen, å vurdere vertslandet der leverandøren har tilhold og hvor tjenesten tilbys fra. Nasjonale forhold kan påvirke en tjenesteleverandørs mulighet til å levere tjenester, eksempelvis gjennom kvaliteten på nasjonal infrastruktur eller nasjonal lovgivning som gir rett til innsyn i data lagret i vertslandet. Risikoen knyttet til vertslandet kan dermed gi avgjørende føringer på behovet for kompenserende sikringstiltak og hvilke tjenestetilbydere som bør vurderes. *Landvurderingen bør inngå som en del av den totale risikovurderingen ved tjenesteutsettingen.* NSM har utarbeidet en egen temarapport som beskriver en modell for å vurdere ulike lands egnethet for tjenesteutsetting. Virksomheten må også vurdere om andre relevante kriterier ved vertslandet skal vurderes. Eksempelvis kan forhold i transittland påvirke risiko.

Virksomheten må revidere risikoen knyttet til tjenesteutsettinger jevnlig og gjennom alle faser av tjenesteutsettingen. Risikobildet vil endres over tid slik at kompenserende tiltak som lå til grunn for

risikoaksept ved kontraktsinngåelse ikke nødvendigvis er tilstrekkelig over tid. Eksempler på faktorer som kan påvirke risikobildet over tid kan være endringer i trusselbildet, økt avhengighet av IKT-tjenesten i det norske samfunnet, endringer i egen bestillerkompetanse, innsikt i nye teknologiske sårbarheter og nye opplysninger knyttet til vertslandet eller leverandøren som leverer tjenesten.

4. Riktige og gode krav til IKT-tjenesten og til leverandør

En kritisk suksessfaktor for en vellykket tjenesteutsetting er å stille riktige og gode krav. Kravene uttrykker et behov og må formuleres slik at de kan bli verifisert. Kravene beskriver hva virksomheten ber om, og spesifiserer hva tjenestetilbyderen skal levere. En tjenesteutsetting blir ikke bedre enn kravene. Sett fra et kontraktsperspektiv er kravene, og verifikasjon av disse, bindeleddet mellom virksomhetens behov og tjenesten som leveres fra tjenestetilbyderen.

Virksomheten må utarbeide en detaljert **kravspesifikasjon for IKT-tjenesten** som skal tjenesteutsettes. Sikkerhetskravene en virksomhet stiller til konfidensialitet, integritet og tilgjengelighet til sine IKT-tjenester må gjelde uavhengig av geografisk lokasjon og om det er tjenesteutsatt eller ikke. Dersom det er forhold som kan ha innvirkning på risikoen, må disse identifiseres og vurderes, og kompenserende tiltak må iverksettes**. NSM anbefaler at *NSMs grunnprinsipper for IKT-sikkerhet* brukes i utarbeidelse av kravene som stilles til IKT-tjenesten.**

Hvis leverandøren ikke kan levere på kravene som stilles er det viktig at virksomheten tar en veloverveid beslutning basert på risikoen tjenesteutsettingen medfører, og vurderer kompenserende tiltak.

Virksomheten bør utarbeide et kravdokument for alle faser av tjenesteutsettingen, det vil si selve anskaffelsen, forvaltning og driftsfasen samt ved terminering av kontrakten. Ved en tjenesteutsetting bør det som minimum stilles **krav til at leverandøren** har:

- Et etablert styringssystem for informasjonssikkerhet og sertifisering i henhold til internasjonale standarder, for eksempel ISO/IEC 27001:2017.
- Innsyn i sikkerhetsarkitekturen som benyttes for å levere tjenesten.
- Utviklingsplaner for sikkerhet i tjenesteproduksjonen i tråd med utvikling i teknologi og trusselbildet over tid.
- En oversikt over hvem som skal ha innsyn i virksomhetens informasjon, hvor og hvordan denne skal behandles og lagres samt grad av mekanismer for segregering fra andre kunder.
- Tilgangsstyring som inkluderer kryptering, aktivitetslogging og fysisk og logisk sikkerhet.
- Sikkerhetsovervåkning egnet til å avdekke hendelser og handlinger i tråd med virksomhetens trusselbilde og relevante trusselaktører.
- Rutiner for hendelseshåndtering og avviks- og sikkerhetsrapportering.
- Krise- og beredskapsplaner som skal harmonisere med virksomhetens egne planer.
- Godkjenningsprosedyrer for bruk av underleverandører og deres bruk av underleverandører.
- Spesifisert hvilke aktiviteter som skal utføres ved terminering av kontrakten, blant annet tilbakeføring/flytting/sletting av virksomhetens informasjon.

5. Riktig beslutning på riktig nivå

I dagens digitaliserte samfunn vil bortfall av IKT-tjenester som oftest påvirke hele eller store deler av virksomheten. Settes virksomhetskritiske tjenester ut til en tredjepart, kan det øke risikoen for både tilsiktede og utilsiktede hendelser som for eksempel bortfall av tjeneste eller tap/endring av data.

Beslutningen om tjenesteutsetting bør ikke utelukkende tas av virksomhetens IKT-miljø alene. Valg av leverandørmodell og tjenesteutsetting av IKT-tjenester er en viktig strategisk del av virksomhetsstyringen. Virksomhetens leder bør sørge for en godt forankret prosess for alle berørte parter i virksomheten. Når en beslutning om tjenesteutsetting tas, bør den baseres på risikovurderinger som beskriver tjenesteutsettingens påvirkning på hele virksomheten, herunder leveranseevne, IKT-portefølje, økonomi og behov for kompetanse.

NSM anbefaler at avtaler om tjenesteutsetting av IKT-tjenester og endringer i slike avtaler skal behandles av øverste ledelse. I mange tilfeller vil dette være styret i en virksomhet. Styret skal forelegges planer for tjenesteutsettingen, med risikovurdering. Dersom tjenesteutsettingen påvirker virksomhetskritiske leveranser, anbefaler NSM at private virksomheter behandler og vedtar tjenesteutsettingen i styret, eller for offentlige virksomheter; at beslutningen om tjenesteutsetting godkjennes av overordnet fagdepartement.

Dokumenthistorikk

2017-12-06 Dokumentet godkjent for publisering.
2020-x-x