FORUM FOR INFORMASJONSSIKKERHET
I KRAFTFORSYNINGEN

Sikkerhetsveileder for Kraftsensitiv Informasjon i Skytjenester

Forum for informasjonssikkerhet i kraftforsyningen

Dato: 29.10.2021

Innholdsfortegnelse

SAMMENDRAG

Databehandling flyttes i økende grad fra interne systemer til skybaserte løsninger og det er utarbeidet nasjonale strategier for å flytte data og prosessering ut i skytjenester. Slike tjenester kan forenkle digitaliseringen av kraftsektoren der det kreves nye modeller for innsamling, prosessering og deling av data. Nye sensorløsninger tilgjengeliggjør ofte data kun via skytjenester. Samtidig har kraftbransjen lover, forskrifter og veiledere om beskyttelse av kraftsensitiv informasjon. De enkelte aktørene i kraftsektoren oppfatter at det er vanskelig å vurdere hva som er godt nok for å overholde regelverket når man skal implementere og forvalte løsninger med kraftsensitiv informasjon i skytjenester.

På vegne av aktørene har medlemmer i FSK etablert et prosjekt for utarbeidelse av denne veilederen. Prosjektet har hatt bred deltakelse fra sektoren og er ledet av DNV.

Veilederen gir innledningsvis en oppsummering av relevante myndighetskrav fra energiloven og kraftberedskapsforskriften, samt føringer, veiledere og standarder som ligger til grunn for veilederen. Deretter greies det ut om noen av de unike utfordringene med kraftsensitiv informasjon i skytjenester, som blant annet at skyleverandører ofte kun tilbyr standardvilkår, revisjon av skyleverandør, kontroll på leverandør- og verdikjeden og den geografiske lokasjonen til informasjonen.

Leveransemodellene for skytjenester utredes, og det tydeliggjøres hvilke elementer i løsningen der virksomheten har kontroll og hvilke elementer der skyleverandøren har kontroll. En referansemodell beskriver typiske anvendelser i kraftbransjen. Det beskrives videre hvilke faser som inngår i livssyklusen til en kraftsensitiv skytjeneste og hvilke aktiviteter virksomhetene må gjennomføre i disse fasene. Under «forberedelse» inngår verdivurdering, etablering av sikkerhetsstyring og forankring/godkjenning. Under «anskaffelse» inngår utarbeidelse av kravspesifikasjon og anbudskriterier samt gjennomføring av konkurranse. «Implementeringsfasen» utføres primært av leverandør, men virksomheten er deltakende i akseptansetest. «Forvaltning» inkluderer kontinuerlig kontroll, revisjon og håndtering av sikkerhetshendelser. «Opphør» inkluderer tilbakeføring eller overføring av tjenesten samt sletting av data. Risikostyring er en aktivitet som går over alle fasene. For disse aktivitetene gis konkrete veiledninger og eksempler.

Veilederen gir konkrete anbefalinger om hva som bør inngå i en kravliste som kan benyttes ved anskaffelser. Det er gitt forslag til krav, dokumentasjonskrav, veiledning og kobling til standarder og myndighetskrav for bl.a.:

- Styringssystem for informasjonssikkerhet og trussel- og sårbarhetsvurderinger
- Datasenterets sikkerhet og separasjon mellom kunder
- Sikkerhetskopi og sletting av data
- Endringshåndtering og sporbarhet
- Tilgangskontroll / Autentisering
- Sikkerhetsbrudd / Varsling
- Sikker utvikling
- Geografisk lokasjon lagring, transport og håndtering
- Beskyttelse mot skadevare
- Oppdatert og herdet sikkerhetsarkitektur
- Kontroll på underleverandører
- Etterlevelse av avtale og relevante lover
- Sikring av data i transitt og data i ro
- Tilgjengelighet
- Administrasjon av krypteringsnøkler
- Revisjon
- Oversikt over hvem som skal ha innsyn i kraftsensitiv informasjon
- Rettigheter til bruk av data
- Identifisering og klassifisering av sensitiv informasjon

I veilederens vedlegg gis en konkret veiledning i hvordan man gjennomfører en verdivurdering.

1 INTRODUKSJON

1.1 Bakgrunn og hensikt

Virksomhetene i kraftbransjen ønsker i stor grad å benytte skytjenester og utviklingen er drevet av leverandører og nedfelt i politiske dokumenter som «Nasjonal strategi for bruk av skytenester» /1/. Virksomhetene i kraftbransjen har tatt i bruk skytjenester, men i mindre grad til behandling av kraftsensitiv informasjon. Virksomhetene ønsker å legge til rette for at kraftbransjen får gode rammer for å håndtere informasjonssikkerhet og risiko i det digitaliserte fremtidsbildet.

Medlemmer av Forum for informasjonssikkerhet i kraftforsyningen (FSK) har med utgangspunkt i dette engasjert DNV til å bistå med utarbeidelse av en veileder. Representanter fra Agder Energi Nett, BKK, Lede/Skagerak Energi, Lnett, NVE, Statnett og Tensio har bidratt i utarbeidelsen av denne veilederen.

Veilederen skal hjelpe virksomhetene til å gjøre grundige vurderinger av skyløsninger som skal behandle kraftsensitiv informasjon, slik at informasjonen er tilstrekkelig sikret i henhold til virksomhetens eget behov for informasjonssikkerhet og i tråd med myndighetskrav. Veilederen inneholder sikkerhetsanbefalinger for å imøtekomme krav fra blant annet kraftberedskapsforskriften for bruk av skybaserte tjenester for lagring, transport og behandling av kraftsensitiv informasjon.

1.2 Omfang

Veilederen begrenser seg til skytjenester som behandler kraftsensitiv informasjon og vil ikke problematisere eksponering av andre informasjonstyper mot skyen. Dette betyr at kun de kravene i energilovgivningen som regulerer behandlingen av kraftsensitiv informasjon diskuteres i veilederen. Veilederen vil ikke dekke problemstillinger knyttet til bruk av skytjenester i driftskontrollsystemer.

Veilederen begrenser seg til de momenter som oppstår på grunn av skyleverandørers og skytjenesters natur. Eksempler på dette er bruken av internett som en informasjonsbærer med tilhørende angrepsvektorer, leverandørers markedsmakt, uoversiktlige leverandørkjeder, større behov for brukeransvar, etc. Veilederen vil ikke gå spesifikt inn på konkrete skytjenester, men vil trekke frem bruken av IIoT/IoT for å illustrere at problemstillinger knyttet til skytjenester ikke bare er knyttet til administrative IT-anskaffelser.

Det forutsettes at leseren av veilederen innehar grunnleggende kunnskaper innen IT, skytjenester og kraftbransjen med tilhørende lovgiving. Det forutsettes at virksomheten utreder om det er forsvarlig å ta i bruk skytjeneste for det aktuelle formålet og har vurdert andre driftsformer.

1.3 Myndighetskrav

Merk at for noen av myndighetskravene er kravteksten avkuttet for å fremheve de mest relevante delene for denne veilederen.

Energiloven

Overordnet for myndighetskrav til grunn for veilederen ligger «Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (Energiloven)» /2/.

Energiloven § 9-2 Beredskapstiltak

Den som helt eller delvis eier eller driver anlegg eller system som er eller kan bli av vesentlig betydning for produksjon, omforming, overføring, omsetning eller fordeling av elektrisk energi eller fjernvarme, plikter å sørge for effektiv sikring og beredskap og iverksette tiltak for å forebygge, håndtere og begrense virkningene av ekstraordinære situasjoner som nevnt i § 9-1 fjerde eller femte ledd og for å gjenopprette normal situasjon.

Beredskapsmyndigheten kan gi forskrift eller treffe enkeltvedtak om beredskapstiltak for å forebygge, håndtere eller begrense virkningene av ekstraordinære situasjoner som nevnt i § 9-1 fjerde eller femte ledd eller for å gjenopprette normal situasjon. Beredskapstiltak kan pålegges den som eier eller driver anlegg eller systemer som nevnt i første ledd. Beredskapstiltak kan gjelde for eksisterende og planlagte anlegg eller systemer som nevnt i første ledd.

Ved tjenesteutsetting må det tas hensyn til at det i ekstraordinære situasjoner må være mulig å utføre all drift fra norsk territorium. Det må derfor finnes planer og løsninger som ivaretar dette dersom noen av tjenestene som settes ut i skytjeneste er nødvendig for drift. System som vil måtte vurderes i denne sammenheng er alle støttesystem som er nødvendige for drift over tid, eksempelvis kundesystem, geografiske informasjonssystem, vedlikeholdssystem, driftsplanleggingssystem, etc.

Energiloven § 9-3 Informasjonssikkerhet

Alle enheter i KBO skal vurdere sikkerheten ved all behandling av informasjon om kraftforsyningen. Enhetene skal kartlegge hvilken informasjon som er sensitiv, hvor den befinner seg og hvem som har tilgang til den. Det skal etableres effektiv avskjerming og beskyttelse av sensitiv informasjon.

Enhver plikter å hindre at andre enn rettmessige brukere får adgang eller kjennskap til sensitiv informasjon om kraftforsyningen

Kraftberedskapsforskriften

Kraftberedskapsforskriften (kbf) /3/ er fastsatt av NVE med hjemmel i energiloven /2/. Hensikten med forskriften er å sikre at kraftforsyningen opprettholdes og at normal forsyning gjenopprettes på en effektiv og sikker måte i og etter ekstraordinære situasjoner for å redusere de samfunnsmessige konsekvensene. Sentral for denne veilederen er kraftberedskapsforskriften - kapittel 6. Informasjonssikkerhet. NVE har utarbeidet en veileder til kraftberedskapsforskriften /4/ som detaljerer hvem som er omfattet av forskriften og hvordan virksomheter kan etterleve kravene.

§ 6-1. Identifisering av kraftsensitiv informasjon og rettmessige brukere

KBO-enheter skal etter energiloven § 9-3 første ledd identifisere hva som er kraftsensitiv informasjon, hvor denne befinner seg og hvem som har tilgang til den.

Kbf § 6-1 plasserer ansvaret for identifisering av kraftsensitiv informasjon, samt kontroll på oversikt over lokasjon og tilganger på KBO-enhetene. Dette gjelder også ved tjenesteutsetting hvor skytjenester som oftest er lokalisert, driftet og utviklet utenfor virksomheten. Kbf § 6-1 setter krav til at KBO-enheten må ha kontroll på hvor kraftsensitiv informasjon befinner seg, samt kontroll på skyleverandør og underleverandørers tilganger.

§ 6-2. Kraftsensitiv informasjon

Kraftsensitiv informasjon er underlagt taushetsplikt etter § 9-3 i energiloven.

Med kraftsensitiv informasjon menes spesifikk og inngående opplysninger om kraftforsyningen som kan brukes til å skade anlegg, system eller annet eller påvirke funksjoner som har betydning for kraftforsyningen …

Kraftsensitiv informasjon er definert i kbf § 6-2 og NVEs veileder til kbf /3/ gir en mer detaljert beskrivelse av hvilke typer informasjon som faller under definisjonen.

Som det presiseres i NVEs veileder til kbf /4/, inneholder bestemmelsen en generell definisjon av hva som er å anse som kraftsensitiv informasjon og listen over typer informasjon som er kraftsensitiv er ikke en uttømmende liste. Dette innebærer at all informasjon som kan benyttes til å angripe og skade eksempelvis kommunikasjonsinfrastruktur og informasjonssystemer som benyttes ifm. drift av kraftforsyningen kan anses å være kraftsensitiv informasjon. Dette må være en del av den skjønnsmessige vurderingen som må foretas av den enkelte virksomhet.

§ 6-3. Beskyttelse, avskjerming og tilgangskontroll

Virksomheter som har eller behandler kraftsensitiv informasjon skal etablere, opprettholde og videreutvikle system og rutiner for effektiv avskjerming, beskyttelse og tilgangskontroll for kraftsensitiv informasjon. Beskyttelse skal omfatte tiltak mot avlytting og manipulering fra uvedkommende.

System og rutiner skal omfatte merking, oppbevaring, bruk og distribusjon, tilintetgjøring og tiltak for intern og ekstern rapportering av hendelser av betydning for informasjonssikkerheten.

Virksomheten må sørge for at de ved tjenesteutsetting har tiltak, rutiner og systemer som beskrevet i kbf § 6-3.

§ 6-5. Anskaffelser

KBO-enheter har ansvaret for at bestemmelsene om informasjonssikkerhet og taushetsplikt for kraftsensitiv informasjon ivaretas i anskaffelser. KBO-enheter skal i anskaffelser påse at leverandører er forpliktet til å etterleve bestemmelsene om informasjonssikkerhet og taushetsplikt for kraftsensitiv informasjon. Det skal i avtale sikres at KBO-enheter gis rett til å kontrollere, herunder revidere, leverandørens etterlevelse av disse bestemmelsene.

KBO-enhetene skal ha system og rutiner for å håndtere all kraftsensitiv informasjon slik som forskriften krever, uavhengig av hvor informasjonen er lagret eller hvem som har tilgang til den. Når kraftsensitiv informasjon skal behandles av leverandør eller samarbeidspartnere må KBO-enheten regulere denne informasjonsbehandlingen i en egen sikkerhetsavtale med leverandør eller samarbeidspartner (jf. kbf § 6-5). En egen mal for dette ligger som vedlegg i NVEs veiledning til kbf /4/.

KBO-enheten må i avtalen med leverandøren sørge for at de har rett til å kontrollere leverandørens etterlevelse av kravene til å beskytte kraftsensitiv informasjon. NVE godtar at etterlevelse kan sjekkes gjennom at KBO-enheten får innsyn i og kan kontrollere tredjepartsrevisjonsrapporter av IKT-sikkerheten hos leverandøren.

For tjenesteutsetting av IKT-systemer som behandler kraftsensitiv informasjon (jf. kbf § 6-2), gjelder særlige hensyn for å sikre at taushetsplikten ivaretas.

§

§ 6-9. Digitale informasjonssystemer

Virksomheter skal sikre digitale informasjonssystemer slik at konfidensialitet, integritet og tilgjengelighet ivaretas.

Det er den enkelte virksomhets ansvar å planlegge, gjennomføre og vedlikeholde sikringstiltak etter det digitale informasjonssystemets type, oppbygging og funksjon.

Kbf § 6-9 bygger på NSMs Grunnprinsipper for IKT-sikkerhet /5/ og plasserer ansvaret for digital sikkerhet på virksomheten. Virksomhet er KBO-enheter, men NVE kan fatte vedtak at det gjelder andre også som faller inn under dekningsområdet til lov og forskrift. I tillegg detaljeres det i paragrafen noen krav for grunnsikring.

1.4 Standarder, rammeverk og veiledere

NVE har publisert flere veiledere som ligger til grunn for denne veilederen:

- NVE veiledning til kraftberedskapsforskriften /4/
- NVEs sjekkliste for IKT-sikkerhet i anskaffelser og tjenesteutsetting i kraftbransjen /6/
- NVE rapport nr 26:2017 Regulering av IKT Sikkerhet /7/.

For skytjenester peker NVEs veiledning til kbf /4/ på råd fra Direktoratet for økonomiforvaltning (DFØ) om anskaffelser av skytjenester /8/ og FSKs veileder for Microsoft 365 /9/.

NSMs Grunnprinsipper for IKT-sikkerhet /5/ og NSMs Sikkerhetsfaglige anbefalinger ved bruk av tjenesteutsetting og skytjenester /10/ ligger også særlig til grunn for denne veilederen. Grunnprinsipper for IKT-sikkerhet bygger igjen på internasjonale anerkjente standarder og veiledninger, spesielt ISO/IEC 27002 /11/.

Denne veilederen fra FSK bygger videre på anerkjent praksis og internasjonale standarder som benyttes av de globale skyleverandørene. ISO/IEC 27017 standarden /12/ definerer sikringstiltak for informasjonssikkerhet for både konsumenter og leverandører av skytjenester. Standarden inneholder veiledning basert på kontrollene i ISO/IEC 27002 /11/ tilpasset skytjenester. Videre er det flere kontroller som er spesifikt rettet mot skytjenester.

Center for Internet Security (CIS) publiserer CIS Controls Cloud Companion Guide /13/ som gir veiledning for å implementere beste praksis fra CIS Controls til en skytjeneste sett fra en konsument/kunde sitt perspektiv. For hver høynivå kontroll er det en kort forklaring på hvordan tolke og iverksette CIS Controls i skytjenester.

CSA Cloud Controls Matrix /14/ er et rammeverk for cybersikkerhetskontroller i skytjenester. Rammeverket består av flere domener med tilhørende kontroller for alle hovedaspekter innen skytjenester. Matrisen kan benyttes som et verktøy for systematisk gjennomgang av implementasjon av en skytjeneste, og gir veiledning for hvordan sikkerhetskontroller burde bli iverksatt for hver aktør i skytjenestens verdikjede. Rammeverket er tilpasset til CSA Security Guidance for Critical Areas of Focus in Cloud Computing v4.0 /15/ som er en anerkjent åpen sikkerhetsveileder for skytjenester.

I vedlegg A inneholder en oversikt over litteraturen beskrevet i dette avsnittet, samt mer litteratur relevant for skytjenester og informasjonssikkerhet.

1.5 Noen utfordringer med kraftsensitiv informasjon i skytjenester

De store globale leverandørene av skytjenester har en meget sterk markedsposisjon og tilbyr i hovedsak kun globale standardvilkår til sine kunder. Kraftberedskapsforskriften setter krav til signering av en informasjonssikkehetsavtale som det er utfordrende å få de globale skyleverandørene til å akseptere.

Kraftberedskapsforskriften § 6.1 stiller krav om at KBO-enheter skal etter energiloven § 9-3 første ledd identifisere hva som er kraftsensitiv informasjon, hvor denne befinner seg og hvem som har tilgang til den. Videre fremheves det at identifiseringen av hva som er kraftsensitiv informasjon og hvor denne befinner seg, skal omfatte oppbevaring på papir, lagring i elektronisk form eller lagring på annen måte.

Kravene i forskriften stilles uavhengig av tjenesteform (skybasert, eget datasenter eller i levert ved bruk av andre aktørers digitale systemer), leverandørenes virksomhetsområder eller andre faktorer. Disse kravene medfører utfordringer med eget innsyn i hvem som har tilgang til kraftsensitiv informasjon utover innsyn i logger eller rapporter fra leverandørene.

Kraftberedskapsforskriftens § 6-4.Sikkerhetsinstruks stiller blant annet krav om at virksomheter som har eller behandler kraftsensitiv informasjon skal utarbeide og praktisere en sikkerhetsinstruks som sikrer at kravene til informasjonssikkerhet ivaretas. Sikkerhetsinstruksen skal omfatte informasjon til ansatte og andre rettmessige brukere om taushetsplikten etter energilovens § 9-3 annet ledd og stille krav til undertegning av taushetserklæring. Flere store leverandører godtar ikke krav om personlig signatur for sine ansatte, og krever at dette ivaretas i virksomhetsavtalene. Utfordringen her ligger i at forskriftskravet i noen tilfeller ikke lar seg løse direkte, og at en da må evaluere om leverandørenes standardkontrakter og ansettelsesvilkår for sine ansatte samlet kan møte kraftberedskapsforskriftens krav i tilfredsstillende grad.

Det er videre utfordrende å gjennomføre revisjon og sikkerhetstesting av skyleverandøren og datasenter. Virksomheten må forholde seg til revisjonsrapporter fra leverandøren eller tredjepart.

Forskriftens § 6-8.Sikkerhetskopier definerer også ansvar for sikkerhetskopier, og påpeker at virksomheter skal ha oppdaterte sikkerhetskopier av nødvendig informasjon, programvare og konfigurasjoner av driftskontrollsystemet som er av betydning for drift, sikkerhet og gjenoppretting av kraftforsyningen. Sikkerhetskopiene skal fjernlagres på et sikkert sted, som er lett tilgjengelig for virksomheten.

Skyløsninger kan være etablert på forskjellige geografiske lokasjoner for bl.a. redundans. Det kan være utfordrende for informasjonseier å vite hvor data og sikkerhetskopier befinner seg. Virksomheter kan ofte sette krav til at alle datasenter involvert skal være lokalisert i EFTA, EU eller NATO, men leverandørens drift kan bli utført fra land og av underleverandører utenfor EFTA, EU eller NATO. Døgnkontinuerlig drift og støtte er ofte strukturert slik at lokasjonen hvor arbeidet utføres fra endres basert på tidspunktet på dagen. En annen utfordring knyttet til informasjonens geografiske lokasjon er at datatrafikk kan rutes utenfor EFTA, EU og NATO og at for eksempelvis analysetjenester kan utføres i land utenfor EFTA, EU eller NATO.

Oppfølging og forvaltning av skyleverandører er ressurskrevende. Virksomhetens infrastruktur kan være basert på forskjellige skyleverandører som medfører at virksomheten må følge opp og forvalte mange skyleverandører samtidig.

Som for alle sikkerhetsløsninger må virksomheten også ha sterke kapabiliteter innen forvaltning av blant annet krypteringsnøkler. Det er mange forskjellige konsepter og løsninger knyttet til oppbevaring og tilgang til krypteringsnøkler og det kan være utfordrende for virksomheten å vurdere om disse løsningene er teknisk gode nok. Tap av krypteringsnøkler kan ha kritiske følger da det vil medføre tap av den krypterte informasjonen.

Det kan også oppstå utfordringer med at virksomhetene blir enda tettere knyttet til én leverandør og dermed får mindre reell mulighet til å bytte leverandør på et senere tidspunkt uten store kostnader eller tap av informasjon. Transaksjonskostnader ved bytte av leverandør bør tas med i beregningene. Det er ikke sikkert at skytjenesten er like lønnsom hvis virksomheten må skifte leverandører med jevne mellomrom som følge av anbudsregimet. Virksomheter kan også bli tvunget til å bytte leverandør hvis vilkår endres slik at de bryter med myndighetskrav.

1.6 Innføring av sensorer/IIoT i kraftbransjen

En av kongstankene innen digitaliseringen er å samle inn store mengder produksjonsdata for å gjøre analyser og optimalisering av produksjonen og drift av nett. Dette inkluderer utplassering av en rekke sensorer for å registrere

relevante data, samt at enheter i kraftforsyningen i økende grad blir i stand til å kommunisere (IIoT). Å integrere slike sensorer og intelligente systemer i egen infrastruktur er utfordrende. Trenden er at leverandørene inkluderer denne integrasjonen, datainnsamlingen og analysen i sine tjenester og tilgjengeliggjør data via en skytjeneste. Det er viktig å påpeke at bruk av IIoT-enheter ofte innebærer bruk av skytjenester og at anskaffelsen av slike komponenter må gjennomgå de samme vurderingene og prosedyrene som for anskaffelse av skytjenester som beskrevet i denne veilederen.

1.7 Leseveiledning

Veilederen er strukturert i følgende kapitler:

- Kapitel 2 Definisjoner og forkortelser
- Kapitel 3 Skytjenester: Definisjon av skytjeneste, tjenestemodeller og leveransemodeller. Referansemodell for forskjellige skytjenester presenteres.
- Kapitel 4 Livssyklus for skytjenester: Veiledning til de forskjellige fasene i livssyklusen til en kraftsensitiv skytjeneste. For hver fase beskrives de viktigste aktivitetene, samt at hver aktivitet oppsummeres i et sett med hovedpunkter.
- Kapitel 5 Kravliste til leverandør av skytjeneste: Kravliste som kan benyttes som et utgangspunkt for krav virksomheten kan stille til skyleverandører. Det er viktig at virksomhetene tilpasser kravene basert på blant annet hva slags skytjeneste som skal anskaffes, egen organisasjon og informasjon som skal lagres, transporteres og behandles.
- Kapitel 6 Referanser

I tillegg består veilederen av følgende vedlegg:

- Vedlegg A – Litteraturliste
- Vedlegg B – Sikkerhetsnivå/skalaer for verdivurdering

2 DEFINISJONER OG FORKORTELSER

2.1 Definisjoner

Begrep	Definisjon
Avanserte måle- og styringssystem (AMS)	Toveis informasjons- og kommunikasjonssystem fra og med elektrisitetsmålere som danner grunnlag for avregning av utveksling, innmating og uttak, til og med sentralsystemet hos nettselskapet eller nettselskapets leverandør
Behandling av kraftsensitiv informasjon	Behandling av kraftsensitiv informasjon omfatter fremstilling, innsamling, registrering, sammenstilling, prosessering, anvendelse, lagring, forvaltning, utveksling, deling, avhending, håndtering og beskyttelse av opplysninger. Noen av de opplistede aktivitetene er overlappende
Informasjonsbehandler	Informasjonsbehandler er en virksomhet som innenfor det fastsatte formålet i denne avtalen behandler kraftsensitiv informasjon på vegne av informasjonseier som del av en tjeneste- eller vareleveranse, og/eller ut fra tjenstlige behov.
Informasjonseier	Informasjonseier er en virksomhet med funksjon innen kraftforsyningen som rettmessig utøver ansvar for kraftsensitiv informasjon, og fastsetter rammer og instruks for håndtering, beskyttelse og behandling av denne.
Integritet	Informasjonen blir ikke endret utilsiktet eller av uvedkommende
Konfidensialitet	Informasjonen blir ikke kjent for uvedkommende
Kraftforsyningens beredskapsorganisasjon (KBO)	Kraftforsyningens beredskapsorganisasjon (KBO) består av de enheter som eier eller driver anlegg eller annet som har vesentlig betydning for drift eller gjenoppretting av eller sikkerhet i produksjon, omforming, overføring, omsetning eller fordeling av elektrisk energi eller fjernvarme. Beredskapsmyndigheten kan ved forskrift eller enkeltvedtak fastsette hvilke enheter som skal inngå i KBO. (Energiloven §9-1)
Kraftsensitiv informasjon	Kraftsensitiv informasjon er spesifikke og inngående opplysninger om anlegg, funksjoner, systemer og annet i kraftforsyningen som kan brukes til å påføre skade eller forstyrre levering av kraft, dersom opplysningene blir kjent for uvedkommende (kraftberedskapsforskriften § 6-2).
Risiko	Virkningen av usikkerhet på oppnåelse av mål
Skytjenester	En modell som gjør det mulig å få tilgang til et sett konfigurerbare dataressurser (for eksempel nettverk, servere, lagring, applikasjoner og tjenester) som er lett tilgjengelige over alt, blir levert og priset etter bruk, kan skaffes raskt og gjøres tilgjengelig med minimalt med administrasjon
Sårbarhet	Uttrykk for et systems manglende evne til å motstå en uønsket handling eller uønsket hendelse, samt manglende evne til å gjenoppta sin funksjon.
Tilgjengelighet	Informasjonen er tilgjengelig for autoriserte ved behov
Trussel	Potensiell årsak til en uønsket hendelse

Trusselaktør	Et individ eller enhet som utgjør en trussel mot sikkerheten til en virksomhet. Aktøren kan være intern eller ekstern til virksomheten og handlingen kan være tilsiktet, utilsiktede eller tilfeldig.
Trusselscenario	Hvordan en aktør agerer, for eksempel angrepsmetode, feilkonfigurering, programvarefeil.
Verdi/Aktiva	Kjerneverdiene/ eiendelene til virksomheten på et overordnet nivå

2.2 Forkortelser

Forkortelse	Beskrivelse
AMS	Avanserte måle- og styringssystem
BYOK	Bring Your Own Key
DFØ	Direktoratet for forvaltning og økonomistyring
Enl	Energiloven
FDV	Forvaltning, Drift og Vedlikehold
HYOK	Hold Your Own Key
IaaS	Infrastructure as a Service
IIoT	Industrial Internet of Things
Kbf	Kraftberedskapsforskriften
KBO	Kraftforsyningens beredskapsorganisasjon
NSM	Nasjonal sikkerhetsmyndighet
NVE	Norges vassdrags- og energidirektorat
PaaS	Platform as a Service
SaaS	Software as a Service
SSA	Statens standardavtale
VM	Virtuell maskin

3 SKYTJENESTER

Virksomheten er *alltid* ansvarlig for sine data og informasjonssikkerheten ved bruk av skytjenester, uavhengig av hvilken tjeneste- eller leveransemodell som velges, hvem som forvalter tjenesten, hvor tjenesten kjøres eller hvem som drifter tjenesten.

3.1 Definisjon av skytjeneste

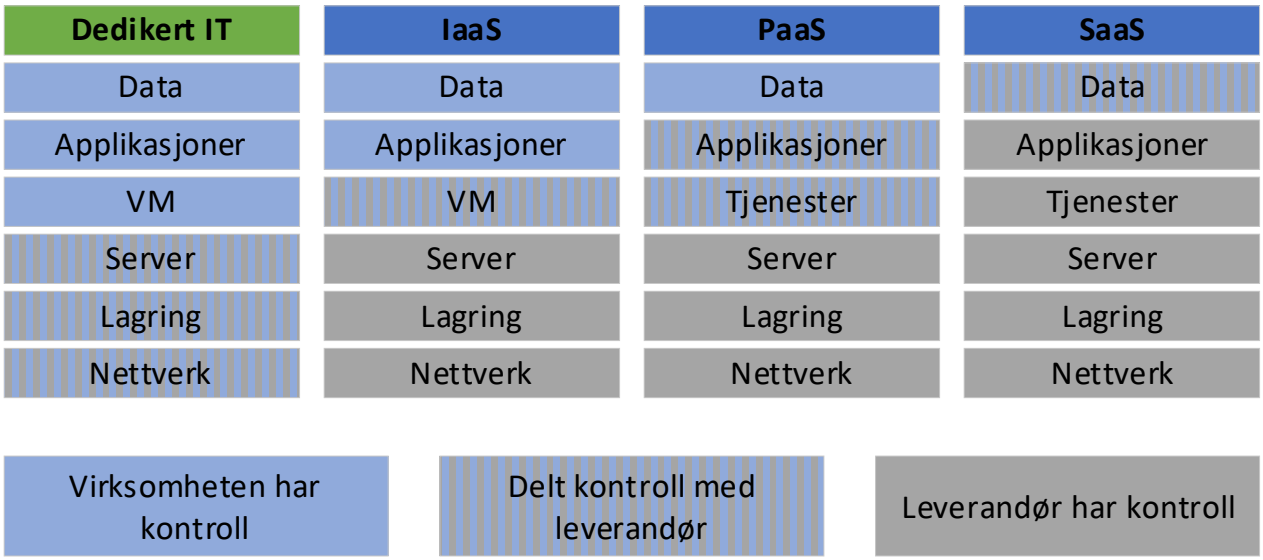
Det er flere konkurrende definisjoner på skytjeneste. Datatilsynet definerer skytjeneste som «en samlebetegnelse på alt fra dataprosessering og datalagring til programvare på servere som er tilgjengelig fra eksterne serverparker tilknyttet internett. Serverparkene kjennetegnes ved at de er laget for dynamisk skalering» /14/.

National Institute of Standards and Technology (NIST) /15/ benytter definisjonen: «Skytjenester (cloud computing) er en modell som gjør det mulig å få tilgang til et sett konfigurerbare dataressurser (for eksempel nettverk, servere, lagring, applikasjoner og tjenester) som er lett tilgjengelige overalt, blir levert og priset etter bruk, kan skaffes raskt og gjøres tilgjengelig med minimalt med administrasjon». NIST sin definisjon benyttes videre i denne veilederen.

NIST deler skytjenester videre inn etter type tjenestemodell og leveransemodell.

3.2 Tjenestemodeller

Skytjenester deles oftest opp i tre forskjellige tjenestemodeller avhengig av hvordan kontrollen deles mellom virksomhet og leverandør.



Figur 1: Sammenligning av tjenestemodeller (Kilde: srmsblog.burtongroup.com)

Infrastruktur som tjeneste (Infrastructure as a Service, IaaS)

Virksomheten kan kontrollere fundamental infrastruktur og har muligheten til å innføre og kjøre vilkårlig programvare. Virksomheten kan kontrollere relevante applikasjoner, servere, operativsystemer, samt i noen tilfeller visse elementer i nettverket (for eksempel brannmur).

Plattform som tjeneste (Platform as a Service, PaaS)

Virksomheten kan innføre egenutviklede eller innkjøpte applikasjoner på leverandørens skyinfrastruktur gjennom å benytte programmeringsspråk og verktøy støttet av leverandøren. Virksomheten kontrollerer ikke den underliggende skyinfrastrukturen, herunder nettverk, servere, operativsystem eller lagringsmuligheter. Virksomheten har kontroll over applikasjoner og i noen tilfeller konfigurasjonsmuligheter for miljøet som applikasjoner kjører i.

Programvare som tjeneste (Software as a Service, SaaS)

Virksomheten benytter applikasjoner som kjører på leverandørens skyinfrastruktur. Virksomheten kan i noen tilfeller kontrollere begrensete kundespesifikke applikasjonsinnstillinger, men kontrollerer ikke den underliggende skyinfrastrukturen, herunder nettverk, servere, operativsystemer eller lagringsmuligheter.

3.3 Leveransemodeller

Skytjenester leveres i forskjellige leveransemodeller basert på hvem skyen gjøres tilgjengelig for.

Privat tilgjengelig sky (Private cloud)

Skytjenesten gjøres tilgjengelig kun for en enkelt virksomhet. Den kan være eid, styrt og driftet av en virksomhet, en tredjepart eller en kombinasjon av dem. Tjenesten kan eksistere internt i virksomheten (on-premise) eller utenfor (off-premise).

Offentlig tilgjengelig sky (Public cloud)

Skytjenesten gjøres tilgjengelig for bruk av allmenheten. Den kan være eid, styrt og driftet av en virksomhet, akademisk institusjon, statlig organisasjon eller en kombinasjon av dem.

Gruppe sky (Community cloud)

Skytjenesten gjøres tilgengelig for en spesifikk gruppe virksomheter som har delte behov (e.g., formål, sikkerhetskrav, policy eller reguleringer). Den kan være eid, styrt og driftet av en eller flere virksomheter i gruppen, en tredjepart eller en kombinasjon av dem. Tjenesten kan eksistere internt i gruppen (on-premise) eller utenfor (off-premise).

Hybrid sky (Hybrid cloud).

Hybrid sky er en sammensetning av to eller flere distinkte leveransemodeller (privat, offentlig eller gruppe).

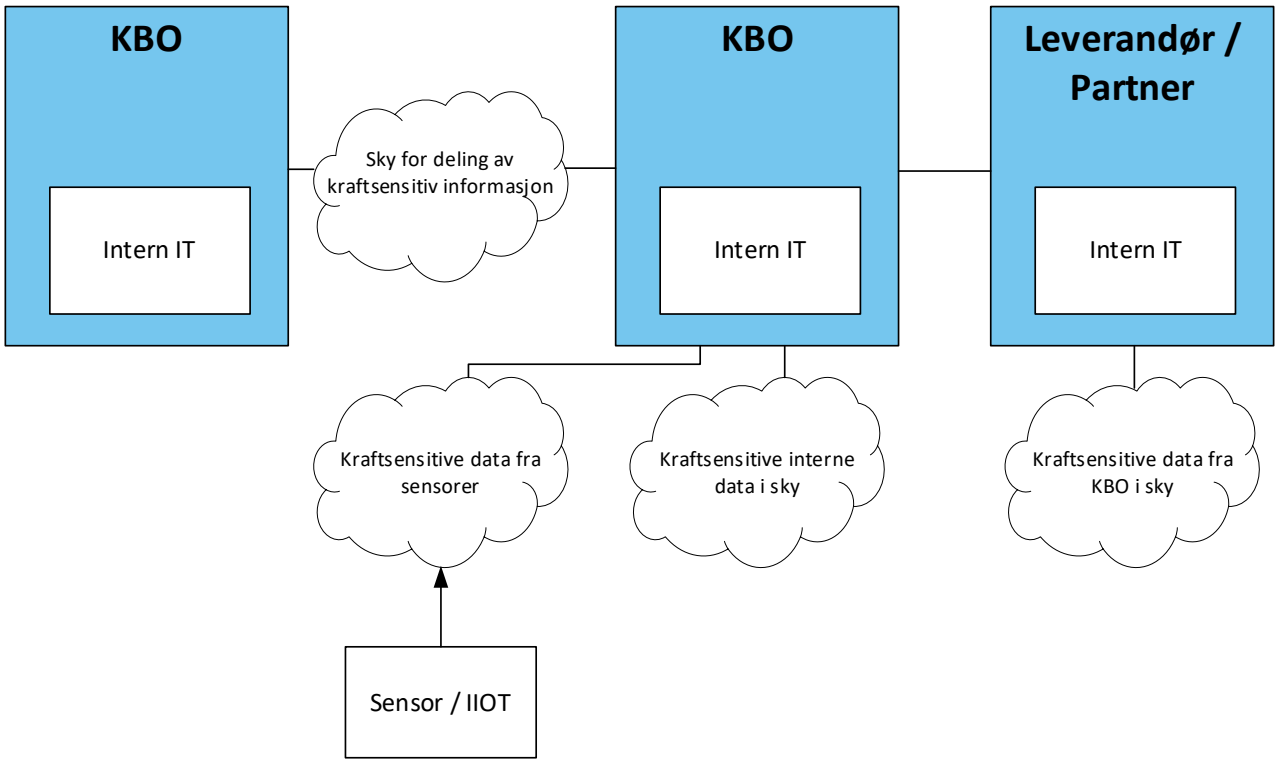
3.4 Multisky (multi cloud) og intersky (inter cloud)

Multisky er bruken av flere skytjenester fra forskjellige leverandører kombinert i en heterogen skyarkitektur. En typisk multisky arkitektur benytter to eller flere offentlige skytjenester fra forskjellige skyleverandører, mulig i kombinasjon med flere private skyer. Multisky skiller seg fra hybrid sky ved at den er en sammensetning av flere skytjenester, i motsetning til hybridsky som er en sammensetning av flere leveransemodeller.

Intersky er et fremtidig konsept for tett koblede skytjenester, inkludert privat, offentlig og hybrid skyer. Intersky inkorporerer flere teknologier for å forbedre interoperabilitet og portabilitet mellom forskjellige skytjenester. Hensikten er å skape sømløs overføring og samhandling av data og applikasjoner mellom forskjellige skytjenester.

3.5 Referansemodell

Figuren viser hvilke bruk av skytjenester som er vektlagt i denne veilederen.



Figur 2: Skytjenester vektlagt i denne veilederen

Under følger noen eksempler fra kraftbransjen på de forskjellige typene skytjenester:

1. Sky for deling av kraftsensitiv informasjon mellom KBO-enheter / partner

Eksempelvis prosjekthotell eller lignende samhandlingsløsninger som benyttes på tvers av forskjellige virksomheter i kraftbransjen. Prosjektene som det samhandles på inneholder ofte kraftsensitiv informasjon. Dette er oftest SaaS applikasjoner som ligger i offentlig sky.

2. Kraftsensitive data fra sensorer

Et eksempel er overvåking av kraftlinjer med sensorer som monteres direkte på linjen. Sensorene henter energi fra magnetfeltet rundt linjen og måler bl.a. strøm, temperatur, helningsvinkel og vibrasjon. Sensordataene overføres over internett til en skytjeneste for å overvåke og analysere data fra kraftlinjene. Slike sensordata behøver ikke være kraftsensitiv informasjon i seg selv, men sammenstilt med annen informasjon kan de gi inngående og spesifikk informasjon om energiforsyningen. Sensorer benytter ofte en offentlig sky med en SaaS applikasjon med et grensesnitt for å lese av eller hente ut målinger.

3. Kraftsensitive interne data i sky

Dette er skytjenester som typisk ligger i den private eller offentlige skyen til en virksomhet. Dette er typisk SaaS applikasjoner som er anskaffet fra spesialiserte leverandører eller applikasjoner som virksomheten selv har utviklet på en PaaS tjeneste. Et eksempel fra kraftbransjen er en skytjeneste for dokumentasjon som brukes som

vedlikeholdssystem for bygninger og oppbevaring av FDV-dokumentasjon. FDV-dokumentasjon for driftssentraler kan være kraftsensitiv informasjon.

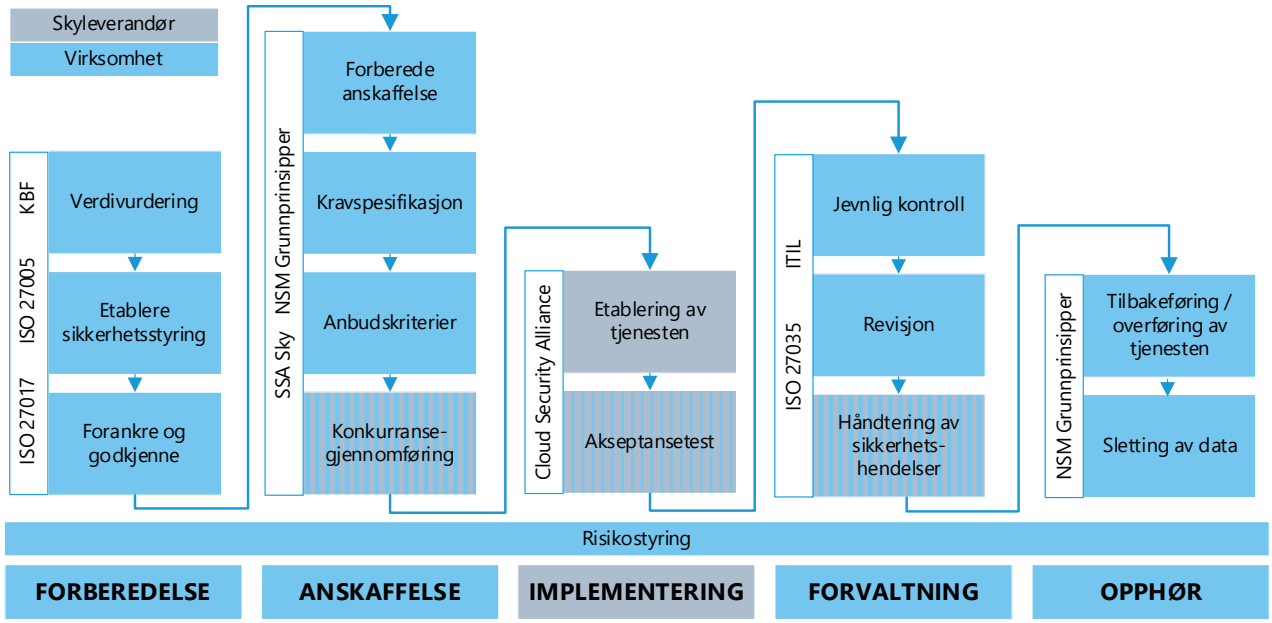
4. Kraftsensitive data fra KBO i sky

Entreprenører for nybygg eller utbedringer av nett og transformatorstasjoner utfører 3D-skanning av bygninger, fjellanlegg, etc. for å kunne tilby en digital tvilling av bygg og anlegg. Den digitale tvillingen blir oppbevart og presentert i en skytjeneste hos leverandør/partner. Detaljert digital tvilling av kraftanlegg kan være kraftsensitiv informasjon. Dette er oftest SaaS applikasjoner som ligger i offentlig- eller gruppesky.

4 LIVSSYKLUS FOR SKYTJENESTER

Figur 3 viser en oversikt over livssyklusen til en skytjeneste. Aktivitetene beskrevet under kan gjøres i ulik rekkefølge og det kan også være nødvendig å gjenta en tidligere aktivitet dersom risikoen ikke anses som akseptabel eller det kommer frem nye momenter underveis i prosessen. Risikostyring er en jevnlig aktivitet som går gjennom hele livssyklusen til skytjenesten.

Livssyklusen er basert på de fire fasene beskrevet i NVEs sjekkliste for IKT-sikkerhet i anskaffelse og tjenesteutsetting i kraftbransjen /7/. Implementering og forvaltningsfasen har i denne veilederen blitt delt i to adskilte deler for å tydelig skille mellom aktiviteter i de forskjellige fasene.



Figur 3 - Livssyklus for skytjeneste

4.1 Risikostyring

Med risikostyring menes å identifisere, vurdere, håndtere og følge opp risikoer som virksomhetens verdier (informasjon, informasjonssystemer, etc.) er eksponert for. Dette gjelder både når virksomheten selv har kontroll over disse verdiene og når de er overlatt i andres varetekt. Risikostyring er derfor en viktig del av virksomhetens styringssystem for informasjonssikkerhet. Det skal være en kontinuerlig prosess som identifiserer og vurderer eksisterende og nye risikoer, etablerer og følger opp tiltak og gir et beslutningsunderlag til risikoeier. Dette gjelder også når virksomheten vurderer å ta i bruk skytjenester.

Virksomheten er *alltid* selv ansvarlig for informasjonssikkerheten ved bruk av skytjenester. For å kunne ivareta dette ansvaret, er det svært viktig at virksomheten ved anskaffelsen av skytjenester innehar nødvendig bestillerkompetanse og stiller passende informasjonssikkerhetskrav, både til selve anskaffelsen og til leverandør av anskaffelsen. For at disse kravene skal være passende, må virksomheten kjenne til hvilken risiko den er eksponert for ved den gjeldende tjenesten. Det er derfor viktig at virksomheten til enhver tid har oppdaterte risikoregistre med oversikt over mulige risikoer i prioritert rekkefølge.

Noen momenter som bør tas hensyn til ved risikostyring av skytjenester er:

- Skytjenester tilgjengeliggjøres via internett og disse grensesnittene og kommunikasjonsprotokoller kan ha sårbarheter

- Datasentre kan ligge utenfor EFTA, EU eller NATO
- Selv om data lagres i EFTA, EU eller NATO, kan drift og support for tjenestene utføres fra andre land (ofte er tjenestene globale dersom man ønsker 24/7 support)
- Leverandørkjedene er komplekse med flere tilknyttede parter
- Lett tilgjengelige tilleggstjenester til standardløsninger kan gi helt andre tjenestevilkår enn standardvilkårene
- De store leverandørene tilbyr kun globale standardvilkår og vil ikke signere individuelle informasjonssikkehetsavtaler eller taushetserklæringer
- Informasjon kan komme på avveie ved tilbakeføring/overføring av skytjenesten
- Tilgjengeligheten til skytjenester kan bli svekket av kommunikasjonssvikt på Internett, etc.
- Beredskapsmyndigheten kan etter energiloven § 9-2 treffe vedtak om at drift i ekstraordinære situasjoner og gjennomføring av tiltak etter dette kapittel skal kunne skje fra norsk territorium.
- Skytjenesters vilkår og funksjonalitet kan være gjenstand for kontinuerlig endring, hvor det ofte er kundens ansvar å holde seg informert om endringene. Dette medfører at nye risikoelementer kan være vanskelige å oppdage og håndtere for kunden. Dette er utfordrende iht. kbf § 6-9 som setter krav til risikovurdering ved systemendringer

For å effektivt håndtere risikoer forbundet med bruk av skytjenester til behandling av kraftsensitiv informasjon eller til forvaltning av forretningskritiske systemer, må virksomheten etablere et langsiktig perspektiv allerede fra oppstart med helhetlig risikostyring gjennom hele anskaffelsens livssyklus.

Risikostyring gjennom de ulike fasene av anskaffelsen utgjør grunnlaget for hvilke tekniske, organisatoriske og personbaserte sikkerhetstiltak virksomheten må kreve at leverandøren implementerer og hvilke sikkerhetstiltak virksomheten selv må implementere. Hva som er å anse som passende sikkerhetstiltak vil avhenge av behovet for beskyttelse til de verdier som eksponeres gjennom skytjenesten, samt hvilke kriterier for risikoaksept virksomheten har fastsatt. Risikostyring er nært knyttet til verdivurdering som dekkes i kapitel 4.2.1.

I tillegg til å ha kompetanse til å håndtere risiko knyttet til bruk av skytjenester, må virksomheten være innforstått med og ha beredskapsplan (kbf § 2-4) for den restrisiko som eksisterer når man overlater verdier i andres varetekt. Det er ikke slik at virksomheten uten videre kan anta at leverandører har gjort alt de har sagt de skal gjøre eller at de har det sikkerhetsnivået de har forpliktet seg til å levere. Selv med robust sikkerhetskompetanse kan både små og store skyleverandører være eksponert for ukjente sårbarheter og trusler, noe virksomheten må hensynta i sin risikostyring.

Hovedpunkter – Risikostyring

Punktene under er basert på metodikk for risikovurdering i ISO 27005 /32/. Andre metodikker som NS 5814:2021 /29/ eller NSM risikovurdering av IKT-systemer /31/ kan også benyttes.

Planlegging (etablere kontekst):

- Risikostrategi som representerer virksomhetens mål.
- Kriterier for evaluering av risiko
  - F.eks. hva som er akseptert risiko og skala for sannsynlighet og konsekvens.
- Rutiner for oppfølging av restrisiko

Risikoidentifisering:

- Identifisere eiendeler
  - Digitale og fysiske
- Identifisere eiere, utøvere, lokasjon og funksjon m.m.
- Identifisere trusler
  - F.eks. fysisk skade, utilsiktet tilgang, teknisk feil, brudd på rutiner m.m.
- Identifisere gjeldende kontroller
- Identifisere sårbarheter
  - F.eks. Prosesser, mennesker, organisasjon, informasjonssystemer, eksterne leverandører m.m.
- Identifisere konsekvenser
  - F.eks. nedetid, økonomi, HMS, tap av renommé, brudd på myndighetskrav m.m.

Risikoanalyse:

- Metode for risikoanalyse (kvantitativ, kvalitativ eller kombinasjon)
- Analyse av konsekvenser
  - Hvilken konsekvens kan risiko ha i forhold til konfidensialitet, integritet og tilgjengelighet,
- Analyse av sannsynlighet
  - Hva er sannsynlighet for at de identifiserte konsekvensene kan oppstå.
- Fastsette nivå for risiko
  - Basert på analysen av konsekvens og sannsynlighet vil man få en kvantitativ, kvalitativ eller kombinert oversikt over nivået på risikoene

Risikoevaluering:

- Liste med risikoer i prioritert rekkefølge i henhold til evalueringskriteriene

Risikobehandling:

- Redusere risiko
  - Gjennomføre tiltak som reduserer sannsynlighet eller konsekvens
- Ta risiko
  - Akseptere risikoen som den er. Forankre aksept i egen virksomhet/ledelse.
- Unngå risiko
  - Avbryte eller endre prosesser som medfører risikoen
- Dele risiko
  - Risikoen deles med andre f.eks. ekstern skyleverandør.
  - Tegne forsikring mot økonomisk risiko

4.2 Forberedelsesfasen

4.2.1 Verdivurdering

Hensikten med å gjennomføre verdivurdering er å identifisere informasjon som skal beskyttes, og hvilken grad av sikringstiltak som er nødvendig å etablere. En verdivurdering av informasjon er et essensielt grunnlag i risikoanalysen, som bidrar til forståelse og oversikt av hva som skal beskyttes, og dermed spisser risikoanalysen.

Verdivurdering krever at informasjonseier utfører en skjønnsmessig vurdering av behovet for beskyttelse for en samling med informasjon. Verdivurdering omhandler blant annet å identifisere hva slags type informasjon det er, presisjonsnivå, mengden informasjon, myndighetskrav informasjonen er underlagt og hvordan informasjonen kan utnyttes av ondsinnede aktører. Det vurderes opp mot konsekvens ved tap av verdiene, og hvilket skadepotensiale det kan medføre for virksomheten dersom informasjonen for eksempel kommer på avveie.

Virksomhetene må være særlig oppmerksomme på hvilken verdi sammenstilling av informasjon kan få når det gjennomføres en verdivurdering. Sammenstilling av informasjon kan føre til at den samlede informasjonsmengden får et større skadepotensial enn enkeltopplysningene. Sammenstilling av ulik informasjon som ellers ikke er verdivurdert til kraftsensitivt kan til sammen kunne gi så spesifikke og inngående opplysninger om kraftforsyningen at den må anses som kraftsensitiv.

Det er derfor viktig å verdivurdere den samlede informasjonsmengden i en skytjeneste. Det vil også være nødvendig å gjøre nye verdivurderinger ved for eksempel utvidelse av en skytjeneste, sammenslåing av flere skytjenester, etc. Virksomhetene må også være observante på risikoen for at deres informasjon kan sammenstilles med informasjon som er utenfor virksomhetens kontroll.

Vedlegg B gir en beskrivelse av sikkerhetsnivåer/skalaer for verdivurdering av informasjon i kraftbransjen. Det er en egen skala for konfidensialitet, integritet og tilgjengelighet for informasjon, hvor kraftsensitiv er et konfidensialitets attributt.

NSMs veileder i verdivurdering av informasjon /16/ gjelder for informasjon underlagt sikkerhetsloven, men flere av elementene i veilederen er relevante også for kraftsensitiv informasjon.

Hovedpunkter – Verdivurdering

- Etabler et rammeverk for verdivurdering. Etabler skala/sikkerhetsnivå for konfidensialitet, integritet og tilgjengelighet.
  - Eksempelvis: Åpen, Intern, Konfidensiell, Sensitiv, Kraftsensitiv.
- Verdivurderingen bør gjennomføres i en eller flere workshops hvor nødvendig kompetanse er samlet innenfor verdivurdering, informasjonssikkerhet og faglig kunnskap om temaet som informasjonen omhandler
- Identifiser mengden, lokasjonen, presisjonsnivået og typen informasjon som skal verdivurderes
- Vurder om informasjonen er kraftsensitiv i henhold til kbf § 6-2 eller underlagt andre myndighetskrav.
  - NVEs veileder til kbf /4/ gir videre retningslinjer for hva som ansees som kraftsensitivt
  - Vurder om sammenstilling av informasjonen kan øke skadepotensialet og derav det nødvendige sikkerhetsnivået
- Beslutt hvilket sikkerhetsnivå som er gjeldende for informasjonen.
  - Se Vedlegg B for eksempler på sikkerhetsnivåer/skalaer som kan benyttes.
- Beslutt hvem som er informasjonseier, kriterier for tilgang og krav til databehandlere.
- Vurder hvor lenge informasjonen har behov for beskyttelse

4.2.2 Etablere sikkerhetsstyring

Kraftberedskapsforskriften § 6-5 setter krav til at det skal iverksettes system og rutiner for å undersøke, og om nødvendig, følge opp at reglene om informasjonssikkerhet og taushetsplikt etterleves /3/. NVE stiller ikke krav til type internkontrollsystem som skal anvendes til dette formålet. I denne veilederen anbefales det at den delen av internkontrollsystemet som omhandler informasjonssikkerhet etableres med grunnlag i anerkjente standarder for sikkerhetsstyring, som for eksempel ISO/IEC 27001 /17/ eller andre rammeverk og veiledere som er utviklet til dette formålet. Eksempler er veiledere fra Digitaliseringsdirektoratet /18/ eller NSM /19/. Videre bør sikkerhetsstyringen integreres med den respektive virksomhetens eksisterende internkontrollsystem og virksomhetsstyringen for øvrig. Styringssystemet må dekke hele infrastrukturen, samtlige skyleverandører, andre leverandører, tjenester, etc.

Under implementering bør virksomheten gjøre seg kjent med**:**

- Hvem som kan påvirkes av uønskede hendelser (hvem skal beskyttes, hvem beskytter, hvem kontrollerer, og hvordan rapportere og forbedre dette)
- Hvilke faktorer som definerer akseptansenivå av uønskede hendelser (vurdere om risiko kan reduseres ved å behandle mindre informasjon eller redusere identifiserbarheten til sårbarhetspunktene på andre vis)
- Formålstjenlige, målbare og forståelige tiltak (Alle tiltak som oppleves kostnadsøkende, begrensende eller uriktige kan virke mot sin hensikt)
- Øving, trening, og opprettholdelse eller økning av kontinuerlig sikkerhetsarbeid. (hvem gjør hva – og når, hvordan sikres personuavhengighet, hvilke manuelle avvik fra rutiner og prosedyrer bør være tilgjengelig ved behov, og hvilke ansvarsmatriser gjelder.)

For å verifisere at styringssystemet fungerer etter hensikt bør kontroller og tiltak fra anerkjente standarder benyttes, eksempelvis ISO/IEC 27002 /11/, ISO/IEC 27017 /12/, NSMs Grunnprinsipper for IKT-sikkerhet /5/ eller lignende. Virksomhetens øverste ledelse skal med planlagte mellomrom gjennomgå styringssystemet for å sørge for at det bidrar til kontinuerlig forbedring ved å planlegge, utføre, kontrollere og forbedre styringssystemet.

Hovedpunkter – Etablere sikkerhetsstyring

Internkontroll-/styringssystems bør være basert på anerkjente standarder som ISO 27001 /17/ og bestå av:

- Styrende (plan) – beskriver virkeområdet for styringssystemet, sikkerhetsinstruks (sikkerhetspolicy) og -strategi, sikkerhetsmål, organisering av sikkerhetsarbeidet, fastsettelse av akseptabelt risikonivå,
- risikostyring, føringer for risikovurderinger, avviksbehandling, o.l.
- Gjennomførende (do) – gir utfyllende opplysninger om ansvar, rutiner, prosedyrer og andre type sikringstiltak som skal gjennomføres i henhold til Styringssystemet.
- Kontrollerende (check) – beskriver kontrollerende aktiviteter for å verifisere at bestemmelsene i styringssystem for informasjonssikkerhet ivaretas og etterleves.
- Korrigerende (act) – gir konkrete fremgangsmåter for forbedring av styringssystemet for å sørge for kontinuerlig forbedring og kontroll.

4.2.3 Forankre og godkjenne

Før overgang til anskaffelsesfasen skal ledelsen i virksomheten forankre og godkjenne anskaffelsen av skytjenesten. Overordnet omfatter dette følgende områder; Identifisere type anskaffelse (støttesystem eller kjernesystem), beskrive hvordan anskaffelsen skal bidra til å nå virksomhetsmålene og definere innhold/produkt anskaffelsen skal resultere i. Ledelsen må videre vurdere risikoen og beslutte eventuell mitigering av risikoen basert på verdi- og risikovurdering av

skytjenester. Merk at verdi- og risikovurdering av skytjenester kan også resultere i at risikoen er for høy til at man kan ta i bruk skytjeneste til det aktuelle formålet.

Interessenter og virksomhetskrav må identifiseres for å sikre at anskaffelsen resulterer i ønsket effekt målt opp mot virksomhetens forretningsmål. Beslutningstakere og virksomhetsledere må involveres i tilstrekkelig grad for å etablere både eierskap og forankring slik at nødvendige mandat og risikoavsetninger etableres. Bestillerkompetanse og fagkompetanse må involveres for å definere anskaffelsesform og planlegge konkurransegjennomføring på overordnet nivå.

En kjent risiko som ofte realiseres er at det legges mye ressurser inn i selve anskaffelsen av en skytjeneste, men få ressurser inn i forvaltningen av tjenesten etter implementering. Dette kan føre til at sikkerhetsnivået til tjenesten forfaller over tid. Virksomheten må identifisere nødvendig ressurser og tilhørende kompetanse som er nødvendig for å forvalte tjenesten på en sikker måte på et tidlig tidspunkt. Kravet til egenkompetanse gjelder gjennom hele livssyklusen til tjenesten.

Energiloven § 9-2.(Beredskapstiltak) sier at «Beredskapsmyndigheten kan treffe vedtak om at drift i ekstraordinære situasjoner og gjennomføring av tiltak etter dette kapittel skal kunne skje fra norsk territorium». Virksomheten må tidlig klargjøre i forhold til krav om å kunne drifte fra norsk territorium under ekstraordinære situasjoner.

Forankringen under forberedende fase skal resultere i et mandat for anskaffelse av skytjenesten med tilhørende aksept av restrisiko identifisert gjennom risikovurdering og ressursallokering.

Hovedpunkter – Forankre og godkjenne

Før overgang til anskaffelsesfasen skal virksomheten:

- Verifisere og avklare behov
- Involvere relevant personell/kompetanse
  - Fagkompetanse
  - Bestillerkompetanse
- Utforme mandat
  - Definere anskaffelsesform
  - Planlegge konkurransegjennomføring på overordet nivå
- Kartlegge og akseptere risikoer
- Planlegge for oppfølging av sikkerhetsstyring
- Godkjenne mandat og vedta anskaffelsen

4.3 Anskaffelsesfasen

NVEs veileder for tjenesteutsetting /6/, NSMs sikkerhetsfaglige anbefalinger ved tjenesteutsetting /10/ og DFØ veileder for skytjenester /8/ kan benyttes som støtte for anskaffelse av skytjenester.

4.3.1 Forberede anskaffelse

Informasjonstyper og behandling

Ved anskaffelse av skytjenester er det viktig å vurdere hvilket formål skytjenesten har og hvilken informasjon som skal lagres og behandles utenfor virksomheten. Se 4.2.1 for verdivurdering. Viktige elementer er hvilken informasjon som skal behandles, hvordan og hvem den skal deles med, levetid, eierskap, de ulike innholdstypene og sammensetningen av informasjonen. Det er virksomhetens ansvar å identifisere hvilke lovverk som gjelder for informasjonen og utarbeide tydelige sikkerhetskrav som er relevante for informasjonen som skal behandles og oppfyller kravene i gjeldende lovverk.

Dette må reguleres gjennom en informasjonssikkerhetsavtale som dekker informasjonen og formål for behandling. Virksomheten må ha kontroll på hele verdikjeden slik at underdatabehandlere som kan ha direkte eller indirekte tilgang kartlegges, beskrives og kontrolleres. Underleverandører må også dekkes av informasjonssikkerhetsavtale.

Valg av informasjonssikkerhetsavtaler blir viktig å utforme slik at disse fanger opp hele aktørbildet, dataflyten, informasjonstypene og ikke minst hvilket ansvar og forpliktelser som reguleres for den behandlingsansvarlige (egen virksomhet) og databehandlere/underdatabehandlere.

Geografisk lokasjon

Kraftberedskapsforskriften § 6-10 setter krav til den geografiske lokasjonen til leverandører som gis tilgang til brytefunksjonalitet i avanserte måle- og styringssystem (AMS) /4/. Utover dette setter ikke kraftberedskapsforskriften kapitel 6 spesifikke krav til den geografiske lokasjonen hvor kraftsensitiv informasjon kan lagres, transporteres og behandles.

Denne veilederen anbefaler at den geografiske lokasjonen for lagring, transport og håndtering av kraftsensitiv informasjon *bør* være innenfor EU, EFTA eller NATO i tråd med NVEs forvaltningspraksis. Dette gjelder også sikkerhetskopier. NVE gir råd om valg av geografisk lokasjon i henhold til trusselvurderinger fra NSM, PST og Etterretningstjenesten, samt praksis i andre myndigheter som Datatilsynet.

Virksomheten må uansett utrede om informasjonsmengden inneholder informasjon som er underlagt andre lovverk enn energiloven og kraftberedskapsforskriften som eksempelvis personopplysninger.

Kontraktstype

Før virksomheten begynner utforming av konkurransegrunnlaget må virksomheten velge relevant kontraktstype og sørge for at sikkerhetsavtalene følger konkurransegrunnlaget. Under følger noen forslag til kontraktstyper:

- SSA-L: Standardiserte skybaserte tjenester som SaaS-applikasjoner /20/
- SSA-SKY: Komplekse skyleveranser, SSA-SKY omfatter både etablering og forvaltning av komplekse skytjenester /21/
- SSA-"lille sky": Beregnet på enklere skyanskaffelser enn det som dekkes av SSA-SKY (under utarbeidelse av DFØ) /21/

De store globale skyleverandørene tilbyr i stor grad kun standardiserte vilkår, se 4.3.2 og 4.3.4 for mer informasjon.

Exit-strategi

Det er viktig å starte planlegging av exit strategi på et tidlig tidspunkt. Virksomheten skal før opphørsfasen vite hvordan dette vil foregå for ulike utløsende faktorer bak opphør (brudd på avtalevilkår, plutselige endringer i pris, endrede behov, konkurs, mv.). Videre må det før opphørsfasen igangsettes være klart hvordan utfasingen skal foregå, hvordan forretningsbehov dekkes, hvordan data håndteres, etc.

Virksomheten må være bevist på kostnadene ved overføring av tjenesten enten til ny skyleverandør eller tilbakeføring til virksomheten. Spesielt må virksomheten ha en klar strategi for:

- Hva kan aksepteres før exit skal iverksettes?

  Ikke akseptable hendelser kan være at skyleverandøren innfører en endring som går imot myndighetskrav, endring i standardavtaler, endringer i underleverandører etc. Det må defineres et punkt (point of no return) hvor det er et klart brudd og exit skal iverksettes.

- Hva er konsekvens av exit?

Virksomheten må ha en god forståelse for hva konsekvensen av exit vil være. Det må forstås hvordan dette påvirker brukere, partnere og kunder. Exit kommer med en kostnad som også må være forstått i forkant av anskaffelsen.

- Hva skjer med data ved en hurtig exit?

  Det må i anskaffelsesfasen etableres klare mekanismer og retningslinjer for sletting av data. Disse retningslinjene bør beskrive hvordan leverandøren sikrer at all data blir slettet og/eller overført ved en hurtig exit.

Virksomhetene må sørge for å ha avtaleverk og prosedyrer som beskriver hvordan data skal tilbakeføres, avhendes og saneres. Dette gjelder både konfigurasjonsdata, og andre informasjonstyper som eies av virksomheten. Ved samarbeid med partnere må det avklares hvordan virksomheten sine data skal kunne skilles fra partneres data etter en exit. Det er ikke gitt at dette er mulig etter data har blitt sammenstilt. Applikasjoner og data bør være løst knyttet til skyplattformen og virksomheten bør tilstrebe en høy grad av portabilitet for å redusere risiko for lock-in med leverandør og forenkle exit.

4.3.2 Kravspesifikasjon

En kravspesifikasjon brukes av virksomheten til å pålegge leverandør de samme krav som virksomheten selv er pålagt gjennom lov og forskrift, samt andre krav som virksomheten vil at leverandør skal oppfylle. Kravspesifikasjonen brukes til å vurdere hvorvidt en leverandør er tilstrekkelig kvalifisert til å levere den konkrete tjenesten og til å stille sikkerhetskrav til selve tjenesten som skal anskaffes.

Kravspesifikasjoner inndeles ofte etter MÅ og BØR krav. MÅ krav er krav som er absolutte kriterier for at leverandør skal kunne levere tjenesten til virksomheten. BØR krav er krav som virksomheten ønsker at leverandør oppfyller, men som ikke er et absolutte kriterier for å kunne levere tjenesten. Et MÅ krav er som oftest utledet fra krav i lov og forskrift som virksomheten må oppfylle. I formuleringen av MÅ krav er det viktig at virksomheten er påpasselig med hvordan kravet formuleres. Dersom kravet i lov eller forskrift er et funksjonskrav, det vil si at det kan oppfylles på ulike måter, må formuleringen av MÅ kravet tilpasses deretter. Virksomheten må altså kunne dokumentere at leverandør oppfyller kravet, men hvordan kravet oppfylles av leverandør er fleksibelt. Målet er at intensjonen bak bestemmelsene i lov og forskrift overholdes.

Eksempel – Skyleverandør vil ikke signere individuell informasjonssikkerhetsavtale

En virksomhet inngår en avtale med en leverandør som innebærer at leverandør behandler kraftsensitiv informasjon på virksomhetens vegne. Når virksomheten gir fra seg kontrollen over denne informasjonen, har virksomheten en plikt til å pålegge leverandør de samme kravene i energiloven og kraftberedskapsforskriften som virksomheten selv er pålagt ved håndtering av kraftsensitiv informasjon. Til dette har NVE utarbeidet maler for sikkerhetsavtale og taushetserklæring som virksomheten kan kreve at leverandør signerer for å oppfylle deler av denne plikten. Imidlertid er det slik at en rekke skyleverandører ikke signerer slike individuelle avtaler med sine kunder, men kun stiller standardvilkår for tjenesten. Der man på forhånd vet at dette vil kunne være tilfellet, er det hensiktsmessig å formulere MÅ kravene slik at man ikke begrenser hvem som kan levere tjenesten når virksomheten faktisk overholder kravet, men på annet vis. Fremfor å stille som MÅ krav at NVEs mal for taushetserklæring signeres, kan det stilles som MÅ krav at personell hos leverandør skal avgi en taushetserklæring overfor leverandøren, som også omfatter den informasjon som leverandør mottar fra virksomheten. Videre, fremfor å stille som MÅ krav at akkurat NVEs mal for sikringsavtale signeres, kan det stilles MÅ krav om at det konkrete innholdet i denne sikringsavtalen skal oppfylles på en måte som sørger for tilsvarende sikkerhetsnivå som malen til NVE er ment å oppnå.

I kravspesifikasjonen er det viktig at virksomheten også tar høyde for at leverandør muligens selv benytter skytjenester i egen virksomhet, eller benytter seg av underleverandører som behandler virksomhetens kraftsensitive informasjon på leverandørs vegne (med eller uten bruk av skytjenester). Dette innebærer blant annet at virksomheten må pålegge leverandør krav om at eventuelle underleverandører, inkludert skyleverandører, som behandler kraftsensitiv informasjon på virksomhetens vegne, pålegges de samme krav som leverandør selv.

Kapitel 5 i denne veilederen består av forslag til krav som kan benyttes inn i en kravspesifikasjon. Kravlisten er basert på:

- Kraftberedskapsforskriften /3/
- DFØ - Krav til informasjonssikkerhet ved kjøp av skytjenester /8/
- NSM Grunnprinsipper for IKT-sikkerhet /5/

Merk at denne kravlisten ikke er uttømmende og standardene/veilederne det henvises til over detaljerer flere tiltak/krav som kan være relevante for virksomheten. I tillegg vises det til ISO 27017 /12/, CSA Cloud Controls Matrix /14/ og CIS Controls Cloud Companion Guide /13/ for flere tiltak/krav.

Hovedpunkter – Konkurransegrunnlag og kravspesifikasjon

- Etabler en prosjektgruppe for utarbeidelse av konkurransegrunnlag og gjennomføring
  - Sørg for tilstrekkelig anskaffelse- og fagkompetanse.
- Identifiser regelverk og myndighetskrav som kan påvirke anskaffelsen, herunder kraftberedskapsforskriften
- Kartlegg behov
  - Vurder forskjellige skytjeneste leveranse- og tjenestemodeller
- Velg en relevant kontraktstype. Typiske eksempler er SSA-L /20/ for SaaS tjenester eller SSA-SKY /21/ for mer komplekse skytjenester
- Inkluder krav til at leverandøren følger alle relevante bestemmelser i kbf.
  - Kapitel 5 gir en ikke uttømmende liste over krav som kan benyttes i anskaffelsen.
  - Hvis leverandøren kun tilbyr standardvilkår må virksomheten forsikre seg om at leverandørens vilkår oppfyller kravene eller anskaffer nødvendig sikkerhetsfunksjonalitet for å oppfylle sikkerhetskrav. Se 4.3.4 for mer informasjon.
- Utarbeid taushetserklæring og informasjonssikkerhetsavtale som også dekker eventuelle underleverandører.
- Inkluder krav til exit-strategi som inkluderer tilbakeføring/overføring/avslutting av skytjenesten, samt forsvarlig sletting av data.

4.3.3 Anbudskriterier

Formålet med å stille kvalifikasjonskrav, er å sikre at leverandørene har tilstrekkelig kompetanse, kapasitet og økonomi til å gjennomføre kontraktsforpliktelsene /8/. Kvalifikasjonskravene gir virksomheten mulighet til tidlig ekskludere leverandører som ikke vil kunne levere nødvendig sikkerhet for skyanskaffelsen. Like viktig som at leverandøren kvalifiseres til å levere på et gitt sikkerhetsnivå er det at produktene eller tjenestene de levere også gir nødvendig sikkerhet.

Kraftberedskapsforskriften § 6-6 pålegger virksomheten en plikt til å bruke begrenset anbudsinnbydelse når det er nødvendig for å forhindre at kraftsensitiv informasjon blir offentlig tilgjengelig gjennom anbudsdokumentene. Se NVE veilederen til kbf for mer utfyllende informasjon rundt denne paragrafen /4/.

Virksomheten må først vurdere om anbudsdokumentene inneholder kraftsensitiv informasjon. Dersom det skal deles kraftsensitiv informasjon i konkurransegjennomføringen må det utføres en prekvalifisering av leverandører (bruk av anskaffelsesformen “begrenset Anbudsinnbydelser”). Leverandører blir prekvalifisert basert på om de oppfyller kvalifikasjonskravene som virksomheten har besluttet og at de i forkant av konkurransen inngår en sikkerhetsavtale med virksomheten. Kun de leverandørene som oppfyller kvalifikasjonskravene og inngår en sikkerhetsavtale blir invitert av virksomheten til å delta i konkurransen og kan gi tilbud.

4.3.4 Konkurransegjennomføring

I gjennomgangen av de mulige leverandørenes oppfyllelse av de spesifiserte krav, vurderer virksomheten både sikkerhetsnivået i leverandørens virksomhet samt sikkerhetsnivået eller -funksjonaliteten i tjenesten som skal anskaffes. Der leverandøren kun tilbyr standardvilkår for informasjonssikkerhet og ikke inngår særavtaler knyttet til informasjonssikkerhet, er det viktig at virksomheten har nødvendig kompetanse til å vurdere hvorvidt vilkårene tilsier at informasjonssikkerhetsnivået hos leverandør oppfyller de spesifiserte informasjonssikkerhetskravene.

For de ulike tjenestene eller produktene som større skyleverandørene tilbyr, er det ulike tilhørende lisenser med tilhørende kvaliteter og sikkerhetsnivå som varierer ut ifra prisnivå. I utvelgelsen av leverandør er det viktig at virksomhetene har nødvendig kompetanse og erfaring til å forstå innholdet i tjenesten eller produktet som skal anskaffes. Ofte tilbyr skyleverandørene et utvalg av valgfri sikkerhetsfunksjonalitet utover standard sikkehetsfunksjonalitet for de ulike tjenestene, som det er viktig at virksomheten vurderer og tar i bruk når det er ansett nødvendig for å oppnå tilstrekkelig sikringsnivå. Eksempler på sikkerhetsfunksjonalitet kan være tilgangskontroll, system for kryptering av sensitiv informasjon og forvaltning av krypteringsnøkler.

Ofte vil skyleverandører være sertifisert i henhold til anerkjente internasjonale standarder for informasjonssikkerhet, som ISO/IEC 27001 /17/, Cloud Security Alliance /14/, etc. Her er det viktig at virksomheten forstår at slik sertifisering ikke er en garanti for at sikkerhetsnivået hos leverandør er av en viss kvalitet, eller at sikkerheten i tjenesten er over en viss standard. En sertifisering er heller ingen garanti for at tjenesten som anskaffes er omfattet av sertifiseringen, så dette er noe virksomheten må spørre leverandør eksplisitt om.

Hovedpunkter – Konkurransegjennomføring

- Sikre nødvendig kompetanse og erfaring til å forstå i dybden innholdet i de ulike tjenestene og produktene som tilbys
- Vurder om standardvilkårene motstrider eller i noen grad avviker fra konkurransegrunnlaget med spesielt fokus på kravene for informasjonssikkerhetsavtale, taushetserklæring, etc.
- Vurder om avvikene gir grunnlag for avvisning grunnet manglende oppfyllelse av krav
    - Risikoen ved avvik må forstås og virksomheten må vurdere om risikoen kan aksepteres.
- Hvis leverandørens standardvilkår avviker fra kbf krav må virksomheten vurdere om kravene kan oppfylles gjennom og for eksempel anskaffe nødvendig sikkerhetsfunksjonalitet som tillegg til tjenesten
- Verifiser at skyleverandøren er sertifisert og benytter for sine tjenester og produkter anerkjente internasjonale standarder som:
    - ISO 27001 /17/
    - ISO 27017 /12/
    - CSA Cloud Controls Matrix /14/

4.4 Implementeringsfasen

4.4.1 Etablering av tjenesten

Virksomheten må ha en klar oversikt og forståelse for hvilke sikkerhetsmekanismer virksomheten forvalter selv og hvilke som forvaltes av leverandør. Ansvar og grensesnitt må være klart avtalt med tydelige skiller mellom kunde og leverandør. Ansvarsfordelingen kan endres i løpet av implementeringsfasen og dette må komme frem i kravstillingen.

Kryptering

Kraftsensitiv informasjon skal være kryptert og dette er en sikkerhetsmekanisme som krever meget klar ansvarsfordeling. Krypteringsnøklene for skytjenesten kan ligge både hos skyleverandøren og/eller virksomheten. Det er flere måter å implementere krypteringsnøkler på i en skytjeneste og de mest vanlige metodene er beskrevet under:

- Bring Your Own Key (BYOK): Virksomheten generer nøkkelen enten direkte i skytjenesten eller generer en lokalt og overfører den til skytjenesten.
- Hold Your Own Key (HYOK): Virksomheten generer en nøkkel lokalt som benyttes for den mest sensitive informasjonen som kun kan benyttes av lokale apper. En annen nøkkel må opprettes for mindre sensitiv informasjon i skytjenesten.
- Double Encryption: Virksomheten generer nøkkelen enten direkte i skytjenesten eller generer en lokalt og overfører den til skytjenesten. Skyleverandøren generere en nøkkel direkte i skytjenesten. Informasjonen krypteres med begge nøklene. Kunden har tilgang til begge nøkler, men skyleverandøren kun har tilgang til en.

Det er viktig å ha en plan for oppbevaring av krypteringsnøkler i relasjon til sikkerhetskopiering av data. Tilgang til krypterte data på en sikkerhetskopi krever tilgang til den krypteringsnøkkelen som ble brukt til krypteringen.

Sikkerhetskopiering

De globale skyleverandørene tilbyr flere forskjellige alternativer for sikkerhetskopiering av data. Virksomheten må vurdere hvilket alternativ som er mest hensiktsmessig for den gitte skytjenesten og virksomheten som en helhet:

- Lokal redundans: Innad i samme datasenter
- Sone-redundans: Fordelt over flere datasenter i samme region
- Geo-redundans: Flere datasenter fordelt på forskjellige regioner

Virksomheten bør i tillegg lagre sikkerhetskopier skjermet fra sitt eget nettverk og skytjenesten (offline backup). Hensikten er å sikre at systemet kan gjenopprettes etter eksempelvis et løsepengevirus som har spredd seg til sikkerhetskopiene gjennom nettverket. Se kbf § 6-8 Sikkerhetskopier.

4.4.2 Akseptansetest

Testing av skytjenesten er kritisk for å sikre at leveransen er i henhold til kontrakt og sikkerhetskrav. Ved testing av en skytjeneste kan det være behov for å teste med en større mengde data. Sensitiv informasjon skal ikke benyttes til testing av tjenester da man på dette punktet ikke har verifisert at løsningen er sikker. Det anbefales å heller benytte syntetiske testdata.

Eksempel – Testdata

Virksomheten har anskaffet en skytjeneste som leverandøren holder på å etablere. Under etableringen er det behov for å gjennomføre en funksjonell test. Skyleverandøren ber virksomheten om å oversende nødvendig data for å gjennomføre testingen.

Virksomheten utfører en risikovurdering og oppdager blant annet at ikke all sikkerhetsfunksjonalitet som er nødvendig for å overholde kraftberedskapsforskriften er aktivert enda. Virksomheten beslutter at det beste alternativet er å lage et sett med syntetiske test data basert på produksjonsdata. Ved å analysere reelle data produserer virksomheten en nytt sett med data som har de samme egenskapene som produksjonsdataen og virksomheten verifiserer at den syntetiske dataen ikke gir spesifikk og inngående opplysninger om kraftforsyningen (jfr. kbf § 6-2). Leverandører mottar deretter den syntetiske dataen og gjennomfører testingen.

Testfasen avsluttes med en akseptansetest. Utover å verifisere akseptansekriteriene som er identifisert for tjenesten skal akseptansetesten i denne konteksten også sikre at implementerte sikkerhetsmekanismer fungerer etter hensikten. Når en akseptansetest for skytjenester skal gjennomføres er det viktig at virksomheten tar høyde for at leverandør og underleverandører er likestilt med virksomheten i henhold til lovverket og hva kommer til behandling, lagring og overføring av kraftsensitiv data.

Hovedpunkter – Akseptansetest

NSMs grunnprinsipper for IKT-sikkerhet /5/ peker på at det burde undersøkes følgende krav som et minimum ved tjenesteutsetting av skytjenester:

Akseptansetest:
Det bør som minimum verifiseres om leverandøren:

- Har et etablert styringssystem for informasjonssikkerhet og eventuelt sertifisering i henhold til internasjonale standarder, for eksempel ISO/IEC 27001:2017
- Gir innsyn i sikkerhetsarkitekturen som benyttes for å levere tjenesten.
- Har utviklingsplaner for fremtidig sikkerhetsfunksjonalitet i tjenestene i tråd med utvikling i teknologi og trusselbildet over tid.
- Har 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.
- Har sikkerhetsfunksjonalitet som tilfredsstiller virksomhetens behov.
- Har sikkerhetsovervåkning for å avdekke sikkerhetshendelser som kan påvirke virksomheten.
- Har rutiner for hendelseshåndtering og avviks- og sikkerhetsrapportering.
- Har krise- og beredskapsplaner som skal harmonisere med virksomhetens egne planer.
- Har godkjenningsprosedyrer for bruk av underleverandører og deres bruk av underleverandører.
- Har spesifisert hvilke aktiviteter som skal utføres ved terminering av kontrakten, blant annet tilbakeføring/flytting/sletting av virksomhetens informasjon.

I tillegg til de styrings- og kontraktbaserte krav skal det også undersøkes om leverandør oppfyller tekniske krav. Disse kravene sørger for at det etableres en sikker IKT-arkitektur og det bør som et minimum ta for seg:

- Funksjonalitet for å styre brukere og kontoer
- Funksjonalitet for å ha kontroll og oversikt på enheter (f.eks. klienter)
- Funksjonalitet for å styre tilgang til ressurser og tjenester
- Funksjonalitet for å ha kontroll på programvare (spesielt på klienter)
- Funksjonalitet som viser at leverandøren har kontroll på programvareleverandørkjenden
- Herding av operativsystemer
- Verktøy for drift og virtualisering av hele eller deler av IKT-arkitekturen («on-prem» og «sky»)
- Nettverksenheter (svitsjer, rutere, aksesspunkter) og brannmurer
- Mekanismer for å håndtere skadevare (antivirus)
- Kryptografiske moduler
- Digitale sertifikater og Public Key Infrastructure (PKI)
- Databaser
- Verktøy for systemovervåkning
- Verktøy for styring av sikkerhetskonfigurasjoner
- Intrusion detection (IDS) og protection (IPS) systemer
- Sikkerhetskopiering og gjenoppretting
- Maskinvare og fastvare (firmware)

4.5 Forvaltningsfasen

4.5.1 Jevnlig kontroll

De store skyleverandørene gjør endringer i eksisterende tjenester og tilfører ny funksjonalitet kontinuerlig. Slike endringer blir ofte automatisk tilgjengeliggjort for kundens sluttbrukere uten at kundens administratorer involveres. Virksomheten må etablere overvåkning og styring for at endringer i skytjenesten identifiseres, evalueres og risikovurderes. Ny eller endret funksjonalitet må konfigureres og tilpasses i henhold til virksomhetens sikkerhetsregime. Brukere og administratorer må få tidlig og tilstrekkelig opplæring.

Virksomheten må sørge for at endringer i skytjenestens avtalevilkår gjennomgås fortløpende og at relevante endringer evalueres og risikovurderes. Samtidig er det en risiko for å må inngå avtaler på nytt med skyleverandør der det allerede er et avtalefestet forhold, grunnet blant annet oppdatering av myndighetskrav som kraftberedskapsforskriften.

Virksomheten må sørge for regelmessig gjennomgang av tredjeparts revisjonsrapporter for skytjenesten og risikovurdere relevante funn. Risikovurderinger av funn i revisjonsrapporter eller endringer i avtalevilkår kan utløse behov for at virksomheten selv etablererer egne risikoreduserende tiltak. Virksomheten bør angi en toleransegrense for risiko ved bruk av skytjenesten, samt opprette en plan for tilbakeføring/overføring/avslutning dersom risikonivået for skytjenesten overskrider satt toleransegrense.

Forvaltning av sikkerhetskontrollene i skytjenesten er en jevnlig prosess og det er viktig at virksomheten inkluderer informasjonssikkerhet i den overordene forvaltningen av skytjenesten. Nye sårbarheter og trusler som blir kjent kan føre til at det er nødvendig å innføre eller endre kontroller.

Hovedpunkter – Jevnlig kontroll

Bruk av skytjenester til behandling av kraftsensitiv informasjon innebærer at virksomheten har en plikt til og jevnlig kontrollere at leverandøren etterlever kravene til informasjonssikkerhet. Det finnes flere verktøy og sjekklister som kan være til hjelp ved kontroll av skytjenesteleverandører:

- Bruk av sikkerhetskontrollene i ISO 27001 /17/.
- Bruk av CSAs sjekkliste /14/. Cloud Security Alliance (CSA) har utarbeidet Cloud Controls Matrix (CCM), en sjekkliste for å vurdere sikkerhetsrisiko forbundet med skyleverandører.
- Gjennomgang av logger fra skyleverandøren.
- Gjennomgang av resultater fra sikkerhetsrevisjoner.
- Gjennomgang av rapporter for avvikshåndtering og endringsstyring.
- Aktiv styring av risiko

Et styringssystem for informasjonssikkerhet bør benyttes for å sikre at arbeidet med oppfølging av skytjenesteleverandører blir en kontinuerlig prosess og ivaretatt på en systematisk og dokumentert måte.

4.5.2 Revisjon

Kraftberedskapsforskriften § 6-9 bokstav f setter krav til at «Virksomheter skal jevnlig gjennomføre revisjoner av iverksatte sikringstiltak for digitale informasjonssystemer» /3/. Gjennomføring av revisjon vil variere basert på interne rutiner hos de forskjellige virksomhetene, men det er anbefalt å benytte anerkjente standarder og metodikk for revisjon.

I kontekst av skytjenester må virksomheten påse at revisjon omfatter både virksomhetens egne sikringstiltak og de tiltak som skyleverandøren har ansvar for. Revisjon må tilpasses den aktuelle ansvarsfordelingen i henhold til de ulike leveransemodellene (IaaS, PaaS eller SaaS) og gjeldende tjenesteavtaler. Etter hvert som virksomheter øker sin bruk av skytjenester er det naturlig at flere av de ovennevnte leveransemodellene er i bruk for ulike tjenester.

De fleste store skyplattformer tilbyr verktøy og tjenester som kan være til nytte i virksomhetens revisjon av egne sikringstiltak, som eksempelvis sikkerhetsportaler med innsikt i relevante konfigurasjoner og sårbarheter med tilhørende forslag til utbedring. Verktøyene har ofte funksjonalitet for sammenligning av gjeldende konfigurasjon mot anerkjente sikkerhetsstandarder. Slike verktøy kan være til stor nytte, men det presiseres at de ikke vil kunne avdekke alle forhold og at virksomheten derfor må sørge for at alle iverksatte sikringstiltak fra risikostyringsprosessen revideres.

Det kan være en utfordring å gjennomføre revisjoner hos store globale skyleverandører med virksomhetens egne revisorer. Skyleverandøren gir derimot ofte tilgang til revisjonsrapporter fra revisjoner de har selv utført med tredjeparts revisorer. Revisjon av leverandøren som tjenestetilbyder kan gjennomføres med gjennomgang av tredjeparts revisjonsrapporter.

Eksempel – Revisjon

En virksomhet skal gjennomføre revisjon av en skytjeneste de benytter. Tjenesten er SaaS-basert samhandlingstjeneste fra en stor skytjenesteleverandør.

Revisor henter frem virksomhetens risikovurdering av tjenesten. Hun gjennomgår identifiserte risikoer og tiltak og påser at disse samsvarer med den ansvarsfordelingen mellom virksomheten og leverandøren som er definert i tjenesteavtalen.

Revisor gjennomgår de tiltak virksomheten selv skal ha implementert, og undersøker at disse fungerer etter sin hensikt. For eksempel kan det være å undersøke at virksomhetens prosess for tilgangsstyring fungerer, at multi-faktor autentisering er aktivert for alle brukere, at brukerne klassifiserer og merker kraftsensitive data, at virksomheten følger opp informasjon og varsler fra leverandøren, at brukernes mulighet til å dele informasjon med eksterne parter er riktig konfigurert, etc. Revisor benytter også tjenestens sikkerhetsportal til å få innsikt i eventuelle øvrige sårbarheter som virksomheten selv må følge opp.

Videre ber revisor leverandøren om innsyn i revisjonsrapport utført av tredjepart. Hun undersøker så om virksomheten selv har implementert tiltak som kan mitigere eventuelle sårbarheter som er påpekt i tredjepartsrapporten, eller om det finnes sårbarheter av en slik karakter at virksomheten bør iverksette sin tilbakeføringsplan.

Hovedpunkter – Revisjon

Virksomhetene må sørge for å:

- Planlegge, etablere, implementere og vedlikeholde revisjonsprogram(mer), herunder frekvens, metoder, ansvar, krav til planlegging og rapportering. Revisjon skal ta hensyn til hvor viktige de aktuelle prosessene er, og resultatene av tidligere revisjoner.
- Definere revisjonskriteriene og omfanget for hver revisjon.
- Velge revisorer og gjennomføre revisjoner som sikrer objektivitet og upartiskhet i revisjonsprosessen.
    - Som oftest er virksomheten begrenset til å gjennomgå tredjeparts revisjonsrapport fra skyleverandøren og bør i tillegg revidere egne sikringstiltak som f.eks. interne prosesser, tilgangsstyring, tjenestekonfigurasjoner, logger, etc.
- Sørge for at resultatene av revisjonene rapporteres til relevant ledelse.
- Oppbevare dokumentert informasjon som bevis på planlagte revisjoner og resultatene fra tidligere revisjoner.

4.5.3 Håndtering av sikkerhetshendelser

Kraftberedskapsforskriften 6-9 bokstav d setter krav til at «Virksomheter skal håndtere uønskede hendelser i sine digitale informasjonssystemer og gjenopprette normaltilstand uten ugrunnet opphold» /3/. Virksomheten skal planlegge og forberede prosedyrer for håndtering av sikkerhetshendelser, inkludert rapportering, ansvarslinjer og eskalerings- og varslingsrutiner. Det skal implementeres tiltak for deteksjon og identifikasjon av sikkerhetshendelser.

Dokumenterte planverk for håndtering av sikkerhetshendelser bør inneholde informasjon som gir rask tilgang til informasjon om topologi, systemer, integrasjoner og endepunkter, samt en plan for stopp og isolasjon av tjenester ved f.eks. spredning av løsepengevirus, skadevare eller annet. Virksomheten må inkludere leverandør i planverket, med tydelig definerte roller og ansvar samt relevant kontaktinformasjon. Planverket skal være lett tilgjengelig, gjerne i papirform.

Virksomheten og leverandør må utarbeide en felles plan for hvordan de skal samhandle når en sikkerhetshendelse inntreffer. Det er viktig med en plan som har klart fordelte roller og ansvarsområder. Underleverandører bør inkluderes i planleggingen.

Virksomheten må sørge for å tildele ansvar og roller for hvem som skal håndtere sikkerhetshendelser før disse inntreffer. Virksomheten må sørge for å ha kompetanse om systemer og kunne vurdere alvorlighetsgrad, omfang og konsekvenser på overordnet nivå for disse.

Virksomheten skal oppbevare dokumentert informasjon som bevis på sikkerhetshendelsens art og eventuelle tiltak som blir truffet som følge av dem, samt resultatene av eventuelle korrigerende tiltak. Det oppfordres til åpenhet om sikkerhetshendelser som har påvirket virksomheten, da dette kan bidra til å øke fokuset på tematikken, samt kompetansebygging i relevante risikomiljø.

Hovedpunkter – Håndtering av sikkerhetshendelse

Basert på NSMs Rammeverk for håndtering av IKT-sikkerhetshendelser /30/, skal virksomheten når en sikkerhetshendelse inntreffer:

- **Detektere og vurdere omfang og alvorlighetsgrad**
  - Hva har skjedd? (f.eks. data på avveie, data er slettet, data er endret)
  - Hvilke systemer er påvirket?
  - Hvilken type data og mengde er påvirket?
- **Krav til varsling av relevante parter hvis kraftsensitiv data på avveie**
  - NVE skal varsles uten ugrunnet opphold etter krav i kraftberedskapsforskriften § 2-5.Varsling. Virksomheten skal sende rapport til NVE innen tre uker /3/.
  - Beredskapsmyndigheten NVE har gitt råd om å varsle KraftCERT
- **Iverksette prosesser og tiltak for håndtering av hendelsen**
  - Isolere berørte systemer
  - Sikre bevis fra hendelsen
  - Fjerning av skadevare og gjenoppretting av sikkerhetskopier (se 4.6.1)
- **Tilbakeføring og læring av hendelsen**
  - Systemet tilbakeføres til samme/tilsvarende tilstand som før hendelsen
  - Ledelsen gjennomgår hendelsen
  - Analysere hendelsen og iverksette tiltak for å hindre lignende hendelser i fremtiden

4.6 Opphørsfasen

Trinnene i opphørsfasen skal planlegges allerede i anskaffelsesfasen, slik at virksomheten har redusert risikoen for å støte på forhold som vanskeliggjør opphør på ønsket tidspunkt og måte. Se 4.3.1 for mer informasjon.

NVEs sjekkliste /6/ peker på at behovet for strengere overvåkning og tilgangsstyring skal vurderes under opphørsfasen.

4.6.1 Tilbakeføring eller overføring av tjenesten

Virksomheten må først vurdere om tjenesten er i stand til å overføres eller om den må endres eller bygges på nytt. Ved overføring eller tilbakeføring av en skytjeneste må virksomheten ha en plan for overføring av kryptert informasjon. Dette gjelder også i det tilfelle hvor virksomheten skal bytte system eller produkt. Dersom skyleverandøren forvalter krypteringsnøklene, må planen beskrive enten hvordan data kan flyttes i kryptert form eller hvordan klartekst data skal beskyttes under overføringen. Kraftsensitiv informasjonen skal være beskyttet både i ro og i transitt. Virksomhetens system for forvaltning av krypteringsnøkler må oppdateres med de nye nøklene og eventuelt utgåtte nøkler.

Ved skifte av nøkler må virksomheten forsikre seg om at data fortsatt kan benyttes etter overføring og leverandørskifte. Nye sikkerhetskopier må umiddelbart tas ved import til ny skyleverandør. I mange sammenhenger vil virksomheten ha et behov for å spare på eldre sikkerhetskopier samt de nøklene som ble brukt. Dette gjelder også for offsite/offline sikkerhetskopiering.

Etter at tjenesten har blitt overført må virksomheten forsikre seg om at informasjon hos tidligere leverandør er slettet. Se 4.6.2 for mer informasjon angående sletting av data.

Hovedpunkter – Tilbakeføring eller overføring av tjenesten

- Vurder behovet for strengere overvåkning og tilgangsstyring i opphørsfasen
- Vurder om virksomheten selv eller ny leverandør innehar nødvendig kompetanse til å ivareta virksomhetens interesser, inklusive sikkerheten.
- Sikre kompetanseoverføring fra gammel til ny leverandør eller virksomheten selv. Dette bør være en del av kontrakten.
- Planlegg og iverksett tilbakeføring av tjenesten til virksomheten eller overføring av tjenesten til ny leverandør. Sikkerheten til data som overføres må også bli ivaretatt.
- Iverksett plan for at data tilhørende virksomheten blir forsvarlig slettet av tidligere leverandør. Se 4.6.2.

4.6.2 Sletting av data

Virksomheten må gjennomgå prosedyren hos skyleverandøren for sletting av data for å forsikre seg om at all informasjon, inkludert sikkerhetskopier, replikerte data og mellomlagrede (cache) data, vil bli slettet ved avslutning av tjenesten. Virksomheten må være bevist på at det er utfordrende å etterprøve leverandørenes sletting- og destruksjonsmekanismer i avanserte IKT systemer som drifter dagens skytjenester. Etter at sletting er utført må virksomheten be om en slettebekreftelse fra leverandør som bekrefter at sletting er utført og dokumenterer hva som er slettet, hvordan det er slettet og hvor det er slettet fra.

Hovedpunkter – Sletting av data

- Gjennomgå leverandøren sin prosedyre for sletting av data og verifiser at prosedyren er tilstrekkelig for å sørge for at informasjonen ikke kan gjenopprettes eller komme på avveie.
- Identifiser alle steder hvor virksomhetens informasjon er lagret hos skyleverandøren, inkludert sikkerhetskopier, replikerte data og mellomlagrede (cache) data.
- Iverksett plan for forsvarlig sletting av data tilhørende virksomheten med skyleverandøren
- Verifiser med leverandør at all informasjon har blitt slettet.
- Motta bekreftelse fra leverandør på at all informasjon har blitt slettet

5 KRAVLISTE TIL SKYLEVERANDØR

Kravlisten er et utgangspunkt for krav virksomheten kan stille til skyleverandører. Det er viktig at virksomhetene tilpasser kravene basert på blant annet hva slags skytjeneste som skal anskaffes, egen organisasjon, skyleverandøren og hva slags informasjon som skal lagres og prosesseres. Kravlisten kan også benyttes for å evaluere eksisterende skytjenester.

Kravlisten er basert på krav fra Kraftberedskapsforskriften /3/, DFØ - Krav til informasjonssikkerhet ved kjøp av skytjenester /8/ og NSM Grunnprinsipper for IKT-sikkerhet /5/.

5.1 Styringssystem for informasjonssikkerhet

Krav

Leverandøren må bekrefte at styring og kontroll av informasjonssikkerheten i skytjenesten har en helhetlig tilnærming, blir kontinuerlig forbedret og tilfredsstiller kravene i ISO 27001 eller tilsvarende og at dette kan dokumenteres gjennom tredjepartsrapportering.

Dokumentasjonskrav

Legg ved dokumentasjon på etterlevelse av kravet, for eksempel gyldig ISO 27001 sertifikat eller tilsvarende. Beskriv hvordan styringssystemet er implementert og hvordan Leverandør og underleverandører følger opp styringssystemet. Bekreft at det kan dokumenteres god internkontroll gjennom tredjepartsrapportering i kontraktsperioden. Legg ved eksempel på siste revisjonsrapport eller attester som bekrefter dette.

Veiledning

Virksomheten må forsikre seg om at sertifiseringen gjelder for tjenesten eller den delen av leverandøren som leverer tjenesten. Det skal stå i sertifikatet hva som er dekket.

Det anbefales i tillegg å sjekke hvilke andre standarder, veiledere og beste praksis leverandør sin virksomhet, tjenester og produkter følger. Eksempelvis bør skyleverandør vise til at de levere tjenester/produkter som er sikret og herdet i henhold til CIS Controls /13/, ISO 27017 /17/ eller CSA Cloud Security Matrix /14/.

Kobling til standarder og myndighetskrav

- DFØ - Krav til informasjonssikkerhet ved kjøp av skytjenester – Krav til styringssystem for informasjonssikkerhet
- Energiloven § 9-3 Informasjonssikkerhet
- Kraftberedskapsforskriften § 6-9. Digitale informasjonssystemer
- Kraftberedskapsforskriften § 6-5. Anskaffelser
- Kraftberedskapsforskriften § 2-10 Internkontroll

5.2 Trussel- og sårbarhetsvurderinger

Krav

Leverandøren skal ha en løpende prosess for å identifisere, vurdere og prioritere trusselbildet for den leverte tjenesten. Det skal også arbeides aktivt og risikobasert for å begrense sårbarheter.

Dokumentasjonskrav

Beskriv prosessen for trussel- og sårbarhetsvurderinger. Prosessen skal omfatte eventuelle underleverandører som leverandør benytter i sin leveranse til Kunden. Beskriv også hvordan risikoer og sårbarheter håndteres, og hvilke prosedyrer med tidsrammer som brukes for de ulike typer av sårbarheter.

Veiledning

Virksomheten og leverandøren må begge ha et aktivt forhold til risiko, da trusselbildet endrer seg kontinuerlig. Nye trusler og sårbarheter må identifiseres og vurderes kontinuerlig. Leverandør må ha rutiner for sikre at det iverksettes relevante tiltak i henhold til det gjeldende trusselbildet.

Virksomheten bør vurdere å inkludere krav om dokumentasjon av håndtering av sårbarheter i programvareleverandørkjeden (tredjepartsprogramvare).

Kobling til standarder og myndighetskrav

- DFØ - Krav til informasjonssikkerhet ved kjøp av skytjenester – R1 - Trussel- og sårbarhetsvurderinger

5.3 Portabilitet

Krav

Data i løsningen skal lagres på relevant standard format. Med dette menes anerkjente standarder som benyttes av flere aktører, og forvaltes industrielt. Eksempler på slike formater kan være (men ikke begrenset til) CIM, XML, CSV og lignende. Informasjonen i løsningen skal kunne eksporteres, deles, eller på annet vis anvendes i andre lignende systemer uten behov for konvertering eller annen manipulasjon av dataformatet.

Utveksling av data mellom løsningens komponenter, med andre løsninger, eller tredjeparts løsninger skal benytte åpne og standardiserte grensesnitt (som eksempelvis API) uten behov for spesialtilpasninger eller ytterligere tilpasninger i systemarkitektur eller datamodeller.

Løsningsarkitekturen skal være av slik karakter at en eller flere moduler eller funksjoner kan byttes ut, erstattes, eller på annet vis komplementeres ut fra Kundens behovsendringer. Løsningen skal gi Kunden mulighet til å flytte funksjoner ut av fra løsningen, eller legge til ny funksjonalitet i løsningen. Med funksjonalitet menes enkeltfunksjoner, eller logiske moduler som dekker et definert behandlingsformål.

Ved terminering av kontrakt må alle Kundens data utleveres, på et egnet format, til Kunden eller tredjepart utpekt av Kunden innen 30 dager etter avtaleperiodens slutt.

Dokumentasjonskrav

Beskriv prosessen for utlevering av data og sletting etter at Kunden har bekreftet å ha mottatt dataene. Beskriv datastrukturer, formater og hvordan dataene er organisert og knyttet sammen.

Veiledning

DFØ /8/ beskriver noen tiltak som virksomheten kan gjøre for å redusere risiko for leverandøravhengighet og forenkle exit:

- **Design applikasjoner frikoblet fra skyplattform:** Skyapplikasjonskomponenter bør være så løst knyttet som mulig til applikasjonskomponentene som samhandler med dem. Dette øker fleksibiliteten.
- **Sørg for høy portabilitet av data:** Unngå proprietær formatering for å maksimere portabiliteten til dine data. Beskriv datamodeller så tydelig som mulig ved å bruke skjemastandarder. I tillegg bør virksomheten sørge for at skyleverandøren tilbyr en måte å trekke ut data enkelt og rimelig.
- **Vurder multi-sky strategi:** Virksomheten kan for eksempel benytte en leverandør til prosessering og en annen for datavarehuset og en tredje til kunstige intelligens. Multi-sky kan føre til at virksomheten blir mindre avhengig av en leverandør for alle behov.
- C**ontainerteknologi:** Containerteknologi levert av ulike tilbydere bidrar til å fjerne avhengigheter til skyleverandørene. De fleste skyleverandører støtter standard containerformat, som gjør det enklere å overføre applikasjoner til ny skyleverandør om nødvendig.

Bruk av multisky medfører oftest en økt arbeidsmengde for virksomheten på grunn av at det vil være nødvendig å gjennomføre blant annet flere risikovurderinger, følge opp flere sikkerhetstiltak og forvalte flere sikkerhetsavtaler.

Kobling til standarder og myndighetskrav

- DFØ - Krav til informasjonssikkerhet ved kjøp av skytjenester – R2 – Lock-in

5.4 Datasenterets sikkerhet

Krav

Leverandør skal forhindre uautorisert fysisk adgang til sine datasenter samt beskytte mot tyveri, skade, tap og at utstyr svikter for å sikre kontinuerlig drift.

Dokumentasjonskrav

Beskriv hvilke fysiske sikringstiltak som benyttes i de datasenter som brukes for å levere tjenesten slik at uvedkommende ikke får adgang til data, systemer og utstyr.

Veiledning

Manglende fysisk sikring av datasenteret kan føre til at uautoriserte får adgang til data, systemer og utstyr.

Kobling til standarder og myndighetskrav

- DFØ - Krav til informasjonssikkerhet ved kjøp av skytjenester – R4 – Datasenterets sikkerhet

5.5 Separasjon mellom kunder

Krav

Leverandøren må ha iverksatt tilstrekkelige tiltak for å segmentere data, applikasjoner (fysiske og virtuelle), infrastruktur og nettverk mellom forskjellige kunder for å begrense en kundes tilgang til andre kunders ressurser. Leverandøren må skille kundens applikasjoner og data fra andre kunder.

Dokumentasjonskrav

Beskriv tiltak for å segmentere data, applikasjoner (fysiske og virtuelle), infrastruktur og nettverk mellom forskjellige kunder og hvordan denne separasjonen kan kontrolleres.

Veiledning

Det er viktig at leverandør har implementert en sterk separasjon mellom forskjellige kunder. Separasjon sørger for at en kunde sin skytjeneste ikke påvirker eller kompromitterer en annen kundes skytjeneste eller informasjon. Separasjon kan implementeres på forskjellige nivåer i skytjenesten, både logisk og fysisk. Virksomheten bør verifisere at skyleverandøren følger beste praksis for separasjon.

Skyleverandører vil oftest ha fellesløsninger for flere kunder som for eksempel identitet- og tilgangsstyring, drift av skyløsningene og andre felleskomponenter. Dette er gjeldende selv om kundenes data er separert og virksomheten må vurdere om leverandøren har iverksatt tilstrekkelig tiltak for å begrense påvirkningen fellesløsninger kan ha på virksomheten sine ressurser.

Kobling til standarder og myndighetskrav

- DFØ - Krav til informasjonssikkerhet ved kjøp av skytjenester – R6 – Seperasjon mellom kunder

5.6 Sikkerhetskopi

Krav

Leverandøren må sikre tilgjengelighet og gjenoppretting av kundens data og tjenester. Kundedata i tjenesten må sikkerhetskopieres og sikkerhetskopiene må sikres.

Dokumentasjonskrav

Beskriv rutiner for sikkerhetskopiering, inkludert rutiner for tilgang til disse. Beskriv hvordan sikkerhetskopiene er beskyttet og oppbevart.

Veiledning

Sikkerhetskopier er nødvendig for å kunne gjenopprette systemer etter en hendelse som eksempelvis løsepengevirus angrep. I henhold til NSM /5/ bør leverandøren og virksomheten utarbeide planer og rutiner som et minimum beskriver:

- Hvilke data som skal sikkerhetskopieres.
- Regelmessighet på sikkerhetskopiering av ulike data, basert på verdi.
- Ansvar for sikkerhetskopiering av ulike data.
- Prosedyrer ved feilet sikkerhetskopiering.
- Oppbevaringsperiode for sikkerhetskopier.
- Logiske og fysiske krav til sikring av sikkerhetskopier.
- Krav til gjenopprettingstid for virksomhetens ulike systemer og data
- Godkjenningsansvarlig(e) for planen.

Virksomheten bør vurdere offline backup for å sikre at systemet kan gjenopprettes hvis sikkerhetskopier tilknyttet nettverket blir utsatt for skadevare som løsepengevirus.

Kobling til standarder og myndighetskrav

- NSM Grunnprinsipper - 2.9.1 - Legg en plan for regelmessig sikkerhetskopiering av alle virksomhetsdata
- Kraftberedskapsforskriften § 6-8. Sikkerhetskopier

5.7 Sletting av data

Krav

Leverandøren må kunne dokumentere hvordan data slettes og hvordan det sikres at slettede data ikke kommer på avveie eller kan gjenskapes. Kravet gjelder også for sikkerhetskopierte, replikerte og/eller mellomlagrede (cache) data, samt for eventuelle underleverandører som benyttes.

Dokumentasjonskrav

Beskriv hvordan data slettes og at det sikres at data som er slettet ikke blir tilgjengelig for andre eller kan gjenskapes. Beskriv også hvordan det sikres at slettede data ikke blir tilgjengelig ved utskifting og fornyelse av infrastruktur.

Veiledning

Ved overføring eller avslutning av en skytjeneste er det kritisk at virksomheten har kontroll på informasjonen som har vært lagret hos skyleverandøren. Det er en risiko for at data kommer på avveie eller kan gjenskapes hvis det ikke slettes på en sikker måte.

Det er flere forskjellige måter å slette dataen på og valg av metode bør gjenspeile verdien til informasjonen som har vært lagret. Virksomheten må være bevist på at det er svært utfordrende å etterprøve leverandørenes sletting- og destruksjonsmekanismer i avanserte IKT systemer som drifter dagens skytjenester.

Kobling til standarder og myndighetskrav

- DFØ - Krav til informasjonssikkerhet ved kjøp av skytjenester – R7 – Sletting av data

5.8 Endringshåndtering

Krav

Alle endringer som kan påvirke tjenestens sikkerhet må identifiseres og håndteres for å hindre utilsiktede hendelser.

Dokumentasjonskrav

Beskriv leverandørens prosess for å håndtere endringer, for eksempel ihht. rammeverket ITIL. Dette gjelder både utvikling, nyanskaffelser og utskifting av applikasjoner, integrasjoner, infrastruktur, nettverk og systemkomponenter. Beskriv hvordan uautoriserte endringer kan oppdages.

Veiledning

De store globale skyleverandørene gjør kontinuerlig endringer i tjenestene sine og publiserer dette eksempelvis i nyhetsbrev, oppdateringsnotater eller lignende. Som oftest opplyses ikke virksomheten om dette direkte og virksomheten må dermed sørge for at de har en prosess for å følge opp de endringene som skyleverandøren gjør i sine tjenester. Virksomheten må også følge med på endringene skyleverandøren gjør i sine tjenester for å vurdere om endringene vil få negative konsekvenser for tjenesten som er satt ut.

Kobling til standarder og myndighetskrav

- DFØ - Krav til informasjonssikkerhet ved kjøp av skytjenester – R9 – Endringshåndtering

5.9 Sporbarhet

Krav

Alle handlinger må logges. Logging skal være på både bruk og drift av tjenesten. Dette gjelder for Kundens brukere, leverandør og ev. underleverandører. Loggene må være sikret og overvåket i forhold til manipulasjon og sletting.

Kunden må ha tilgang til loggene etter behov. Sikkerhetslogger må kunne overføres til kunden kontinuerlig på et strukturert format.

Logger må oppbevares så lenge de har verdi for etterforskning av en hendelse, minimum to år.

Dokumentasjonskrav

Loggen skal f.eks. inneholde brukeraktiviteter (bl.a aksess, lokasjon, lesing/skriving/sletting/endring av data og mengde), feil og avvik. Beskriv hvordan og på hvilket detaljnivå handlinger som kan endre eller eksponere data logges, og hvordan loggene sikres mot manipulasjon.

Beskriv hvordan kunden får tilgang til disse loggene. Leverandøren bes også om å beskrive hvordan sikkerhetslogger, alarmer og advarsler kan integreres med Kundens egen sentrale sikkerhetsovervåkingsløsning.

Veiledning

Leverandøren kan overlagt eller utilsiktet utføre handlinger som skader integriteten, konfidensialiteten eller tilgjengeligheten til virksomhetens tjenester og data. Eksempler på dette er spionasje, inkonsistente databasedumper, overføring av data til lavere sikkerhetsnivå, feil konfigurering, etc.

Skytjenesten skal være designet slik at brukere hos leverandøren ikke kan omgå loggingen eller manipulere loggene. Dette gjelder også for administratorer hos leverandøren. Virksomheten bør undersøke med leverandøren hvordan de forhindrer at en utro tjener med administrator rettigheter misbruker sin stilling og skader virksomheten. Det er fordelaktig å integrere loggene fra skyleverandøren med virksomhetens egen sikkerhetsovervåkningsløsning.

Det bør være implementert varslings- og loggmekanismer også for maskinvare. All tilgang og modifikasjon av maskinvare bør logges i leverandørens loggsystem.

Kobling til standarder og myndighetskrav

- DFØ - Krav til informasjonssikkerhet ved kjøp av skytjenester – R10 – Sporbarhet

5.10 Tilgangskontroll / Autentisering

Krav

All tilgang må være autentisert, autorisert og sikret. Uautorisert tilgang må forhindres.

Leverandør må tilby verktøy for administrasjon av tjenestens brukere og deres tilganger, og ha tilstrekkelig støtte for bruk av eksterne identitetstilbydere.

Leverandøren må kunne dokumentere hvordan tilgang til Kundens data fjernes og hvordan det sikres at tilgangen er fjernet. I tillegg må det dokumenteres hvordan tilgang til Kundens data kan gjenopprettes. Dette gjelder tilganger for tjenesten og i drift av tjenesten, både for kunde og leverandør.

Dokumentasjonskrav

Beskriv hvordan brukere (personer, prosesser og applikasjoner) og privilegerte brukere identifiseres, autentiseres, autoriseres, administreres og hvordan tilgang kan etterprøves (audit).

Beskriv prosesser for forvaltning og kontroll av aksess gjennom hele bruker-livssyklusen, og prinsipper for dette.

Beskrivelsene bør inkludere muligheter for single sign-on, fler-faktor pålogging (MFA), føderasjon med eksterne identitetstilbydere, integrasjon med Identity management systems (IdM) og aksesslogg.

Beskriv hvordan tilgang endres og hvordan det sikres at tilgangen er fjernet. Beskriv hvordan tilgang gjenopprettes.

Veiledning

Tilgangskontroll og autentiseringsmekanismer må sørge for at kun rettmessige brukere får tilgang til virksomhetens informasjon. Leverandøren må vise til at sikkerhetsmekanismene sikrer at uautoriserte brukere hos leverandører, virksomheten eller utenfor ikke kan manipulere eller omgå sikkerhetsmekanismene for tilgangskontroll og autentisering.

Når truslene endres betyr det i praksis at sikkerhetstiltakenes effekt og styrke må følge etter. Leverandøren må videreutvikle sikkerhetsmekanismene slik at de er gir god nok sikring i forhold til trusselbildet. Virksomheten må utrede om sikkerhetsmekanismene som tilbys av leverandøren er tilstrekkelig basert på verdi og risikovurdering av informasjon og applikasjon.

Betingelsesbasert tilgang bør vurderes da dette sikrer tilganger gjennom verifikasjon av flere signaler som brukerens identitet, lokasjonen, enheten, applikasjonen og det nåværende risikobildet.

Under følger noen tiltak som virksomheten kan vurdere og inkludere i kravet:

- Løsningen bør støtte og kunne sette krav til tvungen MFA.
- Løsningen bør støtte betingelsesbasert tilgang
- Aktive sesjoner bør kunne termineres

Kobling til standarder og myndighetskrav

- DFØ - Krav til informasjonssikkerhet ved kjøp av skytjenester – R11 – Tilgangskontroll / Autentisering
- Kraftberedskapsforskriften § 6-3. Beskyttelse, avskjerming og tilgangskontroll
- Kraftberedskapsforskriften § 6-9. Digitale informasjonssystemer bokstav c. Sikre og oppdage

5.11 Sikkerhetsbrudd / Varsling

Krav

Leverandøren må ha sikkerhetsovervåkning av tjenesten og rutiner for umiddelbar varsling til Kunden ved hendelser. Overvåkningen bør kunne avdekke hendelser og handlinger i tråd med Kundens trusselbilde og relevante trusselaktører for tjenesten.

Dokumentasjonskrav

Beskriv prosesser, rutiner og teknologi som utgjør sikkerhetsovervåkingen og sikkerhetssjekk av tjenesten.

Veiledning

Det er god praksis å etablere en risikobasert aksjonsplan basert på tjenestenes kritikalitet for virksomheten. En slik plan bør omhandle krav til overvåkning, relevante konsekvensdimensjoner, varslingsplaner og dokumentasjon som kan behandles i fellesskap mellom virksomheten og skyleverandør. Eksempelvis vil en prioritetsmatrise over digitale tjenester hjelpe leverandøren til prioritering av proaktive grep for å unngå uønskede hendelser. En gjensidig varslingsplan vil være nødvendig for rask allokering av ressurser og tilstøtende beredskapsplaner.

Varslingsrutiner og tidsfrister bør også beskrives i informasjonssikkerhetsavtalen man har med leverandøren.

Som kunde, etabler en mottakende organisasjon for varsler om sikkerhetsbrudd relatert til virksomhetens data og behandling av disse for å vurdere tiltak som må iverksettes for å varsle videre og begrense skadeomfanget. Denne organisasjonen bør integreres i virksomhetens kriseberedskap.

Kobling til standarder og myndighetskrav

- DFØ - Krav til informasjonssikkerhet ved kjøp av skytjenester – R11 – Sikkerhetsbrudd / Varsling
- Kraftberedskapsforskriften § 6-9. Digitale informasjonssystemer

5.12 Sikker utvikling

Krav

Dersom leverandøren utvikler programvaren skal dette gjøres ihht. en Secure Software Development Life Cycle (SSDLC).

Dokumentasjonskrav

Beskrivelse av metodikk og evt. standarder og praksis som følges.

Veiledning

NSM Grunnprinsipper for IKT-sikkerhet /5/ detaljerer viktige momenter som bør inngå i leverandørens SSDLC. Leverandøren skal ha en utviklingsprosess som inneholder metodisk sikkerhetsvurdering av koden. Vær spesielt oppmerksom på kode som har spesiell betydning for sikkerheten, for eksempel kode for:

- tilgangskontroll
- kryptering av trafikk
- logging
- «parsing» av bruker-input
- «buffer overflow»

Det skal gjennomføres tilstrekkelig med testing gjennom hele utviklingsprosessen slik at feil, sårbarheter og mangler rettes opp før idriftsetting. Dette inkluderer test av at sikkerhetsfunksjonalitet fra forskjellige produkter og tjenester fungerer godt sammen.

Det anbefales videre at det benyttes separate miljøer for utvikling, test og produksjon slik at operative virksomhetsprosesser og data ikke blir påvirket ved feil i utviklings- og testløp. OWASP gir veiledning på vanlige sårbarheter i kode /22/.

Virksomheten bør vurdere å inkludere et BØR krav på at «Leverandøren skal liste opp alle tredjeparts bibliotek eller programvare som har blitt benyttet i utviklingen». Dette vil gi virksomheten en bedre oversikt over programvareverdikjeden.

Kobling til standarder og myndighetskrav

- NSM Grunnprinsipper 2.1.5 - Benytt en metode for sikker utvikling av programvare for å redusere sårbarhetene i programvaren.
- NSM Grunnprinsipper 2.1.6 - Benytt separate miljøer for utvikling, test og produksjon
- NSM Grunnprinsipper 2.1.7 - Gjennomfør tilstrekkelig med testing gjennom hele utviklingsprosessen

5.13 Geografisk lokasjon lagring, transport og behandling

Krav

Tjenesten og alle dens komponenter BØR behandle, lagre og transportere data innenfor EFTA, EU eller NATO.

Dokumentasjonskrav

Beskrivelsen skal omfatte følgende:

- hvor datasentre befinner seg fysisk
- hvor supportpersonell og sikkerhetspersonell befinner seg fysisk
- hvor maskinelle prosesser som behandler data befinner seg fysisk
- hvor sikkerhetskopier lagres
- hvor noder som behandler informasjon befinner seg fysisk

Veiledning

Merk at dette kravet er skrevet som et BØR krav. Se 4.3.1 for denne veilederen sin begrunnelse og anbefaling for at kraftsensitiv informasjon skal lagres, transporteres og behandles i land innenfor EFTA, EU eller NATO.

Virksomheter kan ofte kravstille og få gjennomslag for at alle datasenter involvert skal være lokalisert i EFTA, EU eller NATO, men leverandørens drift vil ofte bli utført fra land utenfor EFTA, EU eller NATO. Det er også en utfordring med at kommunikasjonsruter og noder kan være utenfor EFTA, EU eller NATO, selv om datasenter ligger i EFTA, EU eller NATO.

Det er meget utfordrende å overvåke detaljert kommunikasjonsrutene over internett i praksis, men virksomheten bør ha et forhold til nodene som behandler informasjon og hvor de befinner seg. Skyleverandørens revisjonsrapport bør kontrolleres for å få innsyn i den geografiske lokasjonen til nodene. Risikobildet her må forstås og virksomheten må vurdere tiltak for å redusere risikoen til et akseptabelt nivå, eksempelvis krypterte kanaler mellom datasenter.

Hvis datasenteret skal være lokalisert utenfor EFTA, EU eller NATO bør det gjennomføres en risikovurdering, inkludert landrisiko. NSM har publisert «Anbefaling om landvurdering ved tjenesteutsetting» som kan benyttes til dette formålet /23/.

Merk at det er ikke gitt at det er forsvarlig å ta i bruk skytjeneste for det aktuelle formålet. Virksomheten må utrede om dette er tilfellet.

Kobling til standarder og myndighetskrav

- Kraftberedskapsforskriften § 6-1. Identifisering av kraftsensitiv informasjon og rettmessige brukere
- Kraftberedskapsforskriften § 6-10. Brytefunksjonalitet i avanserte måle- og styringssystem (AMS)

5.14 Beskyttelse mot skadevare

Krav

Tjenesten skal ha funksjonalitet for å sikre at dokumenter og filer som lastes opp eller ned ikke inneholder skadevare.

Dokumentasjonskrav

Beskriv antivirusløsning/antiskadevareløsning som benyttes og hvordan det sikres at denne holdes oppdatert. Beskriv hvordan infiserte filer blir håndtert og hvordan brukeren blir informert.

Veiledning

Skadevare kan skade konfidensialiteten, integriteten og tilgjengeligheten til virksomhetens informasjon. Se NSMs tiltak mot skadevare og løsepengevirus /24/ for mer informasjon Tiltakene er basert på NSMs Grunnprinsipper for IKT-sikkerhet /5/ som inneholder flere konkrete tiltak for å beskytte mot skadevare.

I henhold til NSMs Grunnprinsipper bør leverandøren gjennomføre jevnlig sårbarhetskartlegging i skytjenesten ved hjelp av automatiserte verktøy /5/. Kartleggingen bør dekke klienter, servere og nettverk. Leverandøren bør benytte automatiserte sentraliserte verktøy for å håndtere skadevare og tjenester for sikkerhetsetterretning for å være oppdatert på nye sårbarheter slik at sikkerhetshull kan lukkes før en angriper kan utnytte dem. Sikkerhetsmekanismene bør integreres med virksomhetens eget informasjonssikkerhetssystem der det er hensiktsmessig.

Virksomheten må være oppmerksom på at enkelte leverandører av anti-skadevare løsninger benytter egne skytjenester til å laste opp data for kontroll i sine sandkasseløsninger. Dette gjelder også for andre typer løsninger som for eksempel ytelsesmålingsløsninger som laster opp ytelseslogger til egne skytjenester for analyse. Dette kan være i strid med krav for geografisk lokasjon og hvem som har tilgang til sensitiv informasjon.

Kobling til standarder og myndighetskrav

- Kraftberedskapsforskriften § 6-3. Beskyttelse, avskjerming og tilgangskontroll
- NSM Grunnprinsipper 3.1 - Oppdag og fjern kjente sårbarheter og trusler

5.15 Oppdatert og herdet sikkerhetsarkitektur

Krav

Tjenesten skal ha en oppdatert sikkerhetsarkitektur, samt være herdet iht. anerkjent praksis som NSM Grunnprinsipper for IKT-sikkerhet eller tilsvarende. Leverandøren skal ha rutiner for å holde tjenesten sikker over tid.

Dokumentasjonskrav

Leverandøren skal utarbeide et logisk diagram som viser sikkerhetsarkitekturen. Beskriv eller legg ved sikkerhetsarkitekturen og prinsipper for denne (f.eks. Zero Trust, definisjon fra NIST SP 800-207 /25/), samt rutiner for sikring av tjenesten.

Beskriv hvordan herding av tjenesten ivaretas, for eksempel ved bruk av CIS Controls eller beste praksis anbefalt fra leverandører av komponenter som inngår i tjenesten.

F.eks. ønskes beskrivelser av følgende i det logiske diagrammet:

- lagring
- datakommunikasjon
- sertifikathåndtering
- oppdateringer og patcher for å tette sikkerhetshull
- sikring av tilgangskontroll, roller og rettigheter
- sikring av API-er
- sikring av datasenter og nettverk

- kryptografiske mekanismer
- penetrasjonstesting eller andre mekanismer for testing og kontroll av service/applikasjons- og infrastruktursikkerhet

Veiledning

Leverandøren må i dette kravet vise at de har en robust, helhetlig og forsvarbar sikkerhetsarkitektur hvor all sikkerhetsfunksjonalitet samhandler og fungerer godt sammen. Virksomheten må også forsikre seg om at sikkerhetsfunksjonalitet som er driftet eller forvaltet av virksomheten eller andre partnere også vil samhandle med arkitekturen og tjenestene som tilbys fra skyleverandøren.

Skytjenesten bør være inndelt i forskjellige soner/segmenter i henhold til virksomheten sin risikoprofil. Soneinndeling kan gjøres på flere måter som for eksempel VLAN, mikrosegmentering, virtualiserte nettverk, etc.

Kobling til standarder og myndighetskrav

- Kraftberedskapsforskriften § 6-9. Digitale informasjonssystemer
- NSM 2.2 Etabler en sikker IKT-infrastruktur

5.16 Kontroll på underleverandører

Krav

Leverandøren skal ha kontroll på alle underleverandører som benyttes i leveransen til Kunden og skal redegjøre for alle underleverandører som benyttes. Ved bytte av underleverandør skal Kunden informeres og avtalen oppdateres.

Dokumentasjonskrav

Leverandøren skal liste opp underleverandører og angi rolle og ansvar for hver av underleverandørene. En underleverandør kan tilby blant annet (ikke uttømmende) informasjon, programvare, infrastruktur/plattform eller personale.

Veiledning

Virksomheten blir ikke nødvendigvis spesifikt informert om endringer i underleverandører av de store globale skyleverandørene og virksomheten må dermed følge med på nettsidene til skyleverandøren der informasjon om tredjeparter ofte publiseres. Virksomheten må undersøke hvilke muligheter de har til å tilegne seg nødvendig informasjon for å holde kontroll på underleverandører.

Kontroll av underleverandører kan bli en kompleks og ressurskrevende oppgave. Virksomheten må vurdere om de sitter på nødvendig kompetanse og tilgjengelige ressurser til å følge opp dette for anskaffelsen.

Kobling til standarder og myndighetskrav

- Kraftberedskapsforskriften § 6-1.Identifisering av kraftsensitiv informasjon og rettmessige brukere

5.17 Etterlevelse av avtale og relevante lover

Krav

Leverandøren skal ivareta gjeldende krav i avtale og relevante lover etterleves. Kravet gjelder også for underleverandører og Leverandør er ansvarlig for at underleverandører etterlever gjeldende krav i avtale og relevante lover.

Aktuelle lover og forskrifter:

- Energiloven
- Kraftberedskapsforskriften

- GDPR
- Personopplysningsloven, m.m.

Dokumentasjonskrav

Leverandøren skal bekrefte dette og liste opp aktuelle lover og forskrifter. Leverandøren må dokumentere etterlevelse, inkludert etterlevelse av underleverandører.

Veiledning

Dette kravet må tilpasses verdi og sikkerhetskrav for skytjenesten, samt gjeldende lovverk som virksomheten er underlagt. Som nevnt tidligere er det en utfordring å få globale skyleverandører til å akseptere nasjonale lovverk som kraftberedskapsforskriften. Det er enklere å få gjennomslag for mer globale lovverk som GDPR. Virksomheten må forsikre seg om at de enda oppfyller myndighetskrav og eget behov for informasjonssikkerhet gjennom enten standardvilkårene eller ved å anskaffe nødvendig sikkerhetsfunksjonalitet for ivaretakelse av krav.

Kobling til standarder og myndighetskrav

- Energiloven
- Kraftberedskapsforskriften
- GDPR
- Personvernopplysningsloven, m.m.

5.18 Sikring av data i transitt

Krav

Data som overføres via nettverk skal sikres. Dette inkluderer data som overføres til og fra tjenesten, internt i tjenesten og data som utveksles med andre tjenester/underleverandører.

Det skal defineres, velges, dimensjoneres og implementeres passende kryptografiske mekanismer og nøkler, som er sikre og utskiftbare, iht. anerkjente standarder (NIST el. tilsvarende).

Dokumentasjonskrav

Beskriv hvordan plattform og data internt i tjenesten sikres ved bruk av kryptering. Beskriv hvordan data under overføring beskyttes, herunder beskyttelse av nettverk og bruk av kryptering.

Veiledning

Data som overføres via nettverk kan avlyttes og/eller endres av uautoriserte aktører dersom dataen ikke er tilstrekkelig sikret. Dette gjelder både data som overføres til og fra tjenesten, internt i tjenesten og data som utveksles med andre tjenester for eksempel ved bruk av API-er.

Kobling til standarder og myndighetskrav

- DFØ - Krav til informasjonssikkerhet ved kjøp av skytjenester – R3 – Endring og avlytting av data under overføring

5.19 Sikring av data i ro

Krav

All data i ro skal sikres.

Det skal defineres, velges, dimensjoneres og implementeres passende kryptografiske mekanismer og nøkler, som er sikre og utskiftbare, iht. anerkjente standarder (Eksempelvis NIST SP 800-57 Part 3 Rev. 1 /26/ eller tilsvarende).

Dokumentasjonskrav

Beskriv hvordan plattform og lagrede data sikres ved bruk av kryptering, for blant annet disk, database, fil- kryptering

Veiledning

Ofte er det mange ulike aktører som har adgang til en skyleverandørs datasentre, men som ikke skal ha tilgang til virksomhetens data. Virksomhetens data må være sikret mot uautorisert tilgang. Leverandøren kan sikre data i ro gjennom blant annet en kombinasjon av fysisk sikring (se 5.4) og kryptering av data (Se 5.21 og 5.23).

Leverandøren må sikre maskinvare mot uautorisert tilgang og modifikasjon. Det finnes sårbarheter som tilsier at driftspersonell av f.eks. hypervisorlaget vil kunne få tilgang på data selv om det er kryptert. Disse vil ha tilgang på området siden de drifter underliggende IKT-infrastruktur. Det må eksistere varslingsmekanismer ved brudd på maskinvaresikkerhet og ev. tilgang må etterlate spor. Se 5.9 for sporbarhet.

Kobling til standarder og myndighetskrav

- DFØ - Krav til informasjonssikkerhet ved kjøp av skytjenester – R5 – Sikring av lagret informasjon

5.20 Tilgjengelighet

Krav

Tjenesten må være tilgjengelig for Kunden når Kunden har behov for tjenesten. Leverandøren må kunne garantere oppetid og dokumentere historisk oppetid/tilgjengelighet.

Tjenesten bør kunne opereres i «øymodus», altså at tjenesten opprettholder sin funksjon selv ved frafall av integrasjoner og nærliggende tjenester/komponenter.

Dokumentasjonskrav

Beskriv den garanterte tilgjengelighet og dokumenter oppetidsgarantien med historiske data. Dersom det brukes ulike tilgjengelighetsgarantier, så skal disse beskrives og hvilke betingelser som gjelder for de ulike garantiene.

Beskriv hvilke tiltak og prosedyrer som er etablert for å sikre tjenestens robusthet og tilgjengelighet.

Veiledning

Skyleverandøren må levere en skytjeneste som er tilstrekkelig robust for å kunne stå imot tilsiktede angrep, utilsiktede hendelser som menneskelige feil og naturlige hendelser som klima og pandemi.

«Øymodus» eller lignende robusthetsfunksjonalitet sikrer at tjenesten kan fortsette sin funksjon relativt uavhengig av bortfall av nærliggende komponenter/tjenester. Tjenesteplattformen skal sikre fortsatt produksjon selv om for eksempel internett eller strøm bortfaller. Et annet eksempel er at skytjenester kan «henge» slik at funksjonaliteten blir redusert eller gir ingen respons, uten at tjenesten faktisk går ned. Det bør beskrives i kravet i hvilken tilstand tjenesten skal defineres som utilgjengelig og bruk av responskrav bør inkluderes.

Kobling til standarder og myndighetskrav

- DFØ - Krav til informasjonssikkerhet ved kjøp av skytjenester – R8 – Tilgjengelighet

5.21 Administrasjon av krypteringsnøkler

Krav

Kryptering av data må være støttet av en nøkkeladministrasjonsinfrastruktur for å sikre sikker drift av tjenestene. Nøklene må være sikret gjennom hele livssyklusen, støttet av prosesser i et forvaltningsregime. Det gjelder for data i ro, i transitt og under prosessering. All aktivitet skal logges og kunne gjøres tilgjengelig for Kunden.

Dokumentasjonskrav

Beskriv hvordan krypteringsnøkler håndteres og sikres, og hvordan det sikres et skille mellom administrasjon av krypteringsnøkler og bruk av krypteringsnøkler. Beskriv hvilke nøkler som benyttes på de forskjellige tjenestene (data i ro, i transitt og under prosessering). Beskriv hvordan logger kan gjøres tilgjengelig for Kunden.

Veiledning

Virksomheten må sørge for at de på sin side har den nødvendige kompetansen for forvaltning og bruk av krypteringsnøkler. Videre må virksomheten ha en klar plan for hvordan nøkkeladministrasjonsinfrastrukturen skal samhandle med nøkkelinfrastruktur fra andre skyleverandører eller virksomheten selv.

NSMs «Cryptographic recommendations» /27/ og NIST SP 800-57 Part 3 Rev. 1 /26/ gir veiledning til valg av kryptografiske algoritmer med anbefalt nøkkellengde.

Kobling til standarder og myndighetskrav

- Kraftberedskapsforskriften § 6-3. Beskyttelse, avskjerming og tilgangskontroll

5.22 Revisjon

Krav

Kunden, eller en representant for Kunden, skal gis rett til å gjennomføre sikkerhetsrevisjon av Leverandøren for å kontrollere etterlevelsen av avtalen.

Leverandør må på forespørsel gi Kunden tilgang til revisjonsrapporter for vurdering av bla. sikkerhetsovervåkningen, vurdering av tilgangsstyringen til systemer og komponenter for leverandørens egne administratorer og hvilke prosedyrer og rutiner de har for varsling.

Dokumentasjonskrav

Bekreftelse på at Leverandør tillater revisjon eller kan gi Kunden tilgang til tredjeparts revisjonsrapporter.

Veiledning

De store skyleverandørene tillater som oftest ikke at virksomheten benytter egne revisorer, slik at det oftest er nødvendig å gjennomgå tredjeparts revisjonsrapporter. I tillegg til revisjonsrapportene fra leverandøren bør virksomheten revidere egne interne prosesser, tilgangskontroll, forvaltning, etc.

Kobling til standarder og myndighetskrav

- Kraftberedskapsforskriften § 6-9. Digitale informasjonssystemer
- Kraftberedskapsforskriften § 6-5. Anskaffelser

5.23 Sikring av kraftsensitiv informasjon i ro

Krav

Data i ro i tjenesten må krypteres, enten ved at (1) Leverandøren har kontroll over krypteringsnøkkelen på vegne av Kunden eller (2) Kunden har kontroll over krypteringsnøkkelen.

For alternativ (1) må Leverandøren signere Kundens eller tilsvarende dekkende sikkerhetsavtale og oppnå tilstrekkelig kontroll på krypteringsnøkler gjennom kombinasjon av a, b, c og d:

a) Leverandør må kontrollere nøklene på vegne av Kunden (dvs. Leverandøren implementerer alternativ 2 på vegne av Kunden).
b) Leverandøren må ha et regime for hvordan Kunden kan trekke tilbake (revokere) og legge tilbake (restore) nøkler.
c) Leverandøren må tilby logger av nøkkelbruk og nøkkeladministrasjonsaktiviteter til Kunden.

d) Leverandøren må sikre gjennom blant annet sikkerhetskopiering og arkivkapasitet at rekonstruksjon av sertifikater og nøkler er mulig dersom rotnøkkelen blir korrupt, ødelagt eller mistet.

For alternativ (2) må Kunden tilbys funksjonalitet for 'Bring Your Own Key' eller 'Hold Your Own Key'.

Dokumentasjonskrav

Beskriv hvordan krypteringsnøkler forvaltes, og hvilke av alternativene (1) og (2) som tilbys.

Dersom alternativ (1) tilbys, beskriv detaljer for hvordan punktene løses.

Veiledning

NIST SP 800-57 Part 3 Rev. 1 /26/ gir ytterligere veiledning. Virksomheten må gjøre en grundig analyse av hvilket alternativ som er mest egnet for sitt eget behov for informasjonssikkerhet og den aktuelle skytjenesten. «Double Encryption» er et tredje alternativ som også kan vurderes. Virksomheten må på sin side etablere system og rutiner for forvaltning av krypteringsnøkler.

Hvis leverandøren skal ha kontroll over krypteringsnøkkelen på vegne av virksomheten og ikke signerer sikkerhetsavtale må virksomheten sikre at sikkerhetsregimet til leverandøren gitt gjennom standardvilkår oppfyller de samme kravene som sikkerhetsavtalen. Sikkerhetsregimet kan vurderes ved å kontrollere at leverandør med tilhørende tjenester og produkter er sertifisert i henhold til anerkjente standarder og gjennomgå dokumentasjon på leverandørens prosesser, rutiner, tiltak og rapportering.

NVE har utarbeidet en avtale om håndtering og beskyttelse av kraftsensitiv informasjon i henhold til kraftberedskapsforskriften /28/ som kan benyttes.

Kobling til standarder og myndighetskrav

- Kraftberedskapsforskriften § 6-3. Beskyttelse, avskjerming og tilgangskontroll
- Kraftberedskapsforskriften § 6-5. Anskaffelser

5.24 Oversikt over hvem som skal ha innsyn i kraftsensitiv informasjon

Krav

Leverandøren må til enhver tid holde oversikt over hvem hos Leverandøren eller underleverandørene som har tilgang til Kundens ukrypterte informasjon. Denne oversikten må tilgjengeliggjøres for Kunden på forespørsel.

Dokumentasjonskrav

Beskriv rutinene for å holde oversikt og tilgjengeliggjøre denne informasjonen. Kunden må ha tilgang til en komplett oversikt over alle som har tilgang på våre data. F.eks. utvikling, support, drift, forvaltning og tredjeparts revisjonsfirmaer.

Veiledning

Kraftberedskapsforskriften setter krav til at virksomheten skal ha en navngitt oversikt over alle som har tilgang til kraftsensitiv informasjon. Dette kravet kan det være utfordrende å få gjennomslag for med de store skyleverandørene. Skyleverandørene har ofte utskiftning av personell og hvilken lokasjon driften av skytjenesten skjer fra kan variere avhengig av tid på døgnet. Merk at dette kravet gjelder for ukryptert informasjon, slik at gjennom kryptering og forvaltning kan virksomheten redusere risikoen for at ansatte hos leverandøren får muligheten til å tilegne seg ukryptert kraftsensitiv informasjon.

Videre benytter skyleverandørene en stor mengde underleverandører for både drift og vedlikehold av skytjenesten med underliggende infrastruktur. Det er særlig utfordrende å holde oversikt og kontroll på alle disse forskjellige underleverandørene.

Kobling til standarder og myndighetskrav

- Kraftberedskapsforskriften § 6-1. Identifisering av kraftsensitiv informasjon og rettmessige brukere

5.25 Rettigheter til bruk av data

Krav

Kunden skal beholde eierskapet til Kunden sine data under hele kontraktsforholdet og etter at kontrakten er avsluttet til data er flyttet og/eller slettet fra tjenesten.

Kundens informasjon skal ikke benyttes av leverandøren til egne formål eller videreformidles til andre parter uten samtykke fra kunden. Dette gjelder også metadata om kundens informasjon (trafikkvolum, tidspunkt, hyppighet, kommunikasjonspunkt osv.)

Dokumentasjonskrav

Eierskap, rettigheter og behandlingsformål skal defineres i en databehandleravtale eller lignende.

Veiledning

Virksomheten må gjennom dette kravet sikre at de beholder eierskap og rettigheter til sin informasjons under og etter kontraktsforholdet. Det må kontrolleres at leverandør eller underleverandør ikke benytter virksomhetens informasjon til egen vinning. NVE har utarbeidet en avtale om håndtering og beskyttelse av kraftsensitiv informasjon i henhold til kraftberedskapsforskriften /28/ som kan benyttes.

Kobling til standarder og myndighetskrav

- DFØ - Krav til informasjonssikkerhet ved kjøp av skytjenester – R2 – Lock-in

5.26 Hendelseshåndtering

Krav

Leverandøren skal ha egne strukturerte og aktive krise- og beredskapsplaner, som inkluderer prosedyrer for varsling til Kunden uten ugrunnet opphold.

Dokumentasjonskrav

Bekreftelse på at Leverandør har egne krise- og beredskapsplaner og beskrivelse av prosedyre for varsling til Kunden uten ugrunnet opphold.

Veiledning

Virksomheten må sørge for at leverandørens krise- og beredskapsplan integreres med virksomhetens egne planer og rutiner. Varslinger fra skyleverandøren må videreformidles til relevante myndigheter og partner som for eksempel KraftCERT (kbf § 6-9 bokstav c), NVE (kbf § 2-5) og NSM. Hvem som skal varsles er avhengig av typen og mengden av informasjonen med tilhørende sikkerhetsnivå som er påvirket. Se 4.5.3 for informasjon angående varsling.

Kobling til standarder og myndighetskrav

- Kraftberedskapsforskriften § 6-9. Digitale informasjonssystemer
- NSM Grunnprinsipper 4.1.1 Etabler et planverk for hendelseshåndtering

5.27 Identifisering og klassifisering av sensitiv informasjon

Krav

Tjenesten skal ha funksjonalitet for å identifisere og merke sensitiv informasjon.

Dokumentasjonskrav

Beskriv prosessen for å identifisere sensitiv informasjon, hvordan tjenesten oppfyller krav til merking og hvordan dette støttes for ulike filformater.

F.eks. databaser som inneholder kraftsensitiv informasjon, kan merkes gjennom navngivning og koding, eks. enl § 9-3.

Forslag til merking:

Underlagt taushetsplikt etter energiloven § 9-3 jf. kbf. § 6-2. Unntatt fra innsyn etter offentleglova § 13.	Underlagd teieplikt etter energiloven § 9-3 jf. kbf. § 6-2. Unntatt frå innsyn etter offentleglova § 13.

Veiledning

Det eksisterer mange forskjellige løsninger for identifisering og klassifisering av sensitiv informasjon. Noen skyleverandører leverer dette som en tjeneste, hvis ikke kan dette anskaffes fra andre leverandører. Virksomheten må sikre at identifiseringen og merkingen i skytjenesten følger virksomhetens retningslinjer for verdivurdering og klassifisering.

Kobling til standarder og myndighetskrav

- Kraftberedskapsforskriften § 6-1. Identifisering av kraftsensitiv informasjon og rettmessige brukere
- Kraftberedskapsforskriften § 6-3. Beskyttelse, avskjerming og tilgangskontroll (merking)

6 REFERANSER

/1/ Kommunal- og moderniseringsdepartementet. Nasjonal strategi for bruk av skytenester. [Online].; 2016. Tilgjengelig fra: https://www.regjeringen.no/contentassets/4e30afec51734d458596e723c0bdea0e/nasjonal_strategi_for_bruk_av_skytenester.pdf.

/2/ Olje- og energidepartementet. Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energiloven). [Online].; 2021. Tilgjengelig fra: https://lovdata.no/dokument/NL/lov/1990-06-29-50.

/3/ Olje- og energidepartementet. Forskrift om sikkerhet og beredskap i kraftforsyningen (kraftberedskapsforskriften). [Online].; 2013. Tilgjengelig fra: https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157.

/4/ Norges vassdrags- og energidirektorat (NVE). Veiledning til kraftberedskapsforskriften. [Online].; 2020. Tilgjengelig fra: https://www.nve.no/energi/tilsyn/kraftforsyningsberedskap/veiledning-til-kraftberedskapsforskriften/.

/5/ Nasjonal Sikkerhetsmyndighet (NSM). Grunnprinsipper for IKT-sikkerhet 2.0. [Online].; 2020 [sitert 2021 07 09. Tilgjengelig fra: https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/introduksjon-1/.

/6/ Norges vassdrags- og energidirektorat (NVE). IKT-sikkerhet i anskaffelser og tjenesteutsetting i kraftbransjen. [Online].; 2020. Tilgjengelig fra: https://publikasjoner.nve.no/rapport/2020/rapport2020_01.pdf.

/7/ Norges vassdrags- og energidirektorat (NVE). Regulering av IKT-sikkerhet. [Online].; 2017. Tilgjengelig fra: https://publikasjoner.nve.no/rapport/2017/rapport2017_26.pdf.

/8/ Direktoratet for forvaltning og økonomistyring (DFØ). Skytjenester (Cloud). [Online].; 2021 [sitert 2021 07 09. Tilgjengelig fra: https://www.anskaffelser.no/hva-skal-du-kjope/it/skytjenester-cloud.

/9/ Forum for informasjonssikkerhet i kraftforsyningen (FSK). Veileder for beskyttelse av kraftsensitiv informasjon ved bruk av Office 365 i kraftforsyningen. ; 2020.

/10 / Nasjonal Sikkerhetsmyndighet (NSM). Sikkerhetsfaglige anbefalinger ved tjenesteutsetting. [Online].; 2020 [sitert 2021 07 09. Tilgjengelig fra: https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/sikkerhetsfaglige-anbefalinger-ved-tjenesteutsetting/sikkerhetsfaglige-anbefalinger-ved-tjenesteutsetting/.

/11 / ISO/IEC. ISO/IEC 27002:2017 Informasjonsteknologi - Sikringsteknikker - Tiltak for informasjonssikring. [Online].; 2017. Tilgjengelig fra: https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=925901.

/12 / ISO/IEC. ISO/IEC 27017:2021 Informasjonsteknologi — Sikringsteknikker — Tiltak for informasjonssikring for skytjenester basert på ISO/IEC 27002. [Online].; 2021. Tilgjengelig fra: https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=1337002.

/13 / Center for Internet Security (CIS). CIS Controls Cloud Companion Guide. [Online].; 2019. Tilgjengelig fra: https://www.cisecurity.org/white-papers/cis-controls-cloud-companion-guide/.

/14 / Cloud Security Alliance (CSA). Cloud Security Alliance Cloud Controls Matrix and CAIQ v4. [Online].; 2021. Tilgjengelig fra: https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/.

/15 / Cloud Security Alliance (CSA). Security Guidance for Critical Areas of Focus in Cloud Computing v4.0. [Online].; 2017. Tilgjengelig fra: https://cloudsecurityalliance.org/research/guidance/.

/16 / Nasjonal Sikkerhetsmyndighet (NSM). Veileder i verdivurdering av informasjon. [Online].; 2021. Tilgjengelig fra: https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker-til-sikkerhetsloven/veileder-i-verdivurdering-av-informasjon.

/17 / ISO/IEC. ISO/IEC 27001:2017 Informasjonsteknologi - Sikringsteknikker - Ledelsessystemer for informasjonssikkerhet - Krav. [Online].; 2017. Tilgjengelig fra: https://standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=925900.

/18 / Digitaliseringsdirektoratet. Internkontroll i praksis - informasjonssikkerhet. [Online].; 2021. Tilgjengelig fra: https://www.digdir.no/informasjonssikkerhet/veilederen-internkontroll-i-praksis-informasjonssikkerhet-er-oppdatert/1743.

/19 / Nasjonal sikkerhetsmyndighet (NSM). Veileder i sikkerhetsstyring. [Online].; 2021. Tilgjengelig fra: https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker-til-sikkerhetsloven/veileder-i-sikkerhetsstyring/om-denne-veilederen/.

/20 / Direktoratet for forvaltning og økonomistyring. Avtale om løpende tjenestekjøp (SSA-L). [Online].; 2021. Tilgjengelig fra: https://www.anskaffelser.no/verktoy/maler-ogsa-kontrakt-og-avtalemaler/avtale-om-lopende-tjenestekjop-ssa-l.

/21 / Direktoratet for forvaltning og økonomistyring (DFØ). Statens standardavtaler for skytjenester (SSA-SKY). [Online].; 2021. Tilgjengelig fra: https://www.anskaffelser.no/verktoy/maler-ogsa-kontrakt-og-avtalemaler/statens-standardavtaler-skytjenester-ssa-sky.

/22 / Open Web Application Security Project. OWASP vulnerabilities. [Online].; 2021 [sitert 2021 10 05. Tilgjengelig fra: https://owasp.org/www-community/vulnerabilities/.

/23 Nasjonal sikkerhetsmyndighet (NSM). Anbefaling om landvurdering ved tjenesteutsetting. [Online].; 2021 [sitert 2021. Tilgjengelig fra: https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/anbefaling-om-landvurdering-ved-tjenesteutsetting/.

/24 Nasjonal Sikkerhetsmyndighet (NSM). Skadevare. [Online].; 2021 [sitert 2021 09 24. Tilgjengelig fra: https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/skadevare/.

/25 National Institute of Standards and Technology (NIST). SP 800-207 - Zero Trust Architecture. [Online].; 2020. Tilgjengelig fra: https://csrc.nist.gov/publications/detail/sp/800-207/final.

/26 National Institute of Standards and Technology (NIST). SP 800-57 Part 3 Rev. 1 Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance. [Online].; 2015. Tilgjengelig fra: https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final.

/27 Nasjonal sikkerhetsmyndighet (NSM). Cryptograpic reccomendations. [Online].; 2020. Tilgjengelig fra: https://nsm.no/getfile.php/133478-1591960609/Demo/Dokumenter/NSM%20cryptographic%20recommendations.pdf.

/28 Norges vassdrags- og energidirektorat (NVE). Avtale om håndtering og beskyttelse av kraftsensitiv informasjon. [Online].; 2021. Tilgjengelig fra: https://www.nve.no/media/7791/mal-informasjonssikkerhetsavtale-v1-0.pdf.

/29 Norsk Standard. NS 5814 Krav til risikovurderinger. [Online].; 2021. Tilgjengelig fra: https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=1352200.

/30 Nasjonal Sikkerhetsmyndighet (NSM). Rammeverk for håndtering av IKT-hendelser. [Online].; 2017. Tilgjengelig fra: https://nsm.no/regelverk-og-hjelp/andre-publikasjoner/rammeverk-for-handtering-av-ikt-hendelser/.

/31 Nasjonal Sikkerhetsmyndighet (NSM). Risikovurdering av IKT-systemer. [Online].; 2021. Tilgjengelig fra: https://nsm.no/getfile.php/136603-1625054089/Demo/Bildegalleri/Bilder%20til%20grunnprinsipper/Risikovurdering%20av%20IKT-systemer.pdf.

/32 ISO/IEC. ISO/IEC 27005:2018 Informasjonsteknologi - Sikringsteknikker - Risikostyring for informasjonssikkerhet. [Online].; 2018. Tilgjengelig fra: https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=997277.

VEDLEGG A - LITTERATURLISTE

Lovverk

- Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (Energiloven)
- Forskrift om sikkerhet og beredskap i kraftforsyningen (Kraftberedskapsforskriften)
- Lov om offentlige anskaffelser (Anskaffelsesforskriften)

Andre føringer

- Nasjonal sikkerhetsmyndighet (2020), Sikkerhetsfaglige anbefalinger ved tjenesteutsetting
- Norges vassdrags- og energidirektorat (2017), Regulering av IKT-sikkerhet
- Norges vassdrags- og energidirektorat (2020), IKT-sikkerhet ved anskaffelser og tjenesteutsetting i kraftbransjen
- Norges vassdrags- og energidirektorat, Avtale om håndtering og beskyttelse av kraftsensitiv informasjon (mal for sikkerhetsavtaler)

Veiledere og anerkjent praksis

- Forum for informasjonssikkerhet i kraftforsyningen (2020), Veileder for beskyttelse av kraftsensitiv informasjon ved bruk av Office 365 i kraftforsyningen
- Nasjonal sikkerhetsmyndighet, Generelle råd for tjenesteutsetting og skytjenester

Sikkerhetsstyring

- International Standards Organisation (2017), ISO/IEC 27001:2017 - Informasjonsteknologi – Sikringsteknikker - Ledelsessystemer for informasjonssikkerhet - Krav.
- Nasjonal sikkerhetsmyndighet (2020), Veileder i sikkerhetsstyring
- Digitaliseringsdirektoratet (2021), Internkontroll i praksis - informasjonssikkerhet

Sikkerhetskrav og -tiltak

- Nasjonal sikkerhetsmyndighet (2020), NSMs Grunnprinsipper for IKT-sikkerhet 2.0
- International Standards Organisation (2021), ISO / IEC 27002:2017 - Informasjonsteknologi – Sikringsteknikker - Tiltak for informasjonssikring
- International Standards Organisation (2015), ISO / IEC 27017:2015 - Informasjonsteknologi – Sikringsteknikker - Tiltak for informasjonssikring for skytjenester basert på ISO/IEC 27002
- International Standards Organisation (2019), ISO / IEC 27018:2019 - Informasjonsteknologi — Sikringsteknikker — Retningslinjer for beskyttelse av personopplysninger (PII) i offentlige skytjenester som håndterer personopplysninger
- North American Electric Reliability Corporation (NERC), Critical Infrastructure Protection Standards
- National Institute of Standards and Technology, USA, NIST SP 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations
- Cloud Security Alliance, Cloud Control Matrix (CCM)

- Center for Internet Security, CIS Controls

Evaluering av sikkerhetskrav og -tiltak

- National Institute of Standards and Technology, USA, NIST SP 800-53A - Assessing Security and Privacy Controls in Federal Information Systems and Organizations
- Cloud Security Alliance, Consensus Assessment Initiative Questionnaire (CAIQ)

VEDLEGG B – METODE FOR VERDIVURDERING

Dette vedlegget definerer konfidensialitet, integritet og tilgjengelighet for informasjonsprodukter, og tilhørende skalaer/sikkerhetsnivå som benyttes ved verdivurdering av informasjon.

Konfidensialitet

I skalaen for konfidensialitet (K0-K3), grupperes informasjon etter hvor kritisk det er for virksomheten, dvs. hvor stor konsekvens det kan få for virksomheten dersom informasjonen kommer på avveie og blir kjent for uvedkommende.

K3 Sensitiv informasjon: Informasjon med tilgangsbegrensning iht. myndighetskrav: Kraftsensitiv informasjon iht. kbf § 6-2

Dette er informasjon som har et svært høyt beskyttelsesbehov, og som kan gi store konsekvenser for Virksomheten dersom den kommer på avveie.

Spørsmål som kan stilles for å identifisere kraftsensitiv informasjon:

- Er informasjon så spesifikk at den kan brukes til å skade anlegg eller påvirke funksjoner som er av betydning for energiforsyningen? For eksempel
- Detaljert informasjon om energisystemet, herunder enlinjeskjema.
- Detaljert informasjon om klassifiserte transformatorstasjoner med tilhørende koblingsanlegg.
- Detaljert informasjon om alle system som ivaretar viktige driftskontrollfunksjoner, herunder nødvendige støttesystemer.
- Nøyaktig kartfesting av jordkabler
- Detaljerte analyser av sårbarhet som kan brukes til bevisst skadeverk, inkludert ROS-analyser.

Ansvaret for verdivurdering av informasjon ligger hos informasjonseier.

K2 Konfidensiell informasjon: Sensitiv informasjon og/eller informasjon unntatt offentlighet og med tilgangsbegrensning iht. tjenstlig behov, men som ikke faller inn under Virksomheten sensitiv informasjon. Dette er informasjon som har et høyt beskyttelsesbehov, og som kan gi store konsekvenser for Virksomheten dersom den kommer på avveie.

K1 Intern informasjon: Informasjon som kan deles med alle i Virksomheten. Virksomheten intern informasjon kan deles med eksterne samarbeidspartnere med tjenstlig behov. Dette er informasjon som kan gi begrensede konsekvenser for Virksomheten dersom den kommer på avveie.

K0: Åpen informasjon: Informasjon som kan deles offentlig. Dette er informasjon som har et slikt innhold og kvalitet at det ikke utgjør skade for virksomheten dersom den blir delt offentlig.

Integritet

Skalaen for integritet beskriver i hvilken grad feil og/eller mangler i informasjon får konsekvenser for Virksomheten, for eksempel når det kommer til fare for betydelig bortfall av energiforsyningen, uopprettelig økonomisk tap, tap av renommé eller HMS-konsekvenser for ansatt(e).

- I3: Kritiske konsekvenser
- I2: Alvorlige konsekvenser
- I1: Minimale til moderate konsekvenser

Tilgjengelighet

Skalaen for tilgjengelighet beskriver hvor lenge informasjon kan være utilgjengelig for konsekvensen blir kritisk.

- T3: Kritisk hvis informasjon er utilgjengelig > 15 minutter
- T2: Kritisk hvis informasjon er utilgjengelig > 2 timer
- T1: Kritisk hvis informasjon er utilgjengelig > 1 dag
- T0: Kritisk hvis informasjon er utilgjengelig > 1 uke