FORUM FOR INFORMASJONSSIKKERHET
I KRAFTFORSYNINGEN

Veileder for sikkerhet i anskaffelser og leverandørkjeder

Forum for informasjonssikkerhet i kraftforsyningen, august 2023

1 INTRODUKSJON

1.1 Bakgrunn og hensikt

Aktørene i kraftforsyningen er underlagt krav i lov og forskrift som skal bidra til opprettholdelse av et adekvat sikkerhetsnivå ved anskaffelser. Selv om forvalterne av de ulike lover og forskrifter tilgjengeliggjør veiledere for hvordan disse kravene kan etterleves, er det opp til den enkelte virksomhet å fastslå hvilke prosesser og tiltak som faktisk er nødvendig å gjennomføre for å etterleve disse kravene. Denne veilederen er utarbeidet av Forum for Informasjonssikkerhet i Kraftforsyningen (FSK). Formålet med veilederen er å hjelpe virksomhetene i kraftforsyningen med å gjennomføre anskaffelser av IKT-relaterte produkter eller tjenester på en måte som gjør at sikkerhetsnivået i virksomhetene, og dermed også potensielt innen kraftforsyningen, ikke påvirkes negativt. Veilederen fokuserer ikke bare på selve anskaffelsesprosessen, men også på hele levetiden til de produkter og tjenester som anskaffes. FSK ønsker med veilederen å påpeke at virksomheter ikke må undervurdere kundens makt til å påvirke leverandørers betingelser gjennom formell kravstillelse og oppfølging av denne. På generelt grunnlag oppfordrer FSK virksomheter i bransjen til å i større grad samarbeide opp mot felles leverandører av produkter og tjenester for å forbedre det generelle sikkerhetsnivået i kraftforsyningen.

Veilederen er utformet slik at den både kan brukes til generell læring, til forbedring av virksomhetens internkontroll og risikostyring for sikkerhet i anskaffelser og leverandørkjeder, samt til utforming av kravspesifikasjoner innen sikkerhet. Kapittel 1 introduserer sentrale begreper og gir leseren råd om hvordan veilederen skal brukes i praksis. Veilederen tar utgangspunkt i at risikostyring går som en rød tråd gjennom hele levetiden til produktet eller tjenesten man anskaffer, og gir en kort innledning om dette i kapittel 2. I kapittel 3 presenteres de ulike fasene i levetiden til produktet eller tjenesten, og for hver fase presenteres noen forhold som er særlig viktig å tenke på for å unngå at det etableres sårbarheter eller at man overser risiko i den enkelte fase. Ettersom leverandørkjederisiko er et aspekt det er særlig viktig å sette søkelyset på for produkter og tjenester man anskaffer og/eller allerede har anskaffet, presenteres det i kapittel 4 en kort oversikt over hvilke leverandørkjederelaterte aspekter man særlig bør være oppmerksom på. I kapittel 5 presenteres et utvalg av sikkerhetsrelaterte krav som må eller bør inngå i en kravspesifikasjon overfor leverandør ved anskaffelser. Veilederen har også tre vedlegg, med temaer som det er referert til i teksten.

1.2 Om bruk av veilederen

FSK har utarbeidet veilederen med konsulentbistand fra Det Norske Veritas (DNV), og FSK har rettighetene til veilederen og dens innhold. Veilederens innhold kan brukes fritt av virksomheter, men ikke til kommersielle formål uten skriftlig avtale med FSK.

Selv om veilederen er utarbeidet med det formål å bistå aktører i kraftforsyningen til å opprettholde sikkerhetsnivået og etterleve lovpålagte plikter, tar FSK ikke ansvar for eventuelle mangler eller avvik som oppstår som følge av bruk av veilederen.

1.3 Målgruppe, omfang og kravtype

Veilederen er utformet for virksomheter som er en del av *Kraftforsyningens beredskapsorganisasjon* (KBO), slik denne er definert i energiloven. Hvilke sikkerhetskrav

den enkelte KBO-enhet er underlagt, avhenger av nivået på klassifiserte anlegg og driftskontrollsystem, samt om det er fattet enkeltvedtak av NVE om sikring utover klasse. KBO-enheter er av svært varierende størrelse og har varierende kompleksitet i organisering, driftsmodeller og tjenesteutsetting. KBO-enheter vil også ha varierende grad av ressurstilgang, modenhet og kunnskap med hensyn til sikkerhet, og de vil dermed også ha varierende behov for veiledning og råd knyttet til anskaffelser og styring av risiko i leverandørkjeder. Dette er forsøkt gjenspeilet i veilederen, ved at den gir råd om praksiser som samtlige KBO-enheter som minimum bør etablere, men hvor nivå på ressursbruk og prioritering selv velges av den enkelte virksomhet.

Veilederen vil ikke gi en fullstendig beskrivelse av hva som skal til for å etterleve de sikkerhetskrav KBO-enheter er underlagt ved anskaffelse av produkter og tjenester, men vil gi generell veiledning om sikkerhetsrelaterte forhold det er viktig å tenke på ved slike anskaffelser. Sikkerhetskrav finnes i energiloven, samt kraftberedskapsforskriften og damsikkerhetsforskriften. I tillegg er det sikkerhetskrav i måle- og avregningsforskriften og i energilovforskriften, men disse kravene er ikke bestemt av nivå på anleggsklasse. Veilederen tar utgangspunkt i at enkelte KBO-enheter er underlagt anskaffelseslovgivningen og at øvrige KBO-er ofte også gjennomfører anskaffelser på bakgrunn av konkurranse, men gir ikke konkret veiledning om hvordan denne lovgivningen skal etterleves. Merk at KBO-enheter er underlagt en rekke andre forskrifter som kan påvirke hvilke krav som må stilles til en konkret anskaffelse, men disse er ikke beskrevet i veilederen. Som behandlingsansvarlig for personopplysninger, er KBO-enheter er også underlagt sikkerhetsrelaterte krav i personopplysningsloven og personvernforordningen, men dette regelverket dekkes ikke av veilederen. For enkelte typer anskaffelser vil det være overlapp mellom sikkerhetskrav i energilovgivningen og personvernlovgivningen, noe virksomheten bør være oppmerksom på.

Veilederen kan benyttes for enhver anskaffelse som påvirker virksomhetens sikkerhetsnivå, men er mest egnet til anskaffelser relatert til informasjons- og kommunikasjonsteknologi (IKT) – uavhengig av om det er snakk om enkeltkomponenter eller fullstendige løsninger, og uavhengig av hvilket av virksomhetens miljø anskaffelsen skal implementeres i.

Når man anskaffer produkter og tjenester stiller man ulike typer krav til selve produktet eller tjenesten, krav til hvordan produktet eller tjenesten skal implementeres i virksomheten og krav til de leverandører som er involvert i leveransen. Normalt formuleres eksplisitte sikkerhetskrav for en konkret anskaffelse, men virksomheten må være oppmerksom på at også generelle avtalevilkår og andre type krav vil kunne ha sikkerhetsmessige konsekvenser. Ofte er det også overlapp mellom enkelte sikkerhetskrav og tekniske eller funksjonelle krav. Veilederens kapittel 5 foreslår rene sikkerhetskrav som er nødvendig for å opprettholde, eller forbedre virksomhetens sikkerhetsnivå ved anskaffelser, men virksomheten må for den enkelte anskaffelse vurdere disse opp anskaffelsens egenskaper samt mot andre typer krav som skal stilles.

1.4 Standarder, rammeverk og veiledere

Det er opp til den enkelte KBO-enhet å avklare hvilke tiltak som er nødvendige å iverksette for å etterleve sikkerhetskrav i lov og forskrift. NVE og RME gir ut veiledere som skal hjelpe virksomhetene med å etterleve sikkerhetskrav, og i flere av NVE sine veiledere er det referert til en rekke standarder som bransjen kan benytte for å øke eget modenhetsnivå innen sikkerhet. Totalt sett finnes det etter hvert svært mange standarder, rammeverk og

veiledere knyttet til ivaretakelse av informasjonssikkerhet, IKT-sikkerhet eller cybersikkerhet, både i egen virksomhet og ved tjenesteutsettelse. Denne veilederen henviser til et utvalg av dem i vedlegg A. NVE anbefaler KBO-enhetene å etablere sikkerhetsnivå i samsvar med Nasjonal sikkerhetsmyndighet (NSM) sine grunnprinsipper for IKT-sikkerhet, men KBO-enheter står fritt til å bruke andre sikkerhetsrammeverk og -standarder i stedet.

Merk at det de kommende årene er ventet å komme regelverksendringer knyttet til sikkerhet. I Norge har NIS1-direktivet fra EU resultert i et forslag om en ny lov, *Lov om digital sikkerhet,* som trer i kraft i 2024. Fra EU er både NIS2-direktivet, som handler om cybersikkerhet, og den såkalte Cyber Resilience Act, som handler om cybersikkerhetskrav i produkter og tilleggstjenester, til vurdering. Hvilke deler av dette regelverket som er EØS-relevant er ikke avklart, men det er rimelig å forvente at fremtiden byr på stadig strenge krav til virksomheters arbeid med sikkerhet.

1.5 Begrepsbruk

Til nå har veilederen brukt begrepene «sikkerhet», «informasjonssikkerhet» og «cybersikkerhet». I regelverket som KBO-enheter er underlagt, benyttes begrepene «sikkerhet», «sikring», «IKT-sikkerhet» og «informasjonssikkerhet». I denne veilederen benyttes disse begrepene som synonymer.

I veilederen benyttes også begrepene «informasjonsteknologi» (IT) og «operasjonell teknologi» (OT). Dette er mest for å referere til skillet mellom det som for KBO-enheter er administrative IT-miljøer (jf. «informasjonssystemer» i kraftberedskapsforskriften (kbf) kapittel 6) og driftskontrollmiljøer (ja. «driftskontrollsystemer» i kbf. kapittel 7). Informasjonssikkerhet, IKT-sikkerhet og cybersikkerhet angår begge disse miljøer.

2 ANSVAR OG RISIKOSTYRING

2.1 Virksomhetens ansvar

Ansvaret for at krav i lov og forskrifter etterleves, at virksomhetens verdier beskyttes og at sikkerhetsnivået opprettholdes eller forbedres, ligger alltid hos virksomheten selv – også der man overlater til en annen part å levere produkter og tjenester. Det er ledelsens ansvar å sørge for at virksomhetens anskaffelse av produkter og tjenester ikke påvirker virksomhetens sikkerhetsnivå negativt – både gjennom å ha en kvalitetssikret anskaffelsesprosess, og gjennom å etablere et internkontrollsystem eller styringssystem som tilrettelegger for at anskaffede produkter og tjenester gjennom hele levetiden kan forvaltes i tråd med sikkerhetskrav.

Selv om det er virksomhetens ledelse som har det overordnede ansvaret for ivaretakelse av sikkerhet, er gjennomføringen av dette ansvaret ofte delegert til andre roller i virksomheten. Den som gis ansvaret for gjennomføringen av en konkret anskaffelse må sørge for at alle relevante deler av virksomheten involveres i prosessen. Etter hvert som stadig større deler av virksomheten blir digitalisert og tettere sammenkoblet, vil stadig større deler av prosess- og oppgaveutførelsen i virksomheten kunne ha sikkerhetskonsekvenser ved endring i de produkter og tjenester som inngår. Dette betyr at virksomhetene må ha bred involvering når de skal anskaffe slike produkter og tjenester. Avhengig av kompleksiteten til det anskaffede produkt eller tjeneste, vil følgende ansvarsområder eller aspekter kunne være relevant for en konkret anskaffelse:

- Økonomiske og juridiske rammer: samsvar med lov/forskrift, kontraktsforpliktelser, ressurstilgang, forvaltning av kontrakt og lisens, anskaffelseskompetanse, etc.
- Forretningsmål og strategi: risikostyring, forretningsmessige og strategiske behov på kort og lang sikt, prosesseiere, bestillerkompetanse, utviklings- og innovasjonsmuligheter, etc.
- Teknologiske og sikkerhetsmessige rammer: tekniske og sikkerhetsmessige betingelser for integrasjoner og implementering, driftskompetanse, utviklerkompetanse, systemeierskap, teknologitrender, etc.
- Brukerbehov: forbedringsbehov, design og brukergrensesnitt, endringer i kompetansebehov eller opplæringsbehov.

Å jobbe systematisk med sikkerhet i en virksomhet, inkludert ved anskaffelse av produkter og tjenester, krever med andre ord involvering fra alle deler av virksomheten.

2.2 Risiko ved anskaffelser eksisterer i flere dimensjoner

Ved anskaffelse av produkter og tjenester er det flere aspekter som vil kunne påvirke virksomhetens sikkerhetsnivå og dermed også driften negativt:

- Svakheter ved anskaffelsesprosessen eller kravstillelsen kan gjøre at den endelige løsningen blir suboptimal sikkerhetsmessig fordi man etter endt prosess ikke har annet valg enn å implementere løsningen tross mangler oppdaget underveis.
- Enkelte anskaffelser krever at mulige tilbydere gis tilgang til informasjon med høyt skjermingsbehov i anskaffelsesprosessen for at tilbudene skal kunne være tilpasset virksomheten, samtidig som at informasjonen ikke kan tilgjengeliggjøres for uvedkommende.
- Der virksomheten i kravspesifikasjonen stiller feil, for strenge eller for liberale sikkerhetskrav, kan dette ha negative konsekvenser for både kvaliteten på produktet/tjenesten og sikkerhetsnivået til virksomheten.
- Virksomhetens rettigheter med hensyn til kontroll over leverandørkjeden etableres avtalemessig i anskaffelsesfasen, men må følges løpende opp gjennom hele levetiden til produktet eller tjenesten.
- Å være låst til én leverandør for deres leveranse av produkter og tjenester gjør virksomheten sårbar for eventuelt brått bortfall eller kvalitetsforringelse av produktene og tjenestene.
- Tjenester som leveres via elektroniske kommunikasjonsnettverk, kan være sårbare for uautorisert inntrengning, manipulasjon, avlytting, eller utfall.
- Verden omkring oss endrer seg hele tiden. Det gjør også leverandørs produkter/tjenester, organisering, leveringsbetingelser, bruk av underleverandører, eierskap, osv.

Disse eksemplene er ikke utfyllende for hvilken risiko som kan oppstå ved anskaffelse av produkter og tjenester, men illustrerer hvilket risikobilde KBO-enheter står overfor. Veilederen har som mål å veilede leseren til å håndtere dette risikobildet. Risikostyring er den røde tråden gjennom veilederen– alle tiltak innen sikkerhet baserer seg på kartlegging

av risiko og håndtering og prioritering av risikoreduserende tiltak. Selv om sikkerhetskrav i lov og forskrift er absolutte, er etterlevelsen av dem, altså de konkrete valg av sikkerhetstiltak, noe som ofte i praksis baserer seg på en prioritering og en avveining mellom nytte og kostnad, brukervennlighet, leverandørenes leveringsevne og modenhetsnivå, samt virksomhetens evne og kapasitet til oppfølging.

2.3 Risikovurdering og -håndtering

Risikostyring og tilhørende risikovurderinger bør være utgangspunktet for alt sikkerhetsarbeidet i en virksomhet. Ved å avdekke risiko, fastsetter man hvilke sikkerhetstiltak som er nødvendige for å redusere risiko til et akseptabelt nivå. Risikovurderinger bør gjennomføres i forbindelse med anskaffelser egnet til å påvirke virksomhetens sikkerhetsnivå, og deretter løpende gjennom levetiden til det anskaffede produkt eller tjeneste. Merk at risiko ikke bare påvirkes av egenskaper ved selve produktet eller tjenesten, men også av forhold hos leverandør og underleverandører, forhold i egen virksomhet, samt eksterne hendelser som rammer samfunnet og leverandørkjeder generelt (cyberangrep, krig, naturkatastrofe, pandemi, osv.).

Risikovurderinger skal avdekke hvilken sikkerhetsrisiko en konkret anskaffelse vil kunne påføre virksomheten, noe som avhenger av hvilke av virksomhetens verdier som settes på spill gjennom anskaffelsen av produktet eller tjenesten. På den ene siden kan en logisk sammenkobling med leverandør (og underleverandør) utnyttes av ondsinnede aktører som ønsker å ramme virksomheten negativt, og på den andre siden kan avhengighet av leverandørens produkt eller tjeneste gjøre virksomheten sårbar for kvalitetsforringelse eller plutselig bortfall av produktet eller tjenesten. Arbeidet med en anskaffelse bør derfor fra oppstart inneholde en vurdering av hvilke verdier som vil kunne berøres som følge av slik sammenkobling og/eller avhengighet og hvor viktige disse verdiene er for virksomheten og for evnen til drift av kraftsystemet og forretningsprosesser.

Selv om risiko oppstår idet man anskaffer et produkt eller en tjeneste, og man håndterer denne risikoen ved å gjennomføre nødvendige sikkerhetstiltak når man tar i bruk produktet eller tjenesten, vil det fortsatt kunne oppstå ny risiko i hele produktet/tjenestens levetid. Det er derfor viktig at virksomheten gjennom sitt internkontrollsystem eller styringssystem for informasjonssikkerhet sørger for at det etableres prosesser for å overvåke sikkerhetsnivået (jevnlig sårbarhets- og trusselvurdering), har tett kontakt med leverandør vedrørende avvik og hendelser, følger opp leverandørs etterlevelse av krav, har et regime for endringshåndtering, har beredskapsplaner osv. Slik revurdering av risiko og risikohåndtering gjelder både bruken av produktet/tjenesten i egen virksomhet og sikkerhetstilstanden hos leverandøren av produktet/tjenesten. Oppfølging av risiko i produktets/tjenestens sin levetid bør gjennomføres av de som er ansvarlig eller brukere av det gjeldende produkt/tjeneste (som oftest systemeier eller systemansvarlig). Det samme gjelder risikovurderingen som gjennomføres når produktet/tjenesten avvikles og saneres. Deler av risikovurderingen avhenger av innsikt i leverandørers risikovurdering, noe som gjør at det er svært viktig at man i kravspesifikasjonen avtaler retten til å få informasjon om relevant risiko fra leverandør og at man deretter benytter seg av denne retten.

Valg av risikovurderingsmetodikk og risikovurderingens omfang avhenger ofte av hvor kritisk det konkrete produktet eller tjenesten er for virksomheten, eller av hvilke verdier som er utsatt. Det er opp til den enkelte virksomhet å avgjøre hvordan risikovurderinger gjennomføres og følges opp, og om valgene samsvarer med de forskriftsmessige kravene

som virksomheten er underlagt. Energilovgivningen legger ikke føringer for hvilken metodikk virksomheten skal bruke for å gjennomføre risikovurderinger. Virksomheten bør for øvrig være oppmerksom på at risikovurderinger kan være mangelfulle på grunn av manglende informasjon, feil eller manglende kompetanse, begrenset med tid, eller andre relevante forhold. Som en del av risikovurderinger der denne faren er til stede, bør virksomheten foreta en vurdering eller kartlegging av mulige ukjente sårbarhetsområder. Med dette menes at en må avdekke om risikoforståelsen en har er riktig, og om det kan være områder som tidligere var ukjente eller ble ansett usannsynlige. For eksempel er samtidige eller hybride trusler (fysisk og digital, eller ulike sammensetninger av trusler) mer relevante nå enn tidligere - dette gjelder også sannsynligheten for at slike inntreffer.

3 ANSKAFFELSER

3.1 Livssyklusforvaltning av anskaffede produkter og tjenester

Styring av den sikkerhetsrisiko et produkt eller en tjeneste er eksponert for, skjer blant annet ved å sørge for at produktet eller tjenesten dekkes av prosesser, rutiner og tiltak i virksomhetens styringssystem for informasjonssikkerhet. Livssyklusen til en anskaffelse kan deles inn i fem faser: planlegging, anskaffelse, implementering, drift/forvaltning og utfasing/opphør. Nedenfor gis en kort introduksjon av den enkelte fase, før de påfølgende underkapitler beskriver sikkerhetsrelaterte forhold som virksomheten må og/eller bør ta stilling til, for å kunne styre sikkerhetsrisiko for anskaffede produkter og tjenester. Det er mange aktiviteter en virksomhet gjennomfører i de ulike fasene, men denne veilederen omhandler *sikkerhetsrelaterte* forhold. Merk at enkelte forhold som er beskrevet i de senere fasene, må virksomheten ta stilling til allerede i planleggingsfasen. Leseren bør med andre ord forholde seg til underkapitlene som en helhetlig veiledning for anskaffelse og sikkerhetsforvaltning av produkter og tjenester, og ikke kun en trinnvis veiledning eller sjekkliste for hver enkelt fase.

Planleggingsfasen
Planleggingsfasen har ikke nødvendigvis en definert start, men i løpet av planleggingsfasen skal virksomheten identifisere sine behov, samt muligheter, begrensninger og alternativer for hvordan dette behovet kan dekkes gjennom en eller flere anskaffelser. Hvordan planleggingsfasen fortoner seg vil avhenge av hva som skal anskaffes, men virksomheten bør ha lav terskel for å gjennomføre anskaffelser som et formalisert prosjekt. For større anskaffelser bør virksomheten vurdere å gjennomføre et forprosjekt som skal gjennomføre nødvendig planlegging, forarbeider og markedsundersøkelser. Det er viktig å gjøre grundige forberedelser for å sørge for at man har et godt grunnlag for å kunne velge riktige leverandører og teknologi/funksjonalitet som passer inn i virksomheten. Allerede i planleggingsfasen bør en etablere et livsløpsperspektiv og dermed også planlegge utfasing og sanering av tjenesten eller produktet, i tillegg til planlegging av implementering og drift. Siden opphør av en avtale kan komme brått på, og skje av andre grunner enn at avtalen sies opp av virksomheten, bør virksomheten allerede i planleggingsfasen definere en tydelig strategi og definerte ressurser for opphør.

Anskaffelsesfasen
I anskaffelsesfasen tar virksomheten utgangspunkt i arbeidet gjort i planleggingsfasen for å gjennomføre anskaffelsen. Anskaffelsen bør eller må gjennomføres på bakgrunn av konkurranse, og uavhengig av hvordan konkurransen gjennomføres må virksomheten bruke

tid på å utforme kravspesifikasjon overfor tilbyderne. Sikkerhetskrav som spesifiseres skal bidra til å opprettholde eller forbedre virksomhetens sikkerhetsnivå, sørge for at virksomheten oppfyller krav i lov og forskrift, samt sørge for å avtale både ordinære og ekstraordinære sikkerhetsrelaterte vilkår for ytelsen. I anskaffelsesfasen skal man også sørge for at man velger den tilbyderen som best kan dekke virksomhetens behov, noe som krever at vilkårene for gjennomføring av konkurransen og selve gjennomføringen skjer på en standardisert og kvalitetssikret måte.

Implementeringsfasen
Implementeringsfasen er ofte en del av selve anskaffelsesprosessen, men kan identifiseres som en egen fase for å synliggjøre den informasjonssikkerhetsrisiko som ofte er knyttet til implementeringen av produkter og tjenester. Oppgavene som gjennomføres i implementeringsfasen må være regulert gjennom avtalen og kravspesifikasjon med leverandør, men virksomheten må følge opp at de avtalte vilkår og krav faktisk iverksettes. I implementeringsfasen skjer eventuell integrering med andre systemer, testing av funksjonalitet, sikkerhetstesting, og overføring av data og kompetanse fra eventuelle tidligere leverandører. Det er ofte i implementeringsfasen at de praktiske realiteter kommer til syne og at mangler i avtale, kravstillelse eller manglende/oversette forhold skaper utfordringer. Implementeringsfasen kan av disse grunner ofte trekke ut i tid og overlappe med driftsfasen, noe som gjør det viktig å avklare ansvarsdelingen mellom anskaffelsesprosjektet og den delen av forretningen som skal ha driftsansvaret.

Drifts- og forvaltningsfasen
Når implementeringen av anskaffet produkt/tjeneste er fullført, overlater de ansvarlige for anskaffelsen selve produktet/tjenesten til forretningen for å driftes og forvaltes. I tillegg til at virksomheten i denne fasen sørger for at ytelsen og kvaliteten til produktet/tjenesten er i tråd med leverandøravtalen, må virksomheten også løpende bidra til at sikkerhetsnivået i virksomheten ikke svekkes som følge av forhold ved det konkrete produktet eller tjenesten. I praksis innebærer dette å kontrollere eller revidere at avtalte sikkerhetskrav og interne sikkerhetsbestemmelser løpende overholdes, og at man forbereder seg på uforutsette eller ekstraordinære hendelser som vil kunne ha konsekvenser for informasjonssikkerheten.

Opphørsfasen
Det kan være ulike grunner til at anskaffede produkter eller tjenester ikke lenger skal benyttes i virksomheten, eksempelvis utløp av avtale, endring av virksomhetens behov, endrede leveringsvilkår fra leverandør, eller en uforutsett hendelse som resulterer i at en av partene sier opp avtalen. Disse grunnene kan oppstå brått eller tvinge seg frem langsomt. I utfasings- eller opphørsfasen for produktet/tjenesten skal kontrakter avsluttes, det skal ryddes opp, og det skal eventuelt legges til rette for overgang til ny leverandør. I denne fasen er særlig viktig å sikre at planer for utfasing, terminering eller flytting av en tjeneste ivaretar sanering av data, infrastruktur, maskinvare, dokumentasjon og annet som potensielt kan etterlate sårbarheter.

3.2 Gjennomføring av planleggingsfasen

Anskaffelser planlegges vanligvis grundig på forhånd. Det er viktig at sikkerhetsaspektet er en del av denne planleggingen helt fra oppstart for å unngå uforutsette, sikkerhetsrelaterte problemstillinger senere. Ofte er det konkrete forretningsbehov eller virksomhetens strategiske planer som igangsetter en anskaffelsesprosess, men det er viktig at praktiske behov ikke uforvarende overstyrer sikkerhetshensyn. Avhengig av hvilken type anskaffelse det er snakk om, bør virksomheten i planleggingen av en anskaffelse vurdere forholdene beskrevet i de neste underkapitlene. Å ikke planlegge godt for slike forhold kan etablere sårbarheter senere, som kan være vanskelig å håndtere på kort sikt. Eksempelvis er det lett å se fordelene ved overgang til driftsmodeller basert på skytjenester (skalerbarhet, fleksibilitet, enkle brukergrensesnitt, bred funksjonalitet, osv.), for så å glemme ulempene knyttet til økt kompleksitet, raske endringer, lav grad av transparens i løsninger, geografisk spredning og annerledes avtalevilkår.

3.2.1 Avklare forretningens behov og betingelser

Som oftest er det forretningens praktiske eller strategiske behov som er utgangspunktet for en anskaffelse, men det er viktig å avklare om det også er andre behov eller betingelser som vil kunne være førende for hva som kan anskaffes, på hvilken måte og fra hvilke leverandører:

- behov for helt spesifikk funksjonalitet.
- krav til geografisk lokalisering av leverandør og personell som leverer det anskaffede produkt eller tjeneste.
- begrensninger i hvilken grad av kontroll man kan eller bør overlate til leverandør, f.eks. driftskontrollfunksjoner i nettanlegg eller produksjonsanlegg.
- umodent leverandørmarked slik at man ikke får det man ønsker på kort sikt uten å inngå i langsiktig samarbeid med leverandør.
- utdatert leverandørmarked som leverer produkter og tjenester det ikke er utviklingsplaner for, men som man likevel er avhengig av.
- virksomheten (eller dens IT-driftsleverandør) stiller absolutte kriterier eller betingelser for produkter og tjenester som skal integreres med virksomhetens eksisterende teknologi eller infrastruktur – både for å i det hele tatt muliggjøre integrasjon og sørge for optimal IT-arkitektur, men også for å ivareta sikkerhetsnivået.

3.2.2 Avklare krav i lov/forskrift som gjelder for den konkrete anskaffelsen

Virksomheten må for hver enkelt anskaffelse vurdere hvilke krav i lov og forskrifter som vil gjelde, noe som avhenger av hva det er som skal anskaffes og hvilke verdier leverandøren får befatning med gjennom anskaffelsen. Det er ulike forskriftskrav knyttet til informasjonssystemer, driftskontrollsystemer, AMS og til beskyttelse av kraftsensitiv informasjon. Disse kravene kan gjøre at særskilte krav må stilles til produktet eller tjenesten som skal anskaffes, at særskilte krav må stilles til leverandør og underleverandør, og at selve anskaffelsesprosessen må gjennomføres på en bestemt måte. Dersom det er nødvendig at kraftsensitiv informasjon er en del av anbudsdokumentene, må konkurransen gjennomføres

som en begrenset anbudsinnbydelse for å forhindre at informasjonen blir tilgjengelig for uvedkommende.

3.2.3 Kartlegging av verdier og kritikalitetsnivå før risikovurdering

I planleggingsfasen må virksomheten vurdere risiko med hensyn til sikkerhet for den konkrete anskaffelsen, både risiko knyttet til gjennomføring av selve anskaffelsesprosjektet og risiko knyttet til at virksomheten anskaffer et produkt eller en tjeneste som kan påvirke virksomhetens sikkerhetsnivå i driftsfasen. Slike risikovurderinger gjennomføres for å identifisere hvilke tiltak som er nødvendig å iverksette for å opprettholde eller forbedre det sikkerhetsnivået som beskytter virksomhetens verdier, men også for å synliggjøre hvilket tjenestenivå som er nødvendig å avtale med leverandør. En risikovurdering blir mest mulig realistisk når den bygger på en grundig kartlegging eller avklaring av hvilke av virksomhetens verdier som settes på spill ved ulike hendelsesscenarier relatert til objektet som risikovurderes, og hvordan disse verdiene understøtter virksomhetens funksjoner og prosesser. Slike verdier er eksempelvis informasjon, informasjonssystemer, driftskontrollsystemer og tilhørende infrastruktur, og disse verdiene understøtter virksomhetens funksjoner.

Noen virksomheter har etablerte metoder for å systematisk kartlegge verdier, eksempelvis metode for verdivurdering av informasjon eller metode for kritikalitetsvurdering («business impact analysis»), mens andre virksomheter lar slik kartlegging være en implisitt del av risikovurderingene sine. Uansett, bør virksomheten for den enkelte anskaffelse vurdere hvilke verdier som etableres eller omfattes som følge av anskaffelsen, samt vurdere hvilke av virksomhetens funksjoner eller prosesser disse verdiene understøtter eller er egnet til å påvirke. Slik vil virksomheten få et mer realistisk bilde av potensielle konsekvenser for funksjoner og prosesser som kan forårsakes av hendelser som fører til svekkelse, endring eller bortfall av verdiene, og dermed også et bedre grunnlag for å prioritere allokering av ressurser for forvaltning og sikring. Dette er særlig viktig å kartlegge der opprettholdelsen eller forvaltningen av verdiene i praksis er overlatt til leverandør og hvor virksomheten dermed er avhengig av leverandørens pålitelighet, slik at virksomheten kan iverksette passende tiltak knyttet til redundans, alternativ drift og beredskap.

Ofte ligger slik verdivurdering eller kritikalitetsvurdering implisitt til grunn for de krav i lov og forskrift som regulerer hvordan ulike typer informasjon, informasjonssystemer og annen teknologi som minimum skal håndteres og sikres. Likevel bør virksomheten for den enkelte anskaffelse vurdere om omfanget av informasjon, graden av sammenkobling med leverandør (og underleverandører), samt graden av avhengighet av leverandørens pålitelighet, er slik at særlige sikkerhetstiltak bør iverksettes.

3.2.4 Bestillerkompetanse, ressurser og involvering

I planleggingsfasen må virksomheten avklare om den besitter nok kompetanse og ressurser til å gjennomføre anskaffelsen, eller om det er nødvendig med ekstern bistand for å ivareta kvalitet og sikkerhet i anskaffelsen. Husk at mangler ved selve anskaffelsesprosessen eller ved kontraktsvilkår kan etablere sikkerhetsrisiko senere. Virksomheten må også vurdere om den er tilstrekkelig rigget med ressurser og kompetanse for driftsfasen til det produktet eller tjenesten som anskaffes. Sikkerhetsnivået er ikke noe man bare avtaler ved kontraktsinngåelse, og så er det ivaretatt – dedikert personell må i driftsfasen tildeles ansvaret for å følge opp sikkerhetsaspekter ved det anskaffede produkt/tjeneste gjennom hele levetiden til produktet/anskaffelsen.

Det er viktig at virksomheten ikke undervurderer hvilken kompetanse som er nødvendig å involvere i planleggingsfasen, og det bør etableres en oversikt som inneholder definerte roller og ansvarsområder, samt hvilke kompetanseområder som bør delta i de ulike delene av en konkret anskaffelsesprosess (planlegging, kravspesifikasjon, evaluering, kontraktsinngåelse, implementering, osv.). Ofte kan det være slik at en anskaffelse er mer kompleks å implementere (og drifte) og har større sikkerhetsrelaterte problemstillinger enn først antatt. Kompetanseområder/fagpersoner som bør vurderes involvert er:

- Prosesseier, representant fra forretningen
- Sluttbrukere av anskaffelsens leveranse
- Økonomirådgiver, controller
- Juridisk rådgiver, anskaffelsesekspertise
- IT-arkitekt, virksomhetsarkitekt
- Representant for IT-driftsleverandør (nettverksarkitektur, integrasjoner, plattform, tilgangsregimet, osv.)
- Representant for driftskontrollmiljøet
- Sikkerhetsansvarlig
- Tiltenkt systemeier og -ansvarlig
- Eventuell ekstern bistand knyttet til spesifikk fagkompetanse

3.3 Gjennomføring av anskaffelsesfasen

3.3.1 Konkurransegrunnlag

Konkurransegrunnlaget er virksomhetens beskrivelse av hvilket behov som skal dekkes med anskaffelsen og hva virksomheten ønsker at leverandørene gir tilbud på. Konkurransegrunnlaget skal spesifisere produktet/tjenesten som skal anskaffes og hvilke vilkår som gjelder for konkurransen. Grunnlaget bør formuleres og presenteres på en måte som gjør at tilbydere forstår hva som etterspørres slik at tilbudene er i henhold til dette. Konkurransegrunnlaget består for eksempel av:

- En tydelig beskrivelse av virksomheten, virksomhetens behov og hva som skal anskaffes
- Beskriv også gjerne hva som *ikke* skal anskaffes, for å unngå beskrivelser og dokumentasjon som er «off topic»
- Beskrivelse av hvordan virksomheten kommer til å gjennomføre konkurransen
- Hvilke kontraktsvilkår som gjelder for oppdraget, herunder sikkerhetskrav
- Krav til hvordan leverandør skal utforme tilbudet sitt
- Beskrivelse av forventninger til samhandling med virksomhetens ressurser
- Krav og forventninger til forvaltning og videreutvikling av oppdragets innhold
- Eventuelle andre opplysninger av betydning for anskaffelsen eller konkurransegjennomføringen

3.3.2 Maler for avtaledokumenter og kravspesifikasjoner

Den konkrete anskaffelsens egenskaper vil avgjøre hvor omfattende avtaleverk som bør benyttes i anskaffelsen og hvor detaljert spesifikasjonene av sikkerhetskrav må være. Å benytte statens standardavtaler eller andre standard kontraktsmaler som utgangspunkt, bidrar til å høyne kvaliteten på anskaffelsesprosessen og reduserer sannsynligheten for uforutsett sikkerhetsrisiko som skyldes manglende eller svake avtalevilkår. Mange avtalevilkår som normalt er en del av enhver avtale vil kunne ha sikkerhetsmessige konsekvenser dersom de ikke avtales eller oppfylles, eksempelvis avtalevilkår om eierskap til data, vilkår som regulerer avtaleopphør, vilkår som avklarer roller og ansvar, mv.

Husk: når man inngår avtale med leverandør skal man også avtale hvordan avtaleopphør skal skje

I avtale med leverandør skal man sørge for at eventualiteter som kan oppstå underveis i avtaleforholdet eller levetiden til produktet/tjenesten er avtalerettslig regulert. Dette gjelder også hvilke vilkår som gjelder ved avtaleopphør, for eksempel håndtering av informasjon eller utstyr. Ikke alle avtaler opphører planlagt eller kontrollert, og da er det viktig at virksomheten har sikret seg avtalerettslig for situasjoner hvor avtaleopphør skjer av uforutsette og plutselige grunner.

NVE har laget veiledere og sjekklister som kan hjelpe KBO-enheter med å sørge for at de vesentligste krav er dekket i kravspesifikasjoner (jf. vedlegg A), samt maler for taushetserklæring og informasjonssikkerhetsavtale for behandling av sensitiv informasjon om kraftforsyningen. Virksomheten plikter ikke å benytte NVEs veiledere eller maler, og står fritt til å utvikle egne maler eller benytte leverandørens maler så lenge forskriftskravene er i varetatt.

Der man ser behovet for å gjennomføre en internasjonal anskaffelse og at avtaledokumenter og kravspesifikasjoner utformes på engelsk, er det anbefalt å benytte formuleringer som baserer seg på internasjonalt anerkjente standarder fremfor direkte oversettelse av formuleringer fra norsk lovgivning, standarder, og lignende. Se likevel vedlegg A for lenke til NVE sin oversettelse av bestemmelser i kraftberedskapsforskriften. Ved internasjonale anskaffelser eller ved kjøp av produkter/tjenester fra andre land må virksomheten for øvrig være kjent med forskjellen mellom rettssystemet i Norge og de land leverandører er knyttet til. Dersom virksomheten ikke er oppmerksom på dette, kan man ende opp med å undergrave de kravene man har stilt i avtalen, ved at det andre lands rett overstyrer de vilkårene man har avtalt.

3.3.3 Identifisering av anskaffelsestype og gjennomføringsmåte

Etter at virksomheten har planlagt anskaffelsen, må virksomheten ha avklart om kravene i lov eller forskrift medfører at anskaffelsen må eller bør gjennomføres på en spesiell måte.

Ordinær anskaffelsesprosess:

Generelt sett, gjelder det for anskaffelser, uansett hvordan anskaffelsen gjennomføres, at man i prosessen holder oversikt over hvilke aktører som gis tilgang til hvilken informasjon og at man gir formell instruks til alle aktører som gis tilgang til konfidensiell informasjon om behandlingen av denne (taushetserklæring, informasjonssikkerhetsavtale, opplæring, mv.). Virksomheten må sørge for at alle parter (juridiske enheter) som er involvert i tilbudet eller

leveransen fra én leverandør, pålegges krav til sikkerhet. Enkelte tilbydere bruker tredjepartsleverandører som bistår med å levere tilbud og implementere produkt/tjeneste, men som ikke er en underleverandør til det endelige produkt/tjeneste, og disse tredjepartsleverandørene må også signere taushetserklæring og/eller informasjonssikkerhetsavtale dersom det er relevant for oppdraget.

Begrenset anbudsinnbydelse:

Generelt sett, bør det være et mål å minimere informasjonssikkerhetsrisikoen i gjennomføringen av anskaffelsen – uten at det går ut over kvaliteten på gjennomføringen og uten at det begrenser konkurransen. Risiko kan minimeres ved å begrense hvor mye informasjon som inngår i konkurransegrunnlaget (anbudsdokumentene), samt begrense hvilke tilbydere som får tilgang til informasjonen. For anskaffelser hvor konkurransegrunnlaget inneholder kraftsensitiv informasjon, er det imidlertid et forskriftskrav om at det skal benyttes begrenset anbudsinnbydelse. Dette kravet handler om å ha kontroll over og begrense hvilke aktører som får tilgang til kraftsensitiv informasjon i tilbudsfasen av en anskaffelse, samt sørge for at de signerer nødvendig informasjonssikkerhetsavtale og taushetserklæringer før de får tilgang til den kraftsensitive informasjonen i konkurransegrunnlaget. I en begrenset anbudsinnbydelse må tilbydere prekvalifiseres for å få tilgang til konkurransegrunnlaget og levere tilbud. Det betyr at virksomheten må sette opp hvilke kriterier som skal gjelde for en slik prekvalifisering. Ofte handler det om å luke ut tilbydere som faktisk ikke leverer produktet/tjenesten man etterspør, men slik prekvalifisering kan også benyttes til å luke ut tilbydere som ikke oppfyller de viktigste sikkerhetskrav.

Markedsundersøkelser før konkurranse:

Dersom virksomheten er usikker på hva den eksakt ønsker å anskaffe, er ukjent med hva markedet kan levere eller hvem som kan levere, kan det gjennomføres en uforpliktende markedsundersøkelse («Request for Information»/«RFI») før man setter i gang med en forpliktende anskaffelsesprosess. Dette er også nyttig dersom man har indikasjoner på at tilbydere hovedsakelig finnes i land det er nødvendig å gjennomføre en landrisikovurdering av, før man vurderer å anskaffe noe fra leverandører derfra. Slike markedsundersøkelser er uforpliktende, og for å få mest mulig informasjon om hvilke produkter og tjenester som eksisterer, og hvor leverandørmarkedet befinner seg, kan det være nyttig å ikke formulere sikkerhetskrav knyttet til geografisk lokalisering eller andre begrensende faktorer i markedsundersøkelsen. I stedet bør man be tilbydere fritt beskrive sikkerhetsregimet, bruken av datasenterressurser, dataflyt og lokalisering av support, osv. Merk at reglene for begrenset anbudsinnbydelse også gjelder for markedsundersøkelser der det er nødvendig at kraftsensitiv informasjon er en del av informasjonsgrunnlaget man tilgjengeliggjør for dem som skal presentere produktet/tjenesten sin for markedsundersøkelsen.

Markedsundersøkelser vil kunne gjøre det enklere å utforme kravspesifikasjonen for selve anskaffelsen, både når det gjelder sikkerhetskrav og andre krav, fordi man har bedre oversikt over hvor leverandørmarkedet befinner seg, hvilke typer leverandører og underleverandører som er involvert og hvilke driftsmodeller man må belage seg på.

Direkteanskaffelse:

Dersom virksomheten er i en situasjon hvor en direkteanskaffelse er nødvendig for virksomheten og tillatt etter anskaffelsesregelverket, må virksomheten likevel stille adekvate krav til sikkerhet til leverandør og produktet/tjenesten som anskaffes. Det er viktig at

grunnene som tillater direkteanskaffelse (begrenset med tilbydere, usedvanlig fordelaktig tilbud, uforutsette omstendigheter har medført tidsnød, etc.) ikke blir de samme grunnene til at leverandører kan avtale kontraktsvilkår og tjenestenivå i virksomhetens disfavør. Ved direkteanskaffelse anbefales det derfor utarbeidelse av kravspesifikasjon som om anskaffelsen skulle vært gjennomført som konkurranse. Hensikten med dette er å kvalitetssikre behov og forventninger til oppdrages innhold. Kravspesifikasjonen må ha tilstrekkelig kvalitet til at oppdraget kan forvaltes og videreutvikles på lik linje med kontraktstildeling ved bruk av annen anskaffelsesform.

Innovasjonspartnerskap:

Innovasjonspartnerskap er en måte virksomheten kan få dekket sine behov på dersom det ikke eksisterer noen andre passende løsninger i markedet fra før, og hvor virksomheten får skreddersydd en løsning. Slike partnerskap etableres gjennom ordinær anskaffelsesprosess, men vil påvirke hvordan virksomheten spesifiserer krav til sikkerhet (og andre krav). I tillegg til at virksomheten før kontraktsinngåelse må gjøre det klart hvilke sikkerhetskrav som stilles til prosessen og til den endelige løsningen, er det svært viktig at kontraktsvilkårene utformes slik at virksomheten ikke låses til leverandør, at ikke leverandør tildeles makt til å diktere tjenestenivå eller utviklingsprogresjon, etc. Ofte vil man kunne oppleve at leverandører besvarer ordinære anskaffelsesutlysninger med det som i praksis er en forespørsel om innovasjonspartnerskap, det vil si, uferdige produkter eller tjenester hvor de «på sikt» kan levere det virksomheten etterspør). I slike situasjoner anbefales det å avstemme ambisjonsnivå og kontrollere at kontraktsvilkår faktisk vil oppfylles.

FoU-prosjekt:

Virksomheter deltar ofte i FoU-prosjekter med IKT-relaterte aspekter. Selv om slike prosjekter ikke innebærer en anskaffelse, har deltakelsen i dem ofte potensial for å påvirke virksomhetens sikkerhetsnivå, for eksempel gjennom å dele store datasett, gjennom å teste ikke-utprøvd teknologi eller løsninger, ta i bruk ny funksjonalitet på tvers av IT og OT-miljøer som resulterer i utilsiktede sammenkoblinger, osv. Dette betyr at virksomheten må gjøre risikovurderinger og stille sikkerhetskrav tilsvarende det som gjelder ved anskaffelser.

3.3.4 Kravspesifikasjon for sikkerhet

Etter at anskaffelsen er planlagt, må virksomheten også ha avklart hvordan den konkrete anskaffelsens egenskaper vil avgjøre hvilke sikkerhetskrav som må gjøres gjeldende for det produkt eller tjeneste som skal anskaffes og for leverandør som leverer produktet/tjenesten.

- Energilovgivningen pålegger KBO-enheter krav som potensielt må omformuleres til krav som må oppfylles av de leverandører av produkter og tjenester virksomheten benytter, for at KBO-enheten selv kan etterleve disse kravene.
- I tillegg eksisterer det allment anerkjente sikkerhetsstandarder, rammeverk og prinsipper som legger føringer for hvilke krav som må eller bør stilles til leverandører, jf. vedlegg A.
- Sikkerhetskrav til selve produktet/tjenesten overlapper ofte med tekniske eller funksjonelle krav, eller med krav til tjenestenivå – eksempelvis krav om aktivitetslogging og overvåking, krav til ytelse og oppetid (tilgjengelighet), krav om automatiserte feilmeldinger, krav om endringslogg, etc. Slike krav avhenger i stor grad av hva det er som anskaffes.

Veilederens kapittel 5 lister opp sikkerhetskrav som må være en del av kravspesifikasjonen for nesten alle typer anskaffelser som kan påvirke virksomhetens sikkerhetsnivå, samt et utvalg av krav som må eller bør stilles der anskaffelsen oppfyller en (eller flere) av de oppgitte betingelser. Sikkerhetskravene som stilles i den enkelte anskaffelse avhenger for det første av hva det er som anskaffes, så kravene i kapittel 5 fokuserer på *generelle* krav til sikkerhet i selve produktet eller tjenesten som anskaffes. For det andre vil kravene som stilles til en konkret anskaffelse avhenge av hvordan leverandør (og underleverandør) potensielt kan påvirke virksomhetens sikkerhetsnivå i driftsfasen, derfor vil valg av krav fra kapittel 5 avhenge av graden av slik potensiell påvirkning. Jo større potensiell påvirkning, eksempelvis gjennom tett logisk sammenkobling eller høyt behov for pålitelig tjenestenivå, jo viktigere er det å stille krav til sikkerhetsnivået i *leverandørens* egne virksomhet.

Når virksomheten spesifiserer sikkerhetskrav, er det viktig å ikke stille krav på en måte som gjør at leverandører lar være å levere tilbud. For eksempel kan for strenge, rigide, detaljerte, eller mangfoldige sikkerhetskrav føre til at tilbydere tror at de ikke kan levere det virksomheten ønsker. Dette betyr ikke at man skal la være å formulere sikkerhetskrav, men at man i formuleringen av krav må være tydelig på hva formålet med kravet er (med mindre det er underforstått), bruker begreper som er allment kjente, bruker ord som viser at man er åpen for forslag til alternative løsninger (så lenge formålet oppfylles) og at man ikke stiller for rigide dokumentasjonskrav. Virksomheten bør gjennom formulering av kravspesifikasjonen vise at virksomheten besitter bestillerkompetanse og den vet hva den snakker om.

Husk: avtal eksplisitte kriterier for ferdigstillelse av anskaffelsesprosess og implementering
Virksomheten må i avtalen også tydelig spesifisere krav til akseptansetest og godkjenningsperiode for gjennomføringen og/eller implementeringen av anskaffelsen i virksomheten, for å unngå svakheter eller sårbarheter i implementeringen. Slike krav kan med fordel knyttes til betalingsbetingelser og sanksjoner som eksempelvis avkortning, dagbøter, terminering av kontrakt, erstatningskrav, mv. Ved bruk av sanksjoner kan det også være hensiktsmessig med premiering form av eksempelvis bonus, opsjoner eller prosjekter for videreutvikling av leveransens innhold.

3.3.5 Krav, vekting og evaluering

Egenskaper ved den konkrete anskaffelsen vil sammen med bestemmelser i lov og forskrift være avgjørende for hvilke krav som *må* oppfylles av leverandør, hvilke som *kan oppfylles på ulike måter* eller i ulik grad, samt hvilke krav som er *valgfrie* å oppfylle.

Husk: ulike typer anskaffelser krever ulike typer kravspesifikasjoner
Hvor detaljerte sikkerhetskrav som stilles i en kravspesifikasjon, avhenger av egenskapene til produktet/tjenesten, samt av hvilken rolle leverandør spiller i driftsfasen for produktet/tjenesten. Er det snakk om standardiserte produkter/tjenester og hyllevare, kan man stille mer generelle og overordnede krav. Er det snakk om produkter/tjenester med høy kompleksitet, høyt sikkerhetsbehov eller som skal skreddersys til virksomheten, bør man ha mer detaljerte krav. Videre, der det er leverandøren som skal drifte produktet/tjenesten, eller der det er tette logiske koblinger mellom leverandør og virksomheten og virksomhetens verdier, må det stilles mer detaljerte sikkerhetskrav til leverandørens egne virksomhet enn dersom de ikke forestår slik drift eller ikke har tette koblinger.

En enkel strategi for utforming av krav kan være:

- *Absolutte krav (MÅ-krav)*: utledes direkte fra krav i lov eller forskrift eller sikkerhetsstandarder/-anbefalinger.
- *Viktige krav (BØR-krav)*: utledes fra virksomhetens prioriterte behov for å enten øke kvalitet eller redusere risiko på definerte områder.
- *Ønskede krav (OPSJONER)*: behov som ønskes oppfylt fordi det er ventet at det kan bidra positivt til sikkerhetsnivået i virksomheten, men som ikke påvirker sikkerhetsnivået negativt dersom det ikke oppfylles. Slike krav kan dessuten brukes der det av ulike grunner er mindre sannsynlig at de potensielle tilbyderne kan oppfylle kravet.

I tillegg må virksomheten ta hensyn til at:

- De ulike absolutte krav bør vurderes satt som *kvalifikasjonskrav*, altså minimumskrav som må oppfylles av tilbyder for i det hele tatt å være kvalifisert for videre vurdering i prosessen. Kvalifikasjonskrav gjør det mulig for virksomheten å sile ut tilbydere fra prosessen uten å måtte evaluere dem opp mot samtlige krav. Slike krav må formuleres presist og forståelig slik at tilbydere ikke misforstår krav og lar være å levere tilbud på feil grunnlag. Hvilke krav som settes som kvalifikasjonskrav i den konkrete anskaffelsen må være relevant for, og stå i forhold til anskaffelsens egenskaper og omfang. For strenge kvalifikasjonskrav kan begrense konkurransen.
- Sikkerhetskrav som virksomheten aksepterer at kan oppfylles på ulike måter og i ulik grad, og som skal sammenlignes på tvers av tilbydere, omtales som *evalueringskrav*. Slike krav skal formuleres på en måte som gjør at oppfyllelsen av dem kan evalueres og vektes på en hensiktsmessig måte, og dermed være sammenlignbare på tvers av tilbydere. Skala for oppfyllelse kan for eksempel være «under forventning», «som forventet» og «over forventning», eller en tallkarakter fra et forhåndsbestemt intervall. Absolutte, viktige og ønskede krav kan alle behandles som evalueringskrav.
- Verken absolutte, viktige eller ønskede krav behøver å inngå som evalueringskrav. De kan for eksempel *vurderes som oppfylt eller ikke oppfylt*. Tilbyder skal likevel dokumentere at kravet oppfylles.

- For hvert krav må virksomheten vurdere om de skal basere seg på tilbyders egenerklæring eller bekreftelse om at kravet er oppfylt, eller om de skal kreve dokumentasjon som verifiserer at krav er oppfylt og beskriver hvordan det er oppfylt. Egenerklæring brukes mest for krav som tilbyder kun skal bekrefte at de er innforstått med at gjelder for den konkrete anskaffelsen, eksempelvis krav om eierskap til data eller krav om deltakelse i virksomhetens beredskapsøvelser, og fungerer mest som en juridisk garanti for virksomheten. For å bekrefte at en tilbyder faktisk oppfyller et sikkerhetskrav og for å kunne sammenligne tilbydere med hverandre, vil det være nødvendig at tilbyder på ett eller annet vis sannsynliggjør dette gjennom å legge frem dokumentasjon. Det er viktig at virksomheten ber om dokumentasjon som er mulig å fremstille og at selve kravet til dokumentasjon både står i forhold til hva det er som anskaffes og til kravet som skal dokumenteres.
- Å stille passende sikkerhetskrav for den enkelte anskaffelse handler om bestillerkompetanse. Anskaffelsen må ha sikkerhetskrav tilpasset virksomhetens behov, anskaffelsens egenskaper, nødvendige integrasjoner, leverandørmarkedets sikkerhetsmodenhet, virksomhetens betalingsvillighet (kostnad for sikkerhetsnivå), juridiske rammer, samt tilpasset de andre kravene som stilles i anskaffelsen.

Se kapittel 5 for konkrete forslag til sikkerhetskrav som kan stilles i kravspesifikasjoner.

Husk: ikke bruk tid på evaluering av krav som ikke er evaluerbare
Dersom virksomheten forventer at tilbyderne i en konkret anskaffelse vil presentere nokså lik besvarelse og dokumentasjon av et konkret sikkerhetskrav, for eksempel krav om at virksomheten skal ha et visst regime for tilgangsstyring i en tjeneste, vil det være vanskelig å sammenligne besvarelsene opp mot hverandre. Virksomheten bør i slike tilfeller vurdere å ikke la kravet være et evalueringskrav, men et krav som oppfylles eller ikke. Husk i den sammenheng på at «må»-krav som ikke oppfylles innebærer at en tilbyder må forkastes.

3.3.6 Særlig om krav til tilbyderens virksomhet

Vurdering av tilbydere kan kun skje på bakgrunn av objektive kriterier gjort kjent i konkurransegrunnlaget. I en evalueringsprosess kan man derfor ikke vektlegge forhold ved tilbyder som man tilfeldigvis blir gjort kjent med underveis i anskaffelsesprosessen. I tillegg til å stille krav til sikkerhetsarbeidet i leverandørs virksomhet, bør man derfor i kravspesifikasjonen vurdere å stille krav til andre forhold ved leverandørens stilling og stand, som indirekte kan si noe om hvordan virksomhetens sikkerhetsnivå potensielt kan påvirkes ved å kjøpe produkter eller tjenester fra leverandøren. Slike krav er det vanlig å ha som kvalifiseringskrav, og kravene kan enten dokumentere at de er oppfylt eller erklære at de er oppfylt.

Noen forhold man kan ha behov for å stille krav om, er:

- At leverandør har tilstrekkelig finansiell styrke, kredittverdighet, etc. til å kunne oppfylle kontrakten.
- At leverandør er åpen om eierskapsstruktur.

- At leverandør er lokalisert innenfor et angitt geografisk område. Merk at et slikt krav også må være i tråd med anskaffelseslovgivningen.
- At leverandør har et kvalitetsstyringssystem, eksempelvis i tråd med ISO 9001 eller tilsvarende. Merk at styringssystemet for informasjonssikkerhet som man også kan etterspørre, gjerne kan være samkjørt med et slikt kvalitetssystem.
- Tilstrekkelig erfaring med å levere og implementere produktet/tjenesten som etterspørres.
- At virksomheten gis tilgang til andre kunders erfaringsrapporter, evalueringer, etc.
- At virksomheten gis tilgang til informasjon om eventuelle avvik, tilsynssaker, rettssaker, osv. knyttet til offentlige myndigheters revisjoner eller tilsyn.

Behov for kjennskap til slike forhold er ofte mest relevant der det er snakk om store/kostbare og langvarige anskaffelser, hvor anskaffelsen har høy risiko for virksomhetens sikkerhetsnivå, eller anskaffelser hvor behovet for pålitelighet og tilgjengelighet er stort.

3.3.7 Vurdering av besvarelse og dokumentasjon fra tilbyderne

Vurderingen av de enkelte tilbud gjøres på bakgrunn av tilbydernes besvarelse av kravspesifikasjonen, inkludert eventuell dokumentasjon virksomheten har bedt om. Besvarelse og dokumentasjon brukes også til å sammenligne tilbyderne, dersom kravene er satt som evalueringskrav. Besvarelsene og dokumentasjonen må være målbare for at virksomheten skal kunne vurdere om krav faktisk er oppfylt og må være sammenligne på tvers av tilbydere. Dette er noe virksomheten må ta hensyn til i formuleringen av krav og beskrivelsen av hvordan oppfyllelsen av dem skal bekreftes og eventuelt dokumenteres. I den forbindelse, må virksomheten ofte erkjenne at det ikke nødvendigvis er enkelt å fremskaffe verifisert informasjon som dokumenterer faktiske forhold og oppfyllelse av krav hos tilbyderne, og at enhver leverandørrelasjon til syvende og sist alltid vil innebære en grad av tillit til at leverandøren faktisk oppfyller de kravene de påstår er oppfylt. Målet for virksomheten bør derfor være å hente inn dokumentasjon som er tilstrekkelig for å kunne godtgjøre at leverandør faktisk oppfyller krav.

Husk: sjekk at du betaler riktig pris for det sikkerhetsnivået du har bedt om
Virksomheten må i evalueringen av tilbydere verifisere at pristilbudet fra tilbyder faktisk inneholder de sikkerhetskrav virksomheten har stilt, med mindre virksomheten har formulert kravene som opsjoner. En del leverandører lar sikkerhetskrav eller -funksjonalitet være tilleggstjenester eller opsjoner man betaler mer for, eller beskriver at de har planer om å iverksette enkelte tiltak med enn eller annen omtrentlig tidshorisont.

Eksempler på dokumentasjon som kan gi en pekepinn på tilbyders oppfyllelse av krav kan være generelle beskrivelser av sikkerheten i produktet/tjenesten og hos leverandør, spesifikke beskrivelser av hvordan virksomhetens tjenestenivå ivaretas, visuelle fremstillinger, forhåndsinnspilte demoer, fremleggelse av bevis på sertifiseringer, henvisning til uavhengig tredjeparts revisjonsrapport, resultater fra penetrasjonstester eller andre sikkerhetstester, henvisning til åpent tilgjengelige og nøytrale brukervurderinger, referanser fra navngitte kunder som kan kontaktes, tilsynsrapporter fra myndigheter, etc.

Dokumentasjon kan også være muntlig eller virtuell, f.eks. at man spesifiserer at man ønsker en muntlig presentasjon eller visning av løsningen i bruk.

At virksomheten stiller tydelige krav, etterspør dokumentasjon, ber om demonstrasjoner/innsyn og stiller oppfølgingsspørsmål, vil kunne bidra til forbedring hos leverandører i fremtiden. Hvordan kunder opptrer er det som endrer hvordan leverandører opptrer – er man villig til å kjøpe produkter og tjenester med middels sikkerhetsnivå, vil leverandører alltids ønske å selge dem. Det er derfor viktig å vise overfor tilbydere hva man forventer før man signerer kontrakt med en av dem, samt viktig at man gjennom formuleringer og atferd viser at man vet hva man stiller krav om.

Husk: ikke slå dere til ro med vage formuleringer og uklar dokumentasjon
Virksomheten bør stille oppfølgingsspørsmål og be om ytterligere dokumentasjon inntil den er trygg på at krav med høy sannsynlighet faktisk oppfylles.

Husk: vær også grundig i oppfølgingen av ønskede krav/opsjoner
Der virksomheten har tatt med opsjoner i kravspesifikasjonen bør kravene følges grundig opp selv om de kanskje er mindre viktige for virksomheten. Siden kravet er en opsjon, kan tilbydere benytte anledningen til å si at kravet *kan* oppfylles eller er *planlagt oppfylt*, selv om det kanskje er snakk om en løsning som faktisk ikke er planlagt eller utviklet ennå. Virksomheten bør ha det klart for seg hvorvidt kravet vil være oppfylt ved kontraktsinngåelse, eller om det er under utvikling. Hvis sistnevnte er tilfellet, bør virksomheten etterspørre en utviklingsplan for oppfylling av kravet.

3.3.8 Særlig om landrisikovurdering

Energilovgivningen legger få begrensninger på hvilke land KBO-enheter kan anskaffe produkter og tjenester fra, samt hvilke land KBO-enheter kan overføre kraftsensitiv informasjon til. Likevel kan det være gode sikkerhetsmessige grunner til å vurdere risiko forbundet med å anskaffe produkter og tjenester fra land utenfor de interessefellesskapene som Norge er en del av. Veiledning til hvordan virksomheten kan gjennomføre en landrisikovurdering er beskrevet i Vedlegg B.

3.3.9 Særlig om krav til bakgrunnssjekk av leverandørens personell

Det er kun ved ansettelser i egen virksomhet, samt for personer som skal ha adgang til anlegg i klasse 3, at kraftberedskapsforskriften eksplisitt pålegger KBO-enheter å gjennom føre bakgrunnssjekk av personer før ansettelse. For de fleste typer anskaffelser hvor informasjonssikkerhetsrisikoen er av et visst omfang, er det likevel anbefalt å stille krav om at leverandør skal ha et regime for personellsikkerhet i egen virksomhet. Et slikt regime kan blant annet innebære å ha bakgrunnssjekk av ansatte før ansettelse, og bakgrunnssjekk kan eksempelvis innebære å sørge for identifisering og autentisering av personen, verifisering av innhold i CV, gjennomføre intervju og egnethetsvurdering, foreta referansesjekker, etc.

Husk: personlig kjennskap til leverandørens personell kan styrke sikkerhetsnivået
Der virksomheter skal la eksternt personell få tilgang eller adgang til klassifiserte anlegg eller systemer, eller til andre tjenester som er kritisk for virksomhetens forretningsdrift, bør en vurdere å stille krav om at leverandør skal stille dedikert personell til rådighet, som virksomheten gis anledning til å bli kjent med. Personlig kjennskap til nøkkelpersoner hos leverandør kan styrke slike personers ansvarsfølelse og gjøre leverandørrelasjonen mer pålitelig og sikker. Husk imidlertid også at tillitsbånd kan være sårbare for utnyttelse av tredjeparter.

3.3.10 Avtaleinngåelse

All vurdering av kravetterlevelse og avtalevilkår må ferdigstilles før virksomheten signerer avtaledokumenter – i det øyeblikket avtalen er inngått, har virksomheten i praksis gitt fra seg en del av forhandlingsmakten de hadde overfor leverandør før inngåelse. Den konkrete anskaffelsens egenskaper avgjør hvor detaljerte krav man avtaler med leverandør, men generelt sett bør virksomheten ta hensyn til følgende:

- De som signerer kontrakten, må ha fullmakt til å inngå en bindende avtale på vegne av den respektive part som signerer.
- At avtalevilkårene ikke bare regulerer normalsituasjonen hvor alt skjer som planlagt eller ventet, men at de også regulerer leveransen og relasjonen til leverandør under ekstraordinære forhold (konkurs, større feil/mangler eller sikkerhetshendelser på leverandørsiden).
- Plan for igangsetting eller implementering av anskaffelsen skal inngå i det juridiske grunnlaget avtalt mellom partene og foreligge før signering. Planen må beskrive hvordan implementering skal foregå, med beskrivelse av roller, ansvar, fremdriftsplan med oppgaver og tidsfrister, beskrivelse av akseptansekriterier for gjennomført plan, samt hvilke vilkår som gjelder ved forsinket implementering. Gjør det tydelig overfor leverandør hvordan implementeringsplanen skal følges opp – ikke overlat til leverandør alene å sørge for fremdrift.
- Det er viktig å ha det klart for seg hvilke oppgaver og vilkår som gjelder for implementeringsfasen, og hvilke oppgaver og vilkår som gjelder driftsfasen. Førstnevnte reguleres av den implementeringsplan som avtales mellom partene, og sistnevnte av vedlikeholds-/driftsavtalen med avtalt tjenestenivå. Noen ganger vil oppgaver planlagt gjennomført i implementeringsfasen ikke bli utført før driftsfasen (på grunn av uforutsette hindre, forsinkelser, osv.), noe man bør ta høyde for i kontraktsvilkårene. Det må også avtales formelt hvordan endringer i implementeringsplanen skal gjennomføres – dette behovet kan oppstå for store og komplekse anskaffelser.
- Avtal rett til å terminere kontrakt ved eierskifte hos leverandør, bortfall av kritisk personell, eller andre endringer som i stor grad kan påvirke leverandørens leveranseevne eller virksomhetens sikkerhetsnivå.

- Avtal tydelig ansvarsdeling mellom virksomhet og leverandør, inkludert drifts- og sikkerhetsansvar, ansvar for kompetanse, ansvar for varsling av endringer og hendelser, osv.
- Avtalt rett til løpende opplæring og support fra leverandør gjennom hele livsløpet, samt plikt til kompetanseoverføring ved kontraktopphør.
- Avtal tydelig eierskap til data og utledede data.
- Kontroller at pristilbudet dekker alle sikkerhetskrav stilt til produkt/tjeneste og til leverandør.

3.4 Gjennomføring av implementeringsfasen

3.4.1 Implementeringsplanen må inneholde styring av sikkerhetsrisiko

I implementeringsfasen skal man sørge for at produktet eller tjenesten implementeres i virksomheten eller tas i bruk på den måten som er spesifisert i kontrakten, kravspesifikasjonen og implementeringsplanen, og sørge for at det ikke innføres sårbarheter som truer sikkerhetsnivået i prosessen. Normalt er det avtalt tidsfrister og tjenestenivå for implementeringsfasen, og avhengig av anskaffelsens omfang og egenskaper, er det normalt avtalt at det skal gjennomføres formaliserte tester for å kontrollere at produktet eller tjenesten tilfredsstiller funksjonelle krav, brukerbehov, sikkerhetskrav, osv. Først når all identifisert risiko er håndtert – enten ved gjennomførte tiltak eller plan for slik gjennomføring, er implementeringsfasen over, sett fra et sikkerhetsperspektiv.

Virksomheten bør styre sikkerhetsrisiko gjennom hele implementeringsfasen ved å løpende identifisere risiko og tiltak for å håndtere denne. Det er sjelden alt går som planlagt, for eksempel på grunn av undervurdert ressursbehov eller kompleksitet, og det er ikke uvanlig at man på grunn av tidspress i implementeringsfasen iverksetter midlertidige løsninger eller bevisst avviker fra instrukser eller prosedyrer for å løse uforutsette problemstillinger. Ved manglende systematikk og kontroll kan man med andre ord utilsiktet innføre sårbarheter som ikke avdekkes før senere.

Ved anskaffelse av produkter eller tjenester som er spesialutviklet eller skreddersydd til virksomheten, er det enda viktigere med en grundig implementeringsplan og kontroll av at utviklingen/tilpasningen og implementeringen faktisk er gjennomført i tråd med det som er avtalt. Dette kan eksempelvis innebære å kontrollere at leverandørens utviklingsarbeid har skjedd i tråd med krav til sikker utvikling, at endringer eller aktiviteter er logget, at leveransenes integritet kontrolleres, at det foreligger tilstrekkelig dokumentasjon av endelig produkt/tjeneste ved overlevering, etc.

3.4.2 Overgang fra en leverandør til en annen

Enkelte anskaffelser innebærer at man går fra en leverandør til en annen og at virksomheten dermed må sørge for at data og kompetanse skal overføres fra en leverandør (eller tjeneste) til en annen, og at integrasjoner må flyttes. I slike situasjoner må dette selvsagt være en del av implementeringsfasen for den nye anskaffelsen (og en del av opphørsfasen for den forhenværende). Virksomheten bør på forhånd vurdere om leverandøren man avslutter avtalen med benytter ytelser fra underleverandører som krever særskilt håndtering eller oppfølging.

3.4.3 Testing bør også inkludere sikkerhetstester og -kontroller

I implementeringsfasen bør man teste at leverandøren faktisk oppfyller de spesifiserte sikkerhetskrav og at sikkerhetsnivået er som avtalt for det anskaffede produkt/tjeneste. Sikkerhetstester handler mest om testing av IKT-relaterte aspekter (at konfigurasjoner, integrasjoner, sikkerhetsfunksjonalitet, etc. er utført eller implementert som planlagt), men det bør også gjennomføres kontroll av at de administrative tiltak og prosesser faktisk fungerer. Testene utføres som oftest i samarbeid med leverandøren. Eksempler på sikkerhetstester og kontroller er:

- manuell kontroll av planlagte sikkerhetskonfigurasjoner.
- test av tilgangsstyring, at administratorrettigheter er som planlagt, etc.
- inntrengningstester fra utsiden inkl. tjenestenektangrep.
- brukertest for å avdekke eventuell sårbar funksjonalitet i brukergrensesnittet (fare for brukerfeil, sikkerhetshendelser pga. vanvare, osv.).
- øve på at prosedyre for varsling og hendelseshåndtering fungerer mellom partene, inkludert virksomhetens varsling til myndighetene og til KraftCERT.
- kontrollere at leverandør oppfyller de spesifiserte krav til sikkerhet, etterspørre sikkerhetsdokumentasjon, etc.
- statisk analyse av kildekoden.

3.4.4 Registrer dokumentasjon relevant for ivaretakelse av sikkerhet

Enkelte anskaffelser innebærer at virksomheten trenger bistand og opplæring fra leverandør for selv å kunne drifte og forvalte produktet eller tjenesten som er anskaffet, og det er ofte i implementeringsfasen at leverandører stiller til rådighet ressurser (personer og tid) til å drive med kompetanseoverføring og opplæring. Virksomheten bør benytte seg av denne ressurstilgangen, slik at den er mest mulig rustet for drifts- og forvaltningsfasen, og virksomheten bør registrere dokumentasjon relevant for drifts- og forvaltningsfasen før implementeringsfasen er over.

Dokumentasjon, som er relevant for å ivareta sikkerhetsnivået, bør forvaltes løpende og oppdateres ved endringer. Hva slik dokumentasjon består av vil avhenge av den konkrete tjenesten/produktet, men kan blant annet inneholde opplysninger om hvilken informasjon leverandør behandler i sitt miljø, hvordan den behandles, hvordan tjenesten er satt opp, hvilke integrasjoner og avhengigheter som eksisterer, informasjon om maskinvare og programvare, hvem som har ansvar for hva, hvem som er kontaktperson, hvilke underleverandører som benyttes, etc.

3.4.5 Ta høyde for at enkelte forhold ikke fullføres i implementeringsfasen

Avtalen regulerer hvilke vilkår som skal gjelde dersom avtalt implementeringsplan ikke er mulig å følge. Det er ikke uvanlig med forsinkelser, uforutsette hendelser eller kompleksitet og behov for å endre planen underveis. Virksomheten må sørge for at dette ikke fører til økt risiko eller at planlagte sikkerhetstiltak ikke blir innført på grunn av ressursmangel, budsjettsprekk eller tidspress. Virksomheten bør legge realistiske implementeringsplaner og sørge for tilstrekkelig ressurstilgang, men når virksomheten først havner i en situasjon hvor implementering ikke kan gjennomføres i henhold til opprinnelig plan, må forventninger

avklares tydelig underveis og det må avtales tydelige frister for fullføring av resterende oppgaver.

3.4.6 Opprydding og kontroll ved implementeringsfasens slutt

Virksomheten må være oppmerksom på at aktiviteter knyttet til selve implementeringen kan ha sikkerhetsmessige konsekvenser dersom de ikke håndteres eller avsluttes på en kontrollert måte ved implementeringsfasens slutt. Dette kan for eksempel være å glemme at man laget midlertidige nødløsninger, hardkodet data, benyttet felles brukerkontoer, utsatte enkelte oppgaver, tildelte utvidede rettigheter til personer i prosjektet, i for stor grad lot leverandøren utføre ting uten å sørge for kompetanseoverføring til eget personell, utsatte dokumentasjon av gjennomførte aktiviteter eller konfigurasjoner, hadde midlertidige oppbevaringsplasser for dokumentasjon, etc.

3.5 Gjennomføring av drifts- og forvaltningsfasen

3.5.1 Overlatelse til forretningen/driften

Dersom en midlertidig prosjektgruppe har stått for planlegging, gjennomføring og implementering av anskaffelsen i virksomheten, bør ikke anskaffelsesprosjektet avsluttes før ansvaret for eventuelle forsinkede oppgaver eller tiltak fra implementeringsfasen er overført til personer i forretningen/driften. Prosjektet bør heller ikke avsluttes før det er etablert nødvendige roller og ansvar for drift og forvaltning av produktet/tjenesten som er anskaffet, og før nødvendig opplæring er gitt og relevant dokumentasjon er på plass. Fra et sikkerhetsperspektiv handler overlatelse til forretningen/driften dessuten om å innlemme det anskaffede produkt/tjeneste i virksomhetens styringssystem for informasjonssikkerhet, slik at det inngår i regelmessige risikovurderinger, er gjenstand for sikker endringshåndtering, at leverandør blir gjenstand for revisjoner og kontroller, mv.

3.5.2 Overlate risikostyring fra prosjektet til forretningen/driften

Når anskaffede produkter og tjenester er implementert i virksomheten, overlates ansvaret for risikostyring fra anskaffelsesprosjektet til forretningen eller driften. Merk at et konkret produkt eller tjeneste kan inngå i risikostyring på ulike nivåer og med ulik vinkling. I energilovgivningen er det for eksempel er krav om risikovurdering knyttet til ekstraordinære forhold, risikovurdering for å sørge for adekvat sikring av klassifiserte anlegg, risikovurdering ved endringer i digitale informasjonssystemer, risikovurderinger som muliggjør beskyttelse av driftskontrollsystem mot alle typer uønskede hendelser, risikovurdering for å dimensjonere beredskap, ressurstilgang (personell og utstyr) og redundans i driftskontrollsystem, samt risikovurderinger for å ivareta sikkerhetsnivået i AMS. For alle disse områdene vil det kunne være leverandører som leverer produkter og/eller tjenester og som dermed kan påvirke risikoen, og siden leverandørrelasjonen ofte innebærer en lengre verdikjede på tvers av flere leverandører, som kontinuerlig endrer og tilpasser sine bidrag i verdikjeden, må styring av sikkerhetsrisiko være en kontinuerlig prosess i virksomheten.

Normalt er det systemansvarlig, prosesseier eller fagansvarlig som har best innsikt i sårbarhetene i produkt eller tjeneste, og som dermed har forutsetninger for å gjennomføre grundige risikovurderinger. Ofte er det imidlertid mer relevant å se risikovurderinger i et mer helhetlig perspektiv enn på systemnivå og produktnivå, og ledelsen i virksomheten bør sørge for at det eksisterer ressurser og kompetanse til å gjennomføre helhetlige risikovurderinger som også omfatter integrasjoner og avhengigheter – både internt og i leverandørkjeder.

3.5.3 Revisjon og kontroll av leverandør

Virksomheten skal avtale retten til å gjennomføre revisjon av leverandør eller retten til å kreve at en uavhengig tredjepart gjennomfører slik revisjon hos leverandør. Revisjoner utføres for å kontrollere at leverandør oppfyller kravene i avtalen og at sikkerhetsnivået er som forventet. Hvordan denne retten utøves i praksis og hvordan slike revisjoner gjennomføres, henger ofte sammen med i hvilken grad leverandørs produkt eller tjeneste kan påvirke virksomhetens sikkerhetsnivå og hvor viktig det er for virksomheten at dette ikke skjer. Selv om man ved revisjoner ofte følger et definert sett av prosedyrer og kontrollerer noen forhåndsdefinerte aktiviteter – enten i tråd med allment kjent standard eller egenutviklet metodikk, kan man også gjennomføre mer avgrensede kontroller eller undersøkelser av leverandør. Selv om revisjonen har mindre omfang og ikke følger en formell standard, er det likevel hensiktsmessig å definere og dokumentere metodikk, omfang, mål, ressurser, leverandørens besvarelse og virksomhetens evaluering. For en videre veiledning til gjennomføring av revisjoner, se vedlegg C.

Husk: prioriter revisjoner eller kontroller av leverandør når det skjer større endringer
I utgangspunktet skal revisjoner gjennomføres jevnlig, men det kan særlig være aktuelt å gjennomføre dem ved konkrete milepæler, etter sikkerhetshendelser, ved sårbarheter som gjøres kjent, ved indikasjoner på avvik fra avtalte krav, endring i eierstruktur (fusjoner, oppkjøp), utskiftning av nøkkelpersonell, utskifting av større underleverandører, mangel på varsling eller håndtering av sikkerhetshendelser, etc.

3.5.4 Hendelseshåndtering & øvelser

For de mest kritiske produkter og tjenester skal virksomheten øve på hendelseshåndtering – både hendelser i egen virksomhet og i leverandørs virksomhet. Øvelsene bør dekke scenarier knyttet til tap av henholdsvis tilgjengelighet, integritet og konfidensialitet – avhengig av hva som er relevant for de konkrete produkter og tjenester som anskaffes. I hvilken grad man involverer leverandør i slike øvelser avhenger av hvilken kontroll eller påvirkningskraft leverandøren har på de ulike aspekter som det skal øves på. Merk at det må stilles krav i kravspesifikasjonen om at leverandør skal delta på slike øvelser dersom dette er relevant. I vedlegg A ligger en lenke til NVE sin veileder i hvordan man kan planlegge og gjennomføre øvelser innen kraftforsyningen.

3.5.5 Oppfølging og endring av avtalevilkår

Underveis i et avtaleforhold vil det oppstå behov eller situasjoner som gjør at vilkårene avtalt med leverandør må eller bør endres. Dette kan være på grunn av endringer i de lov- og forskriftskrav virksomheten er underlagt, endringer i virksomhetens organisasjon eller marked som utløser nye eller endrede behov, endringer hos leverandør, eller endringer i teknologi eller trusselbildet. Så lenge man i avtalen har vilkår som regulerer slike endringer, bør de kunne gjennomføres uten større problemer. Uavhengig av årsaken som tvinger frem endring i avtalevilkår, bør virksomheten underveis i avtaleforholdet vurdere om det er behov for å reforhandle vilkårene i avtalen, i tråd med den generelle utviklingen i virksomheten, rammevilkår, leverandørmarkedet, det rådende trusselbildet, teknologibruk, osv.

3.6 Gjennomføring av opphørsfasen

Opphør av en leverandørrelasjon kan komme brått på og er ikke nødvendigvis planlagt eller ventet. Opphør kan for eksempel tvinges frem gjennom mislighold fra leverandørs side, men også på grunn av oppkjøp, endret eierskap eller konkurs. Hvis et selskap blir solgt, helt eller delvis, vil dette kunne ha praktiske og sikkerhetsmessige konsekvenser for virksomheten. Der virksomheten har benyttet standard avtalevilkår, vil det normalt være slik at leverandøren plikter seg å informere virksomheten om forholdet, i tillegg til at det normalt vil være anledning til å si opp avtalen ved slike endringer.

Hva som er årsaken til opphør av avtale, vil også legge føringer for hvordan avviklingen kan og bør gjennomføres. Gjennomføring av nødvendige opprydnings- og saneringstiltak vil kunne være vanskeligere der det er konflikt eller uenighet som er årsaken til opphør, fordi utøvelsen av de avtalte rettigheter i slike situasjoner ofte blir mer problematisk. Likevel er det slik at uansett årsak til opphør, vil avslutningen av avtaleforholdet avhenge av hva som ble avtalt med leverandør i anskaffelsesfasen. Benytter man standard avtalevilkår, vil følgende normalt gjelde:

- Eiendomsrett, opphavsrett og andre relevante materielle og immaterielle rettigheter til data, programvare og maskinvare vil være avtaleregulert.
- Plan, metode, forpliktelser og ansvar for overføring eller tilbakeføring av dokumentasjon, data, programvare og maskinvare er individuelt eller samlet sett avtaleregulert for hhv. i) utløp av avtaleperiode, ii) oppsigelse av avtale og iii) heving av avtale.

I de følgende underkapitler beskrives noen typer av avtaleavslutning og hvilke vilkår som normalt gjelder.

3.6.1 Opphør som følge av utløp av avtale

- En passiv avvikling av avtalen der avtalen opphører automatisk ved en avtalefestet dato.
- Avvikling av avtaleforholdet følger normalt i tråd med hva som er avtalt, men virksomheten bør kontrollere at det som er avtalt faktisk gjennomføres. Mangelfull oppfølging eller anvendelse av avtalte rettigheter, eller mangelfulle forberedelser fra virksomhetens side, kan ha negative følger for sikkerhetsnivået.
- Overføring av data til annen leverandør eller avtalepart eller tilbakeføring i sin helhet til virksomheten, følger omforent plan for avvikling, herunder også evt. destruering av dokumentasjon, data, programvare eller maskinvare.
- Overføring eller tilbakeføring gjennomføres normalt med rimelig bistand fra leverandør, men bør etterspørres av virksomheten.
- Virksomheten skal normalt motta fullverdige tjenesteytelser inntil avtaleforhold er utløpt og håndtering av dokumentasjon, data, programvare og/eller maskinvare er tilfredsstillende fullført.
- En formell erklæring fra leverandøren på at overføring, tilbakeføring eller destruering av relevant dokumentasjon, data, programvare eller maskinvare er gjennomført innhentes. Det samme gjelder dokumentasjon på at tilganger er slettet.

3.6.2 Opphør som følge av oppsigelse

- En aktiv avvikling av avtalen der avtalen opphører som følge av at en part velger å tre ut av avtaleforholdet.
- Styrt og minnelig avvikling av avtaleforholdet er avtalt, men virksomheten kan oppleve at leverandør ikke tar initiativ eller unnlater å utføre aktiviteter som forventet. Etterspør derfor aktiviteter og gjør leverandør oppmerksom på virksomhetens forventninger til avslutning av avtaleforholdet.
- Overføring av data til annen leverandør eller avtalepart eller tilbakeføring i sin helhet til kunde, følger omforent plan for avvikling, herunder også evt. destruering av dokumentasjon, data, programvare eller maskinvare.
- Overføring eller tilbakeføring skjer normalt med rimelig bistand fra leverandør, men bør etterspørres av virksomheten.
- Kunde mottar normalt fullverdige tjenesteytelser inntil avtaleforhold er utløpt og håndtering av dokumentasjon, data, programvare og/eller maskinvare er tilfredsstillende fullført.
- En formell erklæring fra leverandøren på at overføring, tilbakeføring eller destruering av relevant dokumentasjon, data, programvare eller maskinvare er gjennomført innhentes.

3.6.3 Opphør som følge av heving av avtale

- En aktiv avvikling av avtalen der en part hever avtalen som følge av det etter avtalens definisjoner foreligger et vesentlig mislighold eller avtalebrudd fra motparten.
- Avvikling av avtaleforholdet kan i motsetning til utløp eller oppsigelse inneholde en grad av konflikt og motstrid, samt være uforutsett og/eller ikke planlagt. Dette gjør at virksomheten bør være særlig oppmerksom på at avslutningen av avtaleforholdet skjer i tråd med virksomhetens interesse og det som er avtalt mellom partene.
- Overføring av data til annen leverandør eller avtalepart eller tilbakeføring i sin helhet til kunde, herunder også evt. destruering av dokumentasjon, data, programvare eller maskinvare skal gjennomføres på lik linje med øvrige scenarier for avvikling av avtalen. Avhengig av konfliktgrad mellom partene og type brudd eller mislighold som gir rett til heving, må det individuelt for hvert scenario evalueres når, hvordan og i hvilken utstrekning utveksling av sensitiv informasjon skal gjennomføres.
- For visse situasjoner kan det være nyttig å minne leverandør på at den lovpålagte taushetsplikten for kraftsensitiv informasjon også gjelder etter opphør av avtalen.
- I den grad det er mulig, kan overføring eller tilbakeføring bli nødvendig å gjennomføre uten, eller med tvungen bistand fra leverandør.
- Leverandøren kan helt eller delvis motsette normalt fullverdige tjenesteytelser inntil en eller flere ensidig satte betingelser er oppfylt. Ekstrahering av dokumentasjon, data, programvare og/eller maskinvare kan bli krevende og betydningen av virksomhetens etterrettelighet i oppfølgingen av avtaleforholdet blir forsterket.

3.6.4 Opphør som følge av leverandørs konkurs

- Konkurs bør avtalefestes til å gi motparten rett til heving med øyeblikkelig virkning.
- Konkursbo kan velge å tre inn i avtalen som part, og motparten kan da rette evt. krav inn til boet.
- Avtalevilkår regulerer normalt eierskap til data, slik at konkursboet ikke kan selge data videre. I særlige tilfeller bør man gjøre konkursboet oppmerksomme på dette.
- Konkursboet bør gjøres oppmerksom på den lovpålagte taushetsplikten for kraftsensitiv informasjon og begrensningene knyttet til videre deling av denne informasjonen.

3.6.5 Generelle råd knyttet til avtaleregulering av opphør

Ved avtaleinngåelse, bør virksomheten vurdere å:

- Avtale at leverandøren ved avvikling skal sette av ressurser til å gjennomføre overføring, tilbakeføring eller destruksjon av dokumentasjon, data, programvare eller maskinvare, krypteringsnøkler, sertifikater og andre tekniske elementer innen en fastsatt frist.
- Avtale leverandørens kompensasjon eller godtgjørelse for overføring, tilbakeføring eller destruksjon av dokumentasjon, data, programvare eller maskinvare.
- Stille krav om at leverandøren skal utstede en formell erklæring på sletting og sanering etter endt avvikling.
- Tilpasse avtalens varighet til produktet/tjenesten som anskaffes, slik at nødvendig grad av fleksibilitet med hensyn til avslutning avtales. Varighet avtales normalt som en gitt tidsperiode pluss et sett av opsjoner på kortere forlengelser. Vær oppmerksom på eventuelle vilkår om automatisk fornyelse.

Merk at disse momentene ofte dekkes av avtalevilkår som eksisterer i standard avtalemaler, men at de kan være generelle og overordnede. Undersøk derfor om det er nødvendig med en nærmere spesifikasjon for den enkelte avtale.

4 LEVERANDØRKJEDEASPEKTET VED ANSKAFFELSER

4.1 Hva mener vi når vi snakker om leverandørkjeden?

Leverandører av et konkret produkt eller en konkret tjeneste benytter ofte produkter og tjenester fra en eller flere underleverandører for å levere sitt produkt/tjeneste til virksomheten. Disse bidragene fra leverandør og underleverandører utgjør til sammen en kjede leveranser, som til sammen må oppfylle alle leveransekrav for at sluttproduktet eller -tjenesten skal leveres med avtalt kvalitet og til avtalt tidspunkt. Dette gjelder også informasjonssikkerhetsaspektet – alle leveranser må oppfylle sikkerhetskrav for at sikkerhetsnivået i hele leverandørkjeden skal ivaretas. Én hendelse som påvirker sikkerhetsnivået ett sted i kjeden av leverandører eller leveranser, kan påvirke sikkerhetsnivået til virksomheten som har anskaffet det endelige produktet eller tjenesten. I tillegg, kan sammenkobling av produkter og tjenester via kommunikasjonsnettverk utnyttes av ondsinnede aktører, slik at virksomheten angripes eller rammes via angrep på, eller hendelser hos, leverandør eller underleverandør. Dette betyr at virksomheter må være

oppmerksomme på mer enn bare relasjonen til leverandøren man har en avtale med, og vurderer hvordan sikkerhetsrisiko i hele leverandørkjeden kan påvirke virksomheten.

Leverandører flest har en sterk egeninteresse av å levere produkter og tjenester med avtalt sikkerhetsnivå, kvalitet og pålitelighet. Med digitalisering, økt sammenkobling via internett og økt kompleksitet i produkter og tjenester, er det imidlertid større fare for at uautoriserte tredjeparter med ondsinnede intensjoner kan trenge seg inn i leverandørkjeden for å forårsake skade eller oppnå vinning. I tillegg vil utilsiktede feil eller handlinger ett sted i leverandørkjeden, kunne spre seg videre og få negative konsekvenser for virksomheten.

Å håndtere den informasjonssikkerhetsrisiko som leverandørkjeder er eksponert for kan være en vanskelig oppgave for virksomheten. Har virksomheten høy grad av tjenesteutsetting eller sammensatte tjenester, vil det kunne være svært mange leverandører og underleverandører å holde oversikt over. I neste kapittel presenterer vi en del aktiviteter, anbefalinger eller forhold som virksomheten må eller bør ta stilling til for å ha bedre håndtering av leverandørkjederisiko.

4.2 Hvordan følge opp leverandørkjedeaspektet i praksis

4.2.1 Etablere planer, ressurser, roller, ansvar og budsjetter for oppfølging.

- Ledelsen må fastsette ambisjonsnivå for oppfølging av sikkerhetsrisiko forbundet med leverandørkjeden og sette av ressurser og budsjetter for faktisk oppfølging av leverandørkjederisiko.
- Ledelsen bør etablere en policy for håndtering av leverandørrelasjoner, som angir regler for samhandling, hvilke roller som har autorisasjon til å beslutte eller bestille på vegne av virksomheten, krav til reforhandlingsfrekvens, osv. Muntlige avtaler/endringer, spesialbestillinger og særunntak for leverandører bør unngås dersom man ønsker best mulig kontroll.
- Ansvar for oppfølging må etableres formelt, og ansvarlige må tildeles tilstrekkelig med ressurser for å faktisk kunne utøve ansvaret.
- Oppfølging handler eksempelvis om revisjoner, kontraktsoppfølging (varighet, vilkår, etterlevelse, kvalitet, etc.), endringshåndtering, kontroll av tjenestenivå, gjennomgang av tredjeparts revisjonsrapporter, kontroll av underleverandør (avtale, etterlevelse), sikkerhetstesting, utvikling av sikkerhetsarbeidet.
- Sørg for at oppfølging følger en viss systematikk og at den dokumenteres.
- Involver brukere og annet personell som kjenner til leveransen og risiko i løpende risikovurderinger.
- Sørg for at virksomhetens roller knyttet til den enkelte leverandør til enhver tid innehas av personell som kjenner rollens ansvar, f.eks. systemansvarlig, avtaleeier, ansvarlig for mottak av informasjon om sårbarheter og sikkerhetshendelser, osv.
- Ha jevnlige møter med leverandør hvor også sikkerhet er på dagsordenen. Følg aktivt opp etterlevelsen av avtalte sikkerhetskrav, samt kvaliteten på etterlevelsen. Still spørsmål egnet til å avdekke om leverandør kun oppfyller de avtalte krav eller om de selv tar initiativ til et høyt sikkerhetsnivå, kontinuerlig herder produkter/tjenester, har høye ambisjoner knyttet til egen sikkerhetskompetanse, osv.

- Der leverandør er av en type som i liten grad tilbyr oppfølgingsmøter, etterspør åpne revisjonsrapporter, status for sertifiseringer, informasjon om gjennomførte sikkerhetstester samt planer for utvikling av sikkerhetsarbeidet.

4.2.2 Skaff oversikt over leverandørkjeden

- Etabler en oversikt over alle leverandører og underleverandører, som oppdateres løpende ved endringer.
- For de mest kritiske produkter og tjenester, bli kjent med leverandører og underleverandørers produkter og tjenester, kompetanse, organisering, geografisk lokalisering, eierstruktur, hvilke sikkerhetsrelaterte lover/forskrifter som regulerer virksomheten deres, osv.
- For de mest kritiske produkter og tjenester, etabler og oppretthold en oversikt over eventuelle ytelser eller leveranser fra underleverandør som er en betingelse for leverandørens oppetid eller ytelse.
- Hold oversikt over hvilke interne prosesser og aktiviteter som er avhengig av leveransene fra den enkelte leverandør.
- Dokumentasjon bør eksistere i et oversiktlig format, og ikke i selve avtaledokumentene.
- Tilpass omfanget av leverandøroppfølging til det kritikalitetsnivået tjenesten/produktet har for virksomheten.

4.2.3 Avtaleinngåelse og -oppfølging

- Sørg for at ivaretakelsen av sikkerhetsnivå er regulert i juridisk bindende avtale. Sikkerhetskrav for de konkrete leverandører og de konkrete produkter/tjenester, identifiseres gjennom en risikovurdering som tar hensyn til forretningens behov, anskaffelsens egenskaper, og det rådende trusselbildet.
- Still krav til leverandør om at de skal avtale sikkerhetskrav med sine underleverandører. Be om kopi av sikkerhetskrav avtalt med underleverandør ved leveranser hvor sikkerhetsrisikoen er av et visst omfang.
- Still krav om at leverandør skal opplyse om hvilke underleverandører de benytter, hva de leverer og fra hvilke geografiske lokasjoner underleverandørene utfører leveransen.
- Ha system og plan for dokumentasjon av endringer i avtalte vilkår og leveringsbetingelser.
- Avklar eventuelle vage eller uklare beskrivelser/dokumentasjon fra leverandørs besvarelse av krav, særlig med hensyn til hvilke underleverandører som benyttes, hva de leverer, hvordan leveransen er organisert, osv.

4.2.4 Hvordan dokumentere sikkerhetsnivå?

- Problemstillinger knyttet til dokumentasjon gjelder både dokumentasjon av kravetterlevelse i anskaffelsesfasen, og dokumentasjon av kravetterlevelse og sikkerhetsnivå i drifts-/forvaltningsfasen.

- Når virksomheten spesifiserer hvilken dokumentasjon tilbyder/leverandør må presentere for å verifisere eller sannsynliggjøre at de og eventuelle underleverandører oppfyller sikkerhetskrav, må virksomheten vurdere hva som er mulig å dokumentere og hva som er nødvendig å dokumentere.
- Først og fremst skal man be om dokumentasjon relatert til tilbyderens/leverandørens virksomhet. Kun der den konkrete anskaffelsen utgjør en særlig sikkerhetsrisiko knyttet til ytelsen/leveransen fra en underleverandør, kan man be tilbyder/leverandør legge frem dokumentasjon egnet til å verifisere eller sannsynliggjøre at sikkerhetsnivået er akseptabelt.
- Det kan være vanskelig å verifisere at sikkerhetskrav eller -andre forhold er oppfylt gjennom skriftlig eller visuell dokumentasjon. Er risikoen lav eller middels, bør virksomheten nøye seg med tilbyders/leverandørs beskrivelse og egenerklæring.
- Dersom det er relevant for en konkret anskaffelse, kan virksomheten stille som krav at de skal kunne gjennomføre besøk hos tilbyder/leverandør eller at de skal settes i kontakt med tidligere eller eksisterende kunder av tilbyder/leverandør. Virksomheten kan også be om å få live-demo av sikkerhetsfunksjonalitet dersom relevant og gjennomførbart.
- Virksomheten bør kreve dokumentasjon fra nøytral tredjepart, eksempelvis resultater fra revisjoner eller sikkerhetstester utført av tredjepart dersom slike foreligger.
- Ikke be om sertifiseringer som beviser at konkrete sikkerhetsstandarder oppfylles dersom det ikke er nødvendig for tjenesten/produktet. For strenge krav kan gjøre at få tilbydere/leverandører oppfyller kravet.
- Underveis i avtaleforholdet kan virksomheten gjennomføre mer uformelle undersøkelser for å få et bedre inntrykk av leverandørens ambisjonsnivå med hensyn til sikkerhet, eksempelvis omtale av leverandør i offentlige fora, leverandørens finansielle posisjon, samtaler med andre kunder av leverandør, leverandørens utviklingsplaner, prioriteringer og tjenestetilbud, m.m.

4.2.5 Risikobasert tilnærming

- Dersom det er begrenset med ressurser tilgjengelig for oppfølging av leverandørkjeder, bør oppfølging prioriteres ut ifra hvor kritisk eller viktig produktet/tjenesten er for virksomhetens drift og hvilken informasjonssikkerhetsrisiko som står på spill.
- Selv om informasjonssikkerhetsrisiko i leverandørkjeden kan være vanskelig å vurdere fordi man ikke har nok kunnskap eller tilgjengelig informasjon til å gi et realistisk anslag på sannsynligheten for ulike forhold eller hendelser, må virksomheten være rustet til både å håndtere hyppige og sannsynlige situasjoner og ekstraordinære situasjoner med antatt lav forekomst.
- Direktekontroll/-revisjon av underleverandører bør begrenses til særlige tilfeller, eksempelvis ved indikasjoner på at leverandør ikke har fulgt opp konkrete hendelser eller avvik som tilsier at det er manglende etterlevelse av sikkerhetskrav. Ellers bør virksomheten i størst mulig grad benytte seg av vilkårene avtalt med leverandør, som sier at leverandør skal pålegge underleverandører tilsvarende sikkerhetskrav.

- Over tid bygges tillitsbaserte relasjoner til enkelte leverandører og personell hos leverandøren. Slik tillit kan være viktig for kvaliteten i arbeidet, men kan også utgjøre en sårbarhet som kan utnyttes av en utro tjener eller ondsinnet tredjepart. Sørg derfor for at det i alle leverandørrelasjoner eksisterer en viss grad av kontroll eller oppfølging av informasjonssikkerhet.

Er leverandør eller underleverandør underlagt eksplisitte sikkerhetskrav i lov eller forskrift, bør virksomheten utnytte dette i relasjonen til leverandør ved å henvise til regelverk, undersøke om de virker å ha gode prosesser for å etterleve krav (jf. internkontrollsystem for sikkerhet), kartlegge hvordan aktuell forvaltningsmyndighet følger opp pliktsubjektene, osv. Merk at leverandør kan være underlagt taushetsplikt som gjør at virksomheten ikke kan gis innsyn i alle typer informasjon.

Husk: også mindre tjenester kan forårsake stor skade dersom de kompromitteres
Informasjonssikkerhetsrisiko er ikke nødvendigvis størst for de mest kritiske produkter/tjenester. Ha derfor også kontroll på sikkerhetsnivået i mindre applikasjoner, API-er, spesialavtaler knyttet til bruk av data, utvidede tilgangsrettigheter til enkeltpersoner, spesialprosjekter/piloter, etc.

4.2.6 Opprettholde oversikt over leverandørs virksomhet

- Etabler system og praksis for overvåking av endringer, slik at den oversikt som er etablert faktisk holdes oppdatert.
- Prioriter å ha oversikt over endringer med betydning for virksomheten, eksempelvis endring i type produkt/tjeneste som leveres og medfølgende endring i intern kompetanse, endring i markeder det opereres i og medfølgende endring i satsingsområder, større endring i eierstruktur eller organisering, endring i tjenestenivå og/eller prisbetingelser, osv.
- Virksomheten bør gjennomføre jevnlige kundemøter med leverandør for å holdes informert om bl.a. leverandørs utviklingsplaner og ambisjonsnivå – både på generelt grunnlag og for det konkrete produkt/tjeneste.

4.2.7 Sårbarhetshåndtering

- Virksomheten bør legge til rette for mottak og håndtering av informasjon om sårbarheter i programvare og programvarekomponenter. Slik informasjon mottas direkte fra leverandør, via KraftCERT eller andre publiseringskanaler, og mottatt informasjon må kontrolleres opp mot de produkter og tjenester som er i bruk av virksomheten og virksomhetens leverandører.
- Bygg opp en best mulig oversikt over hvilke bestanddeler (programvare, programvarekomponenter, kode, etc.) konkrete produkter/tjenester består av, slik at virksomheten kan respondere på sårbarheter som gjøres kjent.
- Der slik oversikt er mangelfull, bør det etableres en rutine med definerte roller og ansvar som brukes for å avklare om virksomhetens produkter/tjenester, leverandører eller underleverandører er eksponert for konkrete sårbarheter som gjøres kjent. Se merknad om *Software Bill of Material* under.

- Sårbarheter med størst konsekvens for virksomheten prioriteres først. Der håndtering av ulike grunner er vanskelig, bør risiko ved manglende håndtering dokumenteres.
- Virksomheten må avtale med leverandør at henvendelser om sårbarheter krever umiddelbar respons, både med hensyn til avklaring av om de er eksponert for den konkrete sårbarheten og med hensyn til patching eller andre tiltak dersom nødvendig.
- Virksomheten må ha tydelige planer og prosedyrer for håndtering av kritiske sårbarheter i OT-miljøet, både med hensyn til eventuelt behov for isolasjon av de eksponerte deler og med hensyn til håndtering. Patching i OT-miljøer krever ofte grundig planlegging og gjennomføring for å forhindre utilsiktede konsekvenser for driften.

Husk: *Software Bill of Materials* – oversikt over bestanddeler i programvare og tjenester
Software bill of materials (SBOM) er betegnelsen på en standardisert og maskinlesbar oversikt over alle bestanddeler i en konkret programvare eller applikasjon, samt deres versjoner, sikkerhetsreferanser, og annen relatert informasjon. SBOM kan inneholde åpen kildekode og proprietær programvare. Med en oppdatert SBOM, kan virksomheten raskt avdekke hvorvidt den er eksponert for konkrete sårbarheter og dermed raskt iverksette tiltak – enten ved at leverandør varsler virksomheten basert på innholdet i den konkrete SBOM eller at denne er åpent tilgjengelig for virksomheten. Selv om dagens SBOM-verktøy er mer tilpasset store og komplekse organisasjoner, er det ventet at SBOM innen få år vil være mer utbredt i samfunnet. Selv om virksomheten ikke selv forvalter en egen SBOM, vil det i hvert fall være noe man trolig vil komme til å stille krav om at tilbydere av programvare og applikasjoner har.

4.2.8 Trusselanalyser

- Det kan være utfordrende for virksomheten å selv gjennomføre trusselanalyser, men flere nasjonale og internasjonale aktører publiserer årlige trusselvurderinger. Det anbefales å basere egne kartlegginger eller vurderinger på trusselvurderinger fra KraftCERT og norske myndigheter – husk at mange aktører som tilbyr trusselanalyser også tilbyr sikkerhetstjenester for å håndtere nettopp de truslene de trekker frem.
- Et trusselscenario er en beskrivelse av hvordan en sårbarhet kan utnyttes, slik at en uønsket hendelse forårsakes. Når virksomheten analyserer trusler mot leverandørkjedene sine, anbefales det å prioritere scenarier som hyppig har forekommet, deretter kan man identifisere scenarier som er mulige, men som sjelden har vært observert. Husk at virksomheten også skal være rustet til å håndtere ekstraordinære situasjoner.
- Vær oppmerksom på at ny eller endret bruk av teknologi og nye praksiser for sosial samhandling ofte etablerer nye sårbarheter som utnyttes av trusselaktører. Trusselaktører etterligner ofte legitime aktiviteter og benytter legitime verktøy.
- Av praktiske grunner kan det være nyttig å skille mellom trusselaktørers kapasitet, evne, ressurser, osv. Enkelte trusselaktører er opportunister som gjennomfører

tilfeldige forsøk inntil de lykkes, mens andre trusselaktører planlegger et målrettet angrep over lengre tid. Leverandørkjedeangrep er en vei inn i virksomheten.

- Også utilsiktede handlinger utgjør en trussel. Vanvare, forsømmelse eller uaktsomhet hos leverandør eller underleverandør, kan resultere i uønskede hendelser på grunn av manglende sikkerhetskontroller, kompetanse, ressurser eller lignende.

4.2.9 Håndtering av hendelser i leverandørkjeden

- Uønskede hendelser kan både være et resultat av ondsinnede handlinger mot leverandøren eller leverandørkjeden, og avvik som følge av forsømmelse eller utilsiktede handlinger på leverandørens side.
- Virksomheten må i avtalen med leverandør avtale at leverandør skal kunne håndtere uønskede hendelser på en måte som minimerer negative konsekvenser for ytelse og sikkerhet, men virksomheten må også sørge for at det som er avtalt faktisk gjennomføres når uhellet er ute.
- Leverandør kan ha en intensjon om å varsle kunder, uten at de faktisk har en policy, rutine eller et system for å gjøre dette. Still spørsmål til leverandør om hvilken policy og rutine de har for varsling dersom de utsettes for en uønsket hendelse av et visst omfang.
- Ved enhver ny anskaffelse, må virksomheten sørge for at relasjonen til den gjeldende leverandøren også dekkes av virksomhetens egne rutine og system for håndtering av uønskede hendelser hos leverandør eller underleverandør. Ved å ha god oversikt over integrasjoner og avhengigheter for ulike produkter og tjenester, kan virksomheten raskt avklare hvordan en konkret hendelse potensielt kan ramme.
- Noen ganger får man varsel om hendelser hos leverandør eller underleverandør fra andre kanaler enn fra leverandøren selv. Ved uoversiktlighet eller ubekreftede meldinger, bør virksomheten vurdere å iverksette «føre var»-tiltak, som nedstenging eller isolasjon av tjenester, deaktivere brukerkontoer, iverksette planer for alternativ drift, osv., samtidig som de oppretter kontakt med leverandør.
- Hendelser skal håndteres i tråd med hendelsens alvorlighetsgrad, men noen ganger kan det ta tid før alvorlighetsgraden blir kjent for leverandøren. For å unngå at konsekvensene blir større som følge av sen reaksjonsevne, bør leverandører oppmuntres til å varsle om hendelser selv om potensielle konsekvenser foreløpig er ukjente. Leverandør bør også oppmuntres til å gi løpende statusoppdateringer (også når det ikke er noe nytt å melde) med jevne mellomrom.
- For de mest kritiske produkter/tjenester bør virksomheten vurdere å involvere leverandør i beredskapsøvelser. Som minimum må det kontrolleres at kommunikasjonskanaler fungerer som planlagt og at kontaktpersoner kan nås.
- Der en leverandør rammes av en uønsket hendelse som ikke rammer virksomheten selv, men som påvirker andre kunder negativt, bør virksomheten etterspørre en rapport om hendelsen (årsak, håndtering, evaluering, etc.).

4.2.10 Revisjoner og kontroller bakover i leverandørkjeden

Hvordan man skal revidere krav underveis i avtaleforholdet, samt hvordan man skal gå frem for å undersøke om leverandør (og underleverandør) faktisk oppfyller sine plikter kan være

utfordrende å gjennomføre. Generelt sett blir slike problemstillinger vanskeligere å håndtere, jo lenger bak i leverandørkjeden man beveger seg, både på grunn av avtalerettslige begrensninger, manglende oversikt og på grunn av manglende ressurser eller kapasitet.

At leverandørkjederisiko av ulike grunner kan være vanskelig å vurdere og håndtere, er i seg selv en del av risikoen ved anskaffelser. For å håndtere leverandørkjederisikoen best mulig, må virksomheten prioritere vurdering og håndtering av den risiko som er mest kritisk for virksomhetens drift og informasjonsforvaltning.

Ved høy restrisiko bør virksomheten dessuten iverksette tiltak som reduserer konsekvensen ved å være avhengig av leverandørers pålitelighet og sikkerhetsnivå, slik som løsninger for alternativ drift, osv.

I tillegg til å gjennomføre revisjoner og kontroller, eksempelvis slik som beskrevet i vedlegg C, bør virksomheten:

- Samarbeide med leverandør for å øke sikkerhetskompetanse og -bevissthet for den konkrete leveransen og hos den konkrete leverandøren. Bygg gode relasjoner med leverandør – still krav og bistå med hjelp på forespørsel.
- Etterspørre kontroll av konkrete deler av leverandørs styringssystem for informasjonssikkerhet (risikostyring, endringshåndtering, utviklingsmiljø, leverandøroppfølging, identitets- og tilgangsregime, osv.).
- Ta i bruk avtalte bestemmelser om prisavslag, erstatning eller reforhandling dersom leverandør eller underleverandør opptrer klanderverdig sikkerhetsmessig.
- Bygge opp forståelse for relevante trusler mot leverandørkjeden, gjennom trusselrapporter fra åpne kilder, kartlegging av faktiske hendelser, osv.
- Etablere bransjesamarbeid med andre kunder av leverandør og bruk kundemakt til å påvirke leverandørs sikkerhetsarbeid.

4.2.11 Løpende kontroller og testing

- Gjennomføre sikkerhetstester i samarbeid med leverandør, herunder pen-tester mot relevante deler av leverandørkjeden.
- Ha periodevis gjennomgang av leverandørens tilganger til virksomhetens miljø/ressurser og fjerne tilganger som ikke er nødvendige.
- Etterspørre leverandørens oppfølging av egne underleverandører.
- Følg opp leverandørens utviklingsarbeid og planer innen sikkerhet.

4.2.12 Leverandørkjedeangrep og motstandsdyktighet

- Forberede virksomheten på at man *kan* rammes av cyberangrep direkte eller via leverandørkjeden, gjennom å øve på bruken av planverk/rutiner for håndtering av situasjoner med tap av konkrete tjenester/produkter.
- Slik forberedelse handler også om skademinimering, gjennom blant annet å:
    - Segmentere virksomhetens miljø for å gjøre det vanskeligere for angripere å bevege seg rundt. Ha kontroll over avhengigheter mellom IT- og OT-miljø.

- Ha rutiner for systematisk sikkerhetsoppdatering og sikkerhetskopiering.
- Redusere angrepsflaten gjennom å begrense administratorrettigheter og synlighet fra internett, ha flerfaktor autentisering på internetteksponerte tjenester.
- Overvåke av inngående og utgående trafikk og ha varsling når terskelverdier passeres.
- La sikkerhetskopier være beskyttet mot overskriving og endring.

- Forberedelse må også innebære oppbygging av evnen til å reagere og ta beslutninger selv om informasjonen er mangelfull eller usikker.
  - Ha oversikt over leverandørkjeden og avhengigheter slik at det raskt kan avklares hva som eventuelt rammes av en konkret hendelse.
  - Gjør det tydelig overfor leverandør at det forventes en proaktiv holdning til varsel om hendelser.
  - Etabler interne prinsipper som alltid skal gjelde ved ekstraordinære hendelser, slik at beslutninger kan tas raskt og effektivt. Slike prinsipper kan eksempelvis dreie seg om føre-var-prinsipper for nedstenging/frakopling av anskaffede tjenester, praksis for prioritering av håndtering/gjenoppretting, avklare hvem som skal kommunisere med leverandørs representant, etc.

4.2.13 Reforhandling av avtalevilkår og sikkerhetskrav

- Dersom avtalevilkår skal revideres eller reforhandles, vurder også om endringer i tjenesten/produktet eller endringer i det rådende trusselbildet, teknologibruk, etc. innebærer at sikkerhetskrav bør endres.
- Avtale må ha rom for vilkårsendringer som følge av endring i lovgivning eller rettspraksis, og virksomheten må faktisk følge opp dette dersom nødvendig.

4.2.14 Sikkerhetspolitikk og leverandøravhengighet

- Virksomheten bør være forberedt på plutselig bortfall av produkter og tjenester, jf. leverandørforbud i forbindelse med krigshandlinger, logistikksvikt under pandemi, produktmangel på grunn av råvaremangel, rask utfasing av produkter/tjenester på grunn av rask teknologiomlegging, etc.
- Slike forberedelser kan handle om å bygge opp reserve-/beredskapslager, etablere oversikt over alternative tilbydere, gjøre seg mindre avhengig av enkeltleverandører, bidra til å bygge opp leverandørmarkeder i land man inngår i et interessefellesskap med, etc.
- Særlig når produkter/tjenester har lang levetid er det risiko for at sikkerhetspolitiske forhold endrer seg betraktelig fra situasjonen slik den var ved avtaleinngåelse, planlegg derfor risikostyring og beredskap deretter for slike produkter/tjenester.

4.2.15 Når opphør skjer brått eller uplanlagt

- Noen ganger kan opphør av en leveranse eller avtale komme brått og uplanlagt, for eksempel på grunn av alvorlig mislighold fra leverandørens side, stans i leveransen av produktet/tjenesten eller konkurs. Der opphør skjer av slike grunner, bør

virksomheten være særlig nøye med å følge opp at tilbakelevering av data, avslutning og opprydding, etc. skjer i tråd med avtalen og at sikkerhetsrisiko håndteres på en kontrollert måte.

- Selv om avtalevilkår regulerer leverandørens plikter også i ekstraordinære situasjoner, kan det være lurt å minne leverandør på at taushetsplikten også gjelder etter opphør av avtale.

4.2.16 Informasjonsdeling innad i bransjen

- Dersom virksomhetene i kraftforsyningen støtter opp om KraftCERT som delingsplattform for sikkerhetsrelatert informasjon, vil det styrke informasjonsdeling og læring i bransjen som helhet.
- Virksomheter bør oppfordre leverandører til å være åpne om sikkerhetsrelaterte hendelser, men respektere behovet for å beskytte sensitiv informasjon inntil sårbarheter er lukket og hendelser håndtert. KraftCERT har prosedyre for å dele informasjon anonymt med bransjen, så leverandør kan på generelt grunnlag oppfordres til å dele direkte med KraftCERT.

5 KRAVSPESIFIKASJON INFORMASJONSSIKKERHET

5.1 Generelt om kravstillelse

Hvor detaljert man er i kravspesifikasjonen når det gjelder sikkerhetskrav, avhenger av hvilke verdier som står på spill, bestemmelser i lov/forskrift, egenskaper ved anskaffet produkt/tjeneste og potensiell risiko. Hvilke krav som stilles for den enkelte anskaffelse, er dermed noe som må vurderes i det konkrete tilfellet. Likevel finnes det en del sikkerhetskrav som nesten alltid stilles til leverandører som gis tilgang til, eller råderett over virksomhetens informasjon og/eller system, og disse listes i kapittel 5.2 under. For den konkrete anskaffelsen må virksomheten selv avklare hvilke av kravene i listen som er nødvendige, tilpasse den enkelte formuleringen, avklare om noen av kravene skal angis som kvalifiseringskrav og om noen skal være evalueringskrav, samt formulere eventuelt krav til dokumentasjon. Merk at kapittel 5.2 ikke inneholder krav som normalt reguleres i selve hovedavtalen. I de formulerte kravene i kapittel 5.2 benyttes benevnelsen «Kunde» for å omtale virksomheten som foretar anskaffelsen, slik man ofte gjør i kravspesifikasjoner.

Husk: samkjør alltid sikkerhetskrav med andre typer krav for å unngå doble eller tvetydige krav
Enkelte sikkerhetskrav vil ofte overlappe med tekniske spesifikasjoner, funksjonelle krav eller generelle avtalevilkår, så det er viktig at de ulike kravstillerne er samkjørte ved utformingen av krav

Ved en anskaffelse stiller man både krav til sikkerhetsnivået i produktet/tjenesten og til sikkerhetsnivået i leverandørens virksomhet. Enkelte sikkerhetskrav er aktuelle eller viktige å spesifisere først når en anskaffelse oppfyller konkrete betingelser. I kapittel 5.3 under er det listet opp en del slike betingelser og hvilke krav som bør formuleres i anskaffelser der disse

er gjeldende. Disse listene er imidlertid ikke fullstendig dekkende for hvilke krav som må eller bør stilles. Generelt sett gjelder det at valg av sikkerhetskrav avhenger av det anskaffede produktet eller tjenestens egenskaper, omfang, verdi/kritikalitet for virksomheten, tilgjengelighetsbehov, leveransemåte, driftsmodell, kompleksitet, egenskaper, bruksområde/-formål, kritikalitet, omfang, konfidensialitetsbehov, forskriftskrav osv.

5.2 Krav som bør stilles uavhengig av hva som anskaffes

Kravene beskrevet i dette kapittelet vil være relevante for de fleste typer anskaffelser og vil som oftest stilles som «må»-krav for at virksomheten skal kunne godtgjøre at de har pålagt leverandør å opprettholde eller forbedre sikkerhetsnivået til virksomheten. Likevel må virksomheten for den enkelte anskaffelse sørge for at utvalget av krav som tas med, samt beslutningen om hvorvidt kravet skal være et «må»- eller «bør»-krav, står i forhold til det som skal anskaffes (type produkt/tjeneste, driftsmodell (hvor stor råderett gis leverandør/underleverandør), omfang, kompleksitet, kritikalitetsnivå, etc.), og at det ikke stilles for mange eller for detaljerte krav. For strenge krav kan begrense konkurransen og føre til at tilbydere lar vær å levere tilbud. Kravene i kapittelet er formulert slik at de i stor grad kan benyttes direkte i en kravspesifikasjon, men virksomheten må selv vurdere om det er nødvendig med omformulering eller tilpasning. Virksomheten kan også variere dokumentasjonskrav ut ifra de konkrete egenskapene og sikkerhetsrisiko knyttet til produktet/tjenestene, og må passe på at dokumentasjonen man ber om faktisk er mulig å fremskaffe eller presentere. Merk at kravene er knyttet til sikkerhet i snever forstand og at tekniske krav og krav til tjenestenivå ikke dekkes.

5.2.1 Styringssystem for informasjonssikkerhet

Leverandør skal ha et styringssystem for informasjonssikkerhet i egen virksomhet, som bidrar til å håndtere tilgjengeligheten, konfidensialiteten og integriteten til Kundes informasjon, tjenester og/eller løsninger som leveres til Kunde. Styringssystemet bør være i tråd med internasjonalt anerkjente standarder og anbefalinger.

Dokumentasjon: gi en overordnet beskrivelse av styringssystemet, beskriv den viktigste styrende dokumentasjonen, angi de viktigste roller og tilhørende ansvar, beskriv hvordan styringssystemet dekker den konkrete leveransen og presenter eventuelle sertifiseringer, revisjonsrapporter, osv.

Merk: dette er et generelt krav om eksistensen av et slikt styringssystem, mens påfølgende krav ofte er en del av et slikt styringssystem. Virksomheten må avklare hva som er hensiktsmessig med hensyn til sammenslåing av krav.

5.2.2 Innsyn i informasjon relevant for virksomhetens sikkerhetsnivå

Leverandør skal gi Kunde innsyn i den overordnede sikkerhetsarkitekturen i Leverandørs virksomhet og/eller for tjenesten/løsningen som leveres til Kunde, samt annen informasjon som indikerer hvordan Kundes sikkerhetsnivå er eksponert gjennom tjenesten/løsningen.

Dokumentasjon: overordnet beskrivelse og/eller visuell fremstilling av sikkerhetsarkitekturen (for eksempel beskrivelse av perimeterbeskyttelse, implementering av brannmurer, inntrengingsdeteksjonssystemer og andre sikkerhetsmekanismer som beskytter nettverksgrensesnittet mot uautorisert tilgang), relevant sikkerhetsinformasjon virksomheten kan stille til rådighet, osv.

Husk: leverandører kan ha legitime grunner til å unnta opplysninger om interne sikkerhetsforhold fra innsyn

Opplysninger om sikkerhetsarkitektur og sikkerhetsnivå i leverandørens egne virksomhet kan utgjøre sensitiv informasjon som kan skade leverandørs virksomhet og/eller andre kunder av leverandøren dersom den blir kjent for uvedkommende. Noen virksomheter vil vegre seg for å dele slike opplysninger og virksomheten bør derfor være påpasselig med å ikke be om mer informasjon enn det som er nødvendig for å kunne verifisere at sikkerhetsløsninger og sikkerhetsnivå er som forventet. Der virksomheten likevel får tilgang til slike opplysninger, må disse behandles med passende sikkerhetsnivå.

5.2.3 Eierskap til informasjon

All informasjon og data som Leverandør får tilgang til er Kundes eiendom og skal ikke deles med andre eller brukes til andre formål utover det avtalte, uten virksomhetens eksplisitte samtykke. Leverandør skal ikke bruke Kundes informasjon til å forbedre sine tjenester eller til annet formål uten eksplisitt samtykke fra virksomheten.

5.2.4 Risikostyring, trussel- og sårbarhetsanalyser

Leverandør skal ha en prosess for løpende identifikasjon, vurdering og håndtering av sårbarheter og trusler som Leverandørens virksomhet og som produkter/tjenester til Kunde er eksponert for. Sårbarheter eller identifisert risiko egnet til å påvirke Kundes sikkerhetsnivå skal varsles til Kunde uten ugrunnet opphold.

Dokumentasjon: beskriv prosess for trussel- og sårbarhetsanalyser og hvordan denne inngår i Leverandørens risikostyring, vise til konkrete sårbarheter og beskrive hvordan disse ble håndtert, osv.

5.2.5 Bruk av underleverandører

Der Leverandør benytter underleverandør/-er for å levere tjenesten/produktet til Kunde, og underleverandørs leveranser er egnet til å påvirke Kundes sikkerhetsnivå, skal Leverandør pålegge underleverandøren/-e krav til informasjonssikkerhet tilsvarende de selv er underlagt gjennom denne avtale. Leverandør skal på forespørsel dokumentere at underleverandør er pålagt tilsvarende sikkerhetskrav.

Dokumentasjon: innsyn i avtaler med underleverandør, innsyn i revisjonsrapporter, dokumentasjon av hvilke underleverandører som benyttes og hva de leverer, beskrivelse av prosess for varsling ved endring i bruk av underleverandør.

5.2.6 Geografisk lokasjon for behandling av informasjon, tjenesteytelse og/eller produktleveranse

Kundes data/informasjon skal kun behandles i, herunder aksesseres fra land i [*sett inn beskrivelse av geografisk avgrensning*]. Kravet innebærer også at tjenesteytelser kun skal utføres fra slike land.

Opsjon: Kunde kan unntaksvis, for enkelte og mindre deler av tjenesten, akseptere behandling i land utenfor det angitte området, så fremt behandlingen i slike land er i tråd med den lovgivning som Kunde er underlagt. Slike unntak skal være gjenstand for Kundes vurdering og eksplisitte samtykke.

Dokumentasjon: vennligst bekreft og opplys om den geografiske lokaliseringen av datasenterressurser og underleverandører som benyttes for å levere tjenesten og/eller produkter.

Merk: energilovgivningen setter ingen eksplisitte begrensninger for geografisk lokasjon for behandling av kraftsensitiv informasjon, men der en anskaffelse også innebærer behandling av personopplysninger, vil personopplysningslovens bestemmelser kunne være førende for mulighetene innen geografisk lokasjon for behandling av informasjon/data og/eller leveranse av tjenesteytelser. Der en anskaffelse innebærer behandling av personopplysninger, kan formuleringen ovenfor inneholde den nevnte opsjonen.

Merk: for leveranser til driftskontrollsystemer klasse 2 og 3 tillater energilovgivningen kun utenlandske leverandører fra land som er medlem i EFTA, EU eller NATO.

Merk: enkelte tjenester har behov forkort latens («latency»), noe som også vil kunne være førende for hvor en tjeneste leveres fra geografisk.

5.2.7 Opprettholdelse av sikkerhetsnivået over tid

Leverandør skal ha et regime for å opprettholde eller forbedre sikkerhetsnivået i egen virksomhet og/eller i tjenesten/produktet over tid, i tråd med den teknologiske utviklingen og det rådende trusselbildet.

Dokumentasjon: beskriv overnevnte regime.

5.2.8 Sikkerhetsoppdateringer/patching

Leverandør skal ha et regime for sikkerhetsoppdateringer og herding av produkter og/eller tjenester som leveres til Kunde, og dette skal bidra til at sårbarheter identifiseres og håndteres på en effektiv måte. Leverandør skal sørge for at utrulling av oppdateringer planlegges og gjennomføres på en måte som minimerer forstyrrelse av ytelsen overfor Kunde.

Dokumentasjon: beskriv regimet for sikkerhetsoppdateringer og distribusjon av disse.

5.2.9 Tilgangsstyring

Leverandør skal ha et regime for tilgangsstyring, herunder brukerkontoadministrasjon, identifisering og autentisering, brukerkontroll og autorisering. For autentisering skal leverandør tilby sterke og anerkjente autentiseringsmetoder.

Dokumentasjon: beskriv regimet for tilgangsstyring, beskriv bruken av administratorrettigheter, beskriv policy for autentisering, osv.

5.2.10 Sikkerhetskopier

Leverandør skal ta sikkerhetskopi av informasjon/data, programvare, konfigurasjonsfiler, loggfiler, systemdokumentasjon, etc. relevant for leveransen. Gjenoppretting fra sikkerhetskopier skal testes regelmessig.

Dokumentasjon: beskriv rutiner for sikkerhetskopiering, inkludert rutiner for tilgang til disse. Beskriv hvordan sikkerhetskopiene er beskyttet og oppbevart. Beskriv test av gjenoppretting fra sikkerhetskopi.

Merk: det kan være særskilte forhold ved den konkrete anskaffelsen som krever at man spesifiserer nærmere hvor hyppig sikkerhetskopi skal tas, hvor den skal oppbevares, krav til

konfidensialitet, tilgjengelighet, integritet, oppbevaringsvarighet, hvor ofte den skal testes, mv.

5.2.11 Separasjon mellom kunder

Der Leverandør benytter servere/datasenterressurser for å levere en tjeneste, skal det eksistere separasjon fra andre kunder slik at kompromittering av andre kunder ikke påvirke Kunde og slik at datalekkasje forhindres.

Dokumentasjon: beskriv hvordan leverandør sørger for slik separasjon mellom kundene.

5.2.12 Sikring av data under lagring, prosessering og overføring

Der det er relevant for tjenesteleveransen, skal Leverandør sørge for at Kundes data beskyttes mot uautorisert tilgang og endring, under lagring, prosessering og overføring.

Opsjon: ved behov kan Leverandør spesifisere mer detaljerte krav til krypteringsnivå og regime for håndtering av krypteringsnøkler, og slike krav spesifiseres i henhold til et slikt behov.

Dokumentasjon: beskriv regimet for beskyttelse av data mot uautorisert tilgang og endring.

5.2.13 Regime for endringshåndtering («change management»)

Leverandør skal håndtere endringer slik at de ikke introduserer utilsiktede feil eller sårbarheter i leveransen til Kunde.

Dokumentasjon: beskriv regimet for endringshåndtering.

5.2.14 Sikker utvikling av produkter og tjenester

Leverandøren skal ha et regime for sikker utvikling («secure development lifecycle») av produkter og/eller tjenester som leveres til Kunden, herunder separate miljøer for utvikling, test og produksjon, samt test av alle utviklingsoppgaver før produksjonssetting.

Dokumentasjon: beskriv regimet for sikkerhet i utvikling av produkter og/eller tjenester. Henvis til eventuelle rammeverk eller metoder for sikker utvikling som benyttes.

Merk: å stille krav om et veldefinert og systematisk regime for sikker utvikling er trolig mest vanlig overfor leverandører som driver med utvikling av programvare. Likevel bør alle virksomheter som driver med utviklingsoppgaver generelt sett ha en viss systematikk i gjennomføringen av disse, for å redusere faren for å utilsiktet etablere feil eller sårbarheter. Å ha separate miljøer for utvikling, test og produksjon, samt å teste før produksjonssetting bør de fleste leverandører ha på plass.

5.2.15 Bakgrunnssjekk av personell.

Leverandøren skal ha en prosess for bakgrunnssjekk av personer som Leverandør ansetter og/eller leier inn. Slik bakgrunnssjekk håndteres typisk gjennom identifisering og autentisering, verifisering av innhold i CV, sjekk av referanser, etc.

Dokumentasjon: beskriv regimet for bakgrunnssjekk av personell.

5.2.16 Sikkerhetsopplæring og bevissthetstrening

Leverandøren skal gjennomføre opplæring innen sikkerhet, ha bevissthetstrening og ha mekanismer egnet til å oppdage uønsket atferd blant eget personell, samt redusere risikoen for sosial manipulasjon og brukerfeil.

Dokumentasjon: beskriv regimet for sikkerhetsopplæring og bevissthetstrening overfor egne ansatte, opplæringsverktøy, bruk av tester mot ansatte, osv.

Merk: dette er et forhold som ofte eksisterer uten at man trenger å spesifisere det, så man bør velge å ta dette med kun i anskaffelser der det er særlig relevant.

5.2.17 Logging, overvåking, avdekking, varsling og håndtering av hendelser

Leverandør skal ha prosesser og tiltak for logging og sikkerhetsovervåking av aktiviteter i de deler av Leverandørens systemer og tjenester som er egnet til å påvirke tjenestenivået eller sikkerhetsnivået til Kunde. Loggene skal benyttes til deteksjon av avvik og uønskede hendelser. Logger skal beskyttes mot uautorisert endring, sletting og tilgang, og skal oppbevares så lenge som leverandøren anser det som nødvendig. Prosessen skal innebære en håndtering av hendelser som minimerer skadevirkningene for Kunde. Leverandøren skal varsle Kunde ved hendelser egnet til å påvirke tjenesteytelsen eller sikkerhetsnivået til Kunde negativt og gi nødvendig bistand for å håndtere hendelsen.

Dokumentasjon: beskriv prosess og tiltak for logging, overvåking, avdekking, varsling og håndtering av hendelser. Beskriv hvordan Kunde varsles ved hendelser.

Merk: jo sterkere logisk kobling det er mellom leverandør og virksomheten, jo mer relevant er det at dette kravet stilles. Når det gjelder varighet på oppbevaring av logger, kan man spesifisere dette nærmere basert på tjenestens/produktets formål eller type.

5.2.18 Redundans, gjenopprettingsevne og beredskapsplanverk

Leverandør skal ha prosesser og planverk som gjør Leverandør forberedt på å håndtere ekstraordinære hendelser i egen virksomhet, herunder system for planer for hendelseshåndtering samt planer for alternativ drift og gjenoppretting.

Dokumentasjon: gi en overordnet beskrivelse av prosesser og hvorvidt det eksisterer slikt planverk.

Merk: tjenestenivå, oppetid og leveringsbetingelser spesifiseres ofte i en tjenestenivåavtale, og slike krav overlapper ofte med krav om at informasjon og informasjonssystem skal være tilgjengelig.

5.2.19 Retten til revisjon og sikkerhetskontroller

Leverandør skal tillate at Kunde gjennomfører revisjon av Leverandør knyttet til etterlevelsen av sikkerhetskrav, eller at virksomheten kan lese revisjonsrapport fra uavhengig tredjepart.

Dokumentasjon: bekreft overnevnte og legg frem eventuelle revisjonsrapporter for gjennomførte revisjoner.

5.2.20 Sikkerhetstesting

Leverandør skal regelmessig (alternativt: på forespørsel fra Kunde) gjennomføre sikkerhetstester, herunder penetrasjonstesting, av de deler av Leverandørens virksomhet

og/eller tjenester egnet til å påvirke sikkerhetsnivået til Kunde. Rapporter eller resultater bør presenteres for Kunde.

Dokumentasjon: beskriv eventuell praksis for sikkerhetstesting.

Merk: det er ikke alltid det er rimelig å forvente å få innsyn i resultater fra sikkerhetstester, fordi disse ofte beskriver sårbarheter som ikke er håndtert.

5.2.21 Sletting av data, avhending av utstyr

Leverandør skal ved opphør av avtalen levere tilbake og/eller slette data mottatt fra Kunde. Eventuelt utstyr skal avhendes på sikker måte.

Merk: virksomheten må sørge for at eierskap til, og leverandørs bruk av, data er regulert av avtalen. Dette er normalt et vilkår i hovedavtalen.

5.3 Krav betinget av produktet eller tjenestens konkrete egenskaper

I de følgende underkapitler beskrives noen scenarier der en gitt betingelse gjelder, og hvilke sikkerhetskrav denne betingelsen vil kunne utløse dersom den eksisterer for en konkret anskaffelse. Merk at kravene her listes opp som kulepunkter og ikke ferdig formulerte krav, og at det er en viss overlapp med kravene beskrevet i kapittel 5.2. Hvilke av kravene som tas med i kravspesifikasjonen og hvordan de formuleres, avhenger av egenskapene til den konkrete anskaffelsen samt virksomhetens behov.

5.3.1 Leverandør skal behandle kraftsensitiv informasjon i driftsfasen

Merk: hvilke av disse kravene som benyttes til å spesifisere krav avhenger av produktet/tjenestens egenskaper, og hvordan produktet/tjenesten leveres. Kravene bør særlig vurderes der leverandør skal behandle kraftsensitiv i klartekst og/eller behandle den på omfattende måter (mange operasjoner, hyppig overføring, utlevering på virksomhetens vegne, osv.).

Husk: ikke still for mange og intrikate krav til håndtering av kraftsensitiv informasjon
Enhver som behandler kraftsensitiv informasjon, skal holde oversikt over hvor virksomhetens informasjon befinner seg og hvem som har tilgang. Mange av kravene beskrevet i kapittel 5.2 er ment å bidra til dette, så det kan være tilstrekkelig å formulere disse. Fokuset bør være på å forhindre utilsiktet og tilsiktet deling eller lekkasjer av kraftsensitiv informasjon.

- Se krav i kapittel 5.2.1 om styringssystem for informasjonssikkerhet. Hvis relevant, vurder å spesifisere at leverandør skal etablere og forvalte en sikkerhetsinstruks egnet til å etablere, opprettholde og videreutvikle system og rutiner for effektiv avskjerming, beskyttelse og tilgangskontroll for kraftsensitiv informasjon.
- Leverandør skal gjøre personell som gis tilgang til virksomhetens kraftsensitive informasjon kjent med den lovpålagte taushetsplikten for kraftsensitiv informasjon, og sørge for de signerer taushetserklæring for tilgang til konfidensiell informasjon underlagt slik lovpålagt taushetsplikt.

- Leverandør skal kun benytte tilgjengeliggjort informasjon/data til å levere den avtalte tjenesten, med mindre noe annet avtales særskilt. Virksomheten eier all informasjon/data tilgjengeliggjort for leverandør.
- Dersom leverandør gir eget personell tilgang til den informasjonen som virksomheten behandler gjennom tjenesten, skal slik tilgang være basert på tjenstlig behov og være underlagt et regime for autorisering og autentisering (se i sammenheng med kapittel 5.2.9).
- Dersom leverandør behandler store mengder kraftsensitiv informasjon med høyt skjermingsbehov, skal leverandør tilby et regime for kryptering og nøkkelhåndtering i tråd med anerkjente og rådende standarder.
- Det skal foreligge særlige instrukser, eller krav til opplæring, for personer som skal behandle kraftsensitiv informasjon på en måte som gjør at får et særlig detaljert overblikk over slik informasjon.
- Der leverandør skal behandle kraftsensitiv informasjon på en måte som gjør at den fremstilles visuelt eller skriftlig i dokumenter eller filer, skal dokument/fil merkes med «Underlagt taushetsplikt etter energiloven § 9-3 jf. kbf. § 6-2. Unntatt fra innsyn etter offentleglova § 13".
- Der leverandør bruker eller tilbyr mobile enheter som kan motta, sende og lese kraftsensitiv informasjon, skal leverandør sørge for sikkerhetsfunksjonalitet som reduserer faren for uautorisert tilgang til slik informasjon.
- Leverandør skal ikke utlevere kraftsensitiv informasjon til underleverandør uten nærmere avtale. Der leverandør bruker underleverandører som behandler kraftsensitiv informasjon, skal leverandør avtale tilsvarende krav.

5.3.2 Leverandør har råderetten over tilgjengeligheten til tjenesten, mv.

Der leverandør kontrollerer eller har den praktiske råderetten over oppetiden eller tilgjengeligheten til en tjeneste, applikasjon, løsning, osv., må virksomheten vurdere behovet for å spesifisere krav utover dem beskrevet i kapittel 5.2.

- Leverandør skal planlegge, gjennomføre og vedlikeholde sikringstiltak etter tjenestens type, oppbygging og funksjon, slik at høy tilgjengelighet ivaretas.
- Leverandør skal identifisere og dokumentere verdier, leveranser, tjenester, systemer og brukere i tjenesten/løsningen. Dokumentasjonen skal holdes oppdatert og tilgjengeliggjøres for virksomheten.
- Leverandør skal gjennomføre risikovurdering regelmessig og ved systemendringer samt varsle virksomheten om risiko som truer tilgjengeligheten til tjenesten.

Merk: virksomheten må sørge for å ha en tydelig tjenestenivåavtale («SLA») for slike anskaffelser, og må passe på at det ikke er overlapp i kravspesifikasjon for sikkerhet og SLA som gjør kravene uklare.

Husk: virksomheten må også tilpasse egen virksomhet til den driftsmodell og risiko en anskaffelse innebærer
I situasjoner der virksomheten er prisgitt en leverandørs innsats for opprettholdelse av tilgjengeligheten til en tjeneste, løsning, mv., bør virksomheten forberede seg selv på et eventuelt bortfall av denne. Dette innebærer f.eks. å ha planer for alternativ drift i egen virksomhet, ha regime for prioritering av oppgaver, varsling til kunder, interessenter og myndigheter, mv.

5.3.3 Leverandør benytter underleverandør for server-/datasentertjenester

Underleverandør må pålegges å ha:

- Fysisk perimetersikring av bygninger og anlegg der det oppbevares datalagringsressurser.
- Adgangskontroll som gjør at kun autorisert personell har adgang til bygninger og anlegg.
- Beskyttelse mot eksterne hendelser knyttet til uvær, strømtilførsel, vannskade, osv. gjennom redundans i tjenesten.
- Beskyttelse & vedlikehold av maskinvare og annet utstyr relevant for tjenesteytelsen.
- Redundant nettverkstilgang (spesifiser særskilte krav tjenestenivå hvis relevant).
- Nettverksbeskyttelse som forhindrer uautorisert lekkasje og avlytting.
- Separasjon fra andre kunder for tjenester som leveres via nettverk.
- Logisk tilgangskontroll til datalagringsressurser.
- Logging, overvåking, deteksjon, analyse, håndtering og varsling knyttet til tjenesteytelsen.
- Kryptografi og kryptografiske kontroller for data som oppbevares og overføres.
- Sikker avhending av utstyr brukt i tjenesteytelsen.

5.3.4 Leverandør leverer produkt som skal installeres i driftskontrollsystemet

Det bør stilles særlige krav til sikkerhet ved anskaffelse av enheter, komponenter og programvare som skal installeres og brukes i driftskontrollsystemet. Driftskontrollssystem har ofte særskilte krav til tilgjengelighet, integritet og pålitelighet og har ofte lengre levetid enn teknologi benyttet i administrative miljøer. Hvilke krav som stilles til produkt/tjeneste og leverandøren avhenger av hva som skal installeres, men slike krav kan eksempelvis være:

- Leverandør skal bidra med dokumentasjon av enheter, komponenter og/eller tjenester som leveres for installasjon i driftskontrollsystemet. Dokumentasjonen skal eksempelvis inneholde asset ID eller tag, navn og beskrivelse, type (printer, SCADA server, historian server, HMI, PLS, etc.), modell, produktnummer, spesifikasjoner og konfigurasjonsinformasjon, plassering, lisenser, garanti, ansvarlig, programvareversjon, og livsyklusinformasjon.

- Leverandør skal ha et regime for endringshåndtering (oppdatering og patching) av de produkter/tjenester som leveres til virksomheten, og skal på forespørsel gi råd om hvordan virksomheten unngår å etablere sårbarheter og risiko ved konkrete endringer og oppdateringer. (Se i sammenheng med kapittel 5.2.13 om endringshåndtering).
- For virksomheten er det viktig at sikkerhetstiltak ikke utformes eller etableres på en måte som påvirker tilgjengelighet eller ytelsen til driftskontrollsystemet negativt, og leverandøren bes beskrive hvilke prosedyrer de har for å unngå dette.

Der produktet som skal installeres er industrielle kontrollere (PLC/PLS), er det viktig å stille krav om:

- Leverandør skal gjøre tilgjengelig dokumentasjon som beskriver hvordan kontrollerne er konfigurert.
- Leverandøren skal sikre enheter og systemer ved å blant annet:
    - Sørge for at enheter har nyeste versjon av fastvare og programvare ved levering til kunde.
    - Deaktivere eller blokkere ubrukte porter.
    - Endre standard passord.
- Leverandøren skal dokumentere hva som har blitt gjort for å sikre systemet.

Der produktet som skal installeres er et operatørpanel/HMI, er det viktig å stille krav om at leverandøren skal sikre enheter og systemer ved å blant annet:

- Fjerne eller deaktivere ubrukte prosesser og tjenester.
- Deaktivere ubrukte eller usikre protokoller (http, FTP, Telnet, VNC, eldre versjon av Modbus, osv.).
- Sørge for at enheter har nyeste versjon av fastvare og programvare ved levering til kunde.
- Deaktivere eller blokkere ubrukte porter.
- Endre av standardpassord.
- Ha forskjellige kontoer for brukere og operatører.
- Sørge for at HMI må omstarte automatisk og i driftsmodus ved en eventuell omstart, også ved for eksempel strømbrudd.
- Ha «view only»-modus på brukere som automatisk logges inn. *Merk:* her kan det være unntak for sikkerhetskritiske systemer.
- HMI skal være konfigurert med «kiosk-modus» slik at det er sperre for muligheten for å benytte det bakenforliggende operativsystemet (med mindre virksomheten har behov for HMI som er konfigurert med programvare som kjører på et fullversjons operativsystem. Ved bruk av HMI på fullversjons operativsystem bør det stille samme krav som til datamaskiner som skal være koblet til industrielle nettverk som forhindrer uautorisert tilgang til virksomhetens industrielle nettverk).

- Ha sikkerhetsdokumentasjon som beskriver hvordan enheter er konfigurert. Denne skal være detaljert nok til at den kan brukes til å sørge for rask tilbakeføring ved for eksempel utstyrshavari eller andre feil.

5.3.5 Leverandør kommer fra en sektor med lavt modenhetsnivå innen sikkerhet

Der virksomheten har vurdert restrisikoen som akseptabel, kan virksomheten vurdere å foreta anskaffelser fra bransjer eller markeder med lavt modenhetsnivå innen sikkerhet. Dessuten forekommer det at start-up-selskaper eller selskaper som tilbyr tjenestene i andre sektorer enn det de er vant til, ikke har det samme modenhetsnivået som andre bransjer. I slike situasjoner bør virksomheten utvise forsiktighet ved bruk av innholdet i kapittel 5.2 til å formulere krav, og bør sørge for å ha vilkår i avtalen som regulerer plan for videreutvikling av tjeneste eller produkt, samt rett til prisavslag dersom utviklingsplanene ikke overholdes. Slike vilkår kan eksempelvis være:

- Leverandør skal ha en plan for utvikling av sikkerhetsnivået i tjenesteleveransen og rapportere månedlig på fremgang.
- Leverandør skal stille på kvartalsvis møter med virksomheten for å diskutere fremdrift i plan.
- Leverandør skal stille til rådighet informasjon og være tilgjengelig for gjennomføring av risikovurderinger.
- Leverandør og leverandørs personell skal delta på kurs avholdt av virksomheten og skal lese opplæringsmateriell som distribueres.

5.3.6 Leverandør skal ha fjerntilgang til virksomhetens driftskontrollsystem

- Leverandør skal stille til rådighet dedikerte personer for virksomheten, og virksomheten skal gjøres kjent med deres identitet, rolle, bakgrunn, mv.
- Leverandør og leverandørens personell skal forholde seg til virksomhetens skriftlige prosedyre for ekstern tilkobling til virksomhetens driftskontrollsystem.
- Leverandørs personell som skal utføre tjenester via fjerntilgang til driftskontrollmiljøet, skal kun gjøre dette fra en adgangskontrollert sone. *Merk*: virksomheten bør presisere hva den anser «adgangskontrollert sone» å være.
- Virksomheten skal kunne gjennomføre egne bakgrunnssjekker av leverandørs personell som gis logisk eller fysisk tilgang til virksomhetens klassifiserte anlegg.

5.3.7 Leverandør og virksomhet skal i fellesskap utvikle et produkt/en tjeneste

Der virksomheten i fellesskap med leverandør eller samarbeidspartner skal utvikle et produkt eller en tjeneste, er det en del spesielle forhold man bør ta høyde for før man signerer en avtale. I situasjoner hvor det ikke er tydelig definert hva sluttresultatet skal være, eller hvor det legges opp til en mer åpen og fleksibel prosess, bør virksomheten vurdere å la avtalen ha vilkår som:

- Sørger for at virksomheten ikke gjør seg selv helt avhengig av én leverandør når produktet/tjenesten er ferdig. Dette kan løses ved å avtale bruk av standardiserte løsninger, stille krav om interoperabilitet, avtale exit-muligheter, stille krav om at produkt/tjeneste skal kunne tilbys til andre kunder, stille krav om tilgang til dokumentasjon og opplæring, mv.

- Sørger for at leverandør på kort og lang sikt har tilgang til nødvendige ressurser (reservemateriell, kompetanse, personell, support, mv.).
- Tydelig regulerer hva leverandør kan bruke virksomhetens data til, samt avklarer eierskap til utledede data fra virksomhetens data.
- Stiller krav om utdanningen og de faglige kvalifikasjonene til nøkkelpersonell som skal delta i utviklingsløpet.
- Sørger for at virksomheten har tilstrekkelig innsikt i leverandørens databehandlingsteknikker/ analysemetoder.
- Sørger for at leverandør tar i bruk eventuelle anonymiserings- og pseudonymiseringsteknikker dersom de skal behandle sensitiv informasjon.
- Sørger for mer detaljerte krav til sikkerhet i utvikling:
    - Ha policyer/styrende dokumentasjon for styring av utviklingsprosesser.
    - Ha dokumenterte prosedyrer for endringshåndtering, inkl. test av endringer.
    - Ha restriksjoner på hvem som kan utføre endringer.
    - Ha prinsipper for innebygget sikkerhet.
    - Separate miljøer for utvikling, test og produksjonssetting.
    - Etablere fiktive eller anonymiserte datasett for testing.
    - Ha regime for ulike typer akseptansetester og sikkerhetstester.
- Sørger for at leverandøren utvikler løsninger med hensyn til prinsipper om innebygget sikkerhet («secure by design») og sikkerhet som standardinnstilling («secure by default»).
- Ha tydelige krav til løpende dokumentasjon av løsningen og endringer.
- Løpende rapportere om større endringer/oppdateringer til virksomheten.
- Krav om opplæringsplaner i metodikk for sikker utvikling, som leverandørs personell skal gjennomføre.

5.3.8 Anskaffet produkt/tjeneste har særlig lang levetid

Der virksomheten anskaffer produkter/tjenester med særlig lang levetid, er det viktig at avtalen med leverandør inneholder krav som sørger for at kvaliteten på leveransen ikke forvitres over tid eller at man plutselig kommer i en situasjon der leverandør ikke lenger kan tilby support. I kravspesifikasjonen/avtalen bør det vurderes å ta inn krav som særlig regulerer:

- At leverandør skal sørge for support i henhold til tjenestenivåavtale, at leverandør skal holde virksomheten løpende informert om eventuelle større endringer i kompetanse- og personellbeholdning.
- At leverandør regelmessig (årlig, halvårlig eller kvartalsvis) skal holde virksomheten oppdatert om status for leveransen, utviklingsplaner, identifiserte risikoer, etc.
- At leverandør regelmessig skal holde virksomheten oppdatert om planer for utvikling av sikkerhetsnivået/-funksjonaliteten i produktet/tjenesten.

- At leverandør skal ha planer for opprettholdelse av kompetanse hos eget personell

5.3.9 Leverandør tilbyr kun egne avtalevilkår

Mange av de store teknologileverandører aksepterer ikke enkeltvirksomheters avtalevilkår eller krav. I anskaffelser der det forventes at slike typer leverandører leverer tilbud eller inngår som en del av et tilbud, bør virksomheten være påpasselig med hvordan krav spesifiseres og hva man krever som dokumentasjon for oppfyllelse. Dette betyr ikke at man skal stille svakere eller færre sikkerhetskrav, men at de må spesifiseres eller formuleres på en måte som gjør at leverandør leverer tilbud.

Eksempelvis kan man bruke formuleringene:

- «Tilbyder skal [*sett inn krav*] ved å [*sett inn beskrivelse*] eller på en annen tilsvarende måte som gjør at kravet oppfylles».
- «Tilbyder skal dokumentere oppfyllelsen ved å [*sett inn krav til dokumentasjon*] eller ved å legge frem dokumentasjon egnet til å sannsynliggjøre at kravet er oppfylt».

Merk: virksomheten bør ikke uten videre akseptere at leverandør kun tilbyr standardvilkår – der det er rom for forhandlinger, bør virksomheten benytte muligheten til det, enten alene eller i samarbeid med andre potensielle kunder av leverandøren.

Merk: mange av de store teknologileverandørene tilbyr et utvalg av sikkerhetsfunksjonalitet mot høyere lisenskostnad – sørg for at tilbyders pristilbud dekker det sikkerhetsnivået virksomheten faktisk ber om.

5.3.10 Leverandør leverer en driftskritisk tjeneste med høyt krav til tilgjengelighet

Dersom en anskaffelse er av en slik type at forhold ved leverandør eller produktet/tjenesten kan påvirke kraftforsyningen negativt, bør virksomheten pålegge leverandør:

- målbare krav til ytelse, oppetid og tilgjengelighet.
- mer spesifiserte krav til hvem som kan tildeles administratorrettigheter og hva de kan utføre.
- krav til særlige beskyttelsestiltak for å forebygge, håndtere og begrense virkningene av ekstraordinære situasjoner.
- mer spesifiserte krav til logging av handlinger og hendelser, overvåking, deteksjon og varsling til virksomheten, samt krav om deltakelse og informasjonsdeling ved etterforskning av hendelser.
- mer detaljerte krav til sikkerhetskopiering, oppbevaring av sikkerhetskopier, samt planer for alternativ drift og gjenoppretting.
- mer detaljerte krav til beredskapsplaner, samt en organisasjon med nødvendig personell, ressurser og kompetanse til å gjenopprette tjenestenivået ved uønskede hendelser i leverandørens virksomhet og hendelser som rammer tjenesten.
- mer detaljerte krav til deltakelse i virksomhetens beredskap og beredskapsøvelser.
- åpenhet om utdanningen og de faglige kvalifikasjonene til nøkkelpersonell, dersom relevant for tjenestenivået.

- å gjøre spisskompetanse tilgjengelighet for virksomheten over tid (tjenesteutsetting innebærer ofte samtidig utsetting av spisskompetanse).
- å akseptere virksomhetens godkjenningsprosedyre for leverandørs endring i bruk av underleverandører eller endring i tjenestene de bruker fra underleverandører.
- krav om regelmessige statusmøter og rapportering av sikkerhetstilstand.
- detaljerte krav til hvordan tjenesten skal opphøre (opprydding, sanering, osv.).

6 VEDLEGG A – VEILEDERE, STANDARDER OG RETNINGSLINJER

I det følgende presenteres en rekke veiledere, standarder og retningslinjer som kan benyttes av virksomheten.

Generelle 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 Forum for informasjonssikkerhet i kraftforsyningen - Sikkerhetsveileder for kraftsensitiv informasjon i skytjenester
- Veiledning til kraftberedskapsforskriften - NVE
- IKT-sikkerhet i anskaffelser og tjenesteutsetting i kraftbransjen - Sjekkliste
- Nasjonal sikkerhetsmyndighet, Generelle råd for tjenesteutsetting og skytjenester
- NVE Ekstern rapport 5/2023: Sett krav til IKT-sikkerhet i anbud og kontrakter: en forstudie
- NVE Rapport 39 (2015) Øvelser. En veiledning i hvordan planlegge og gjennomføre øvelser innen energiforsyningen.
- NVE – engelsk oversettelse av kraftberedskapsforskriften, Engelsk oversettelse av krav i Kbf

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

Sikkerhetsrammeverk og -standarder:

- Nasjonal sikkerhetsmyndighet (2020), NSMs Grunnprinsipper for IKT-sikkerhet 2.0
- International Standards Organisation (2022), ISO / IEC 27002:2022 - 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
- International Electrotechnical Commission (ulike årstall til ulike deler av standard serien) ISA/IEC62443 - Internasjonal standardserieder som tar for seg cybersikkerhet for operasjonell teknologi i automasjons- og kontrollsystemer. Standardserien er omfattende og detaljert, men Norsk Elektronisk Komité (NEK) har utarbeidet et sammendrag som kan være enklere å forholde seg til.
- 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
- Britiske National Cyber Security Centre har oversiktlige og praktisk orienterte veiledere for alt relatert til cybersikkerhet
- EUs byrå for cybersikkerhet (ENISA) har mange veiledere knyttet til cybersikkerhet – både generelle og spesifikke for utvalgte områder, Enisa

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)

Åpen trusselinformasjon:

Rapporter fra PST, Kripos, Etterretningstjenesten, NSM, mv. gode utgangspunkt for å etablere forståelse for det rådende trusselbildet og hvordan trusselaktører utnytter aktuelle sårbarheter.

Oversikt over land som EU har iverksatt sanksjoner overfor, https://sanctionsmap.eu/#/main

7 VEDLEGG B – LANDRISIKOVURDERING

I energilovgivningen er det kun leveranser til driftskontrollsystemer, samt tjenesteytelser som innebærer fjerntilgang til brytefunksjonaliteten i AMS som eksplisitt krever at leverandør holder til i land som er medlem i EFTA, EU eller NATO. Medlemskap i disse institusjoner/organisasjoner innebærer i praksis at et land har et sikkerhetssamarbeid med de andre medlemslandene, noe som vil være til nytte for muligheten til å sivilrettslig og strafferettslig forfølge leverandører som skulle komme til å bryte avtalte sikkerhetskrav eller krav til pålitelighet. Å samhandle med leverandører i slike land innebærer også at man anskaffer produkter og tjenester fra land innenfor samme geopolitiske interessefellesskap, som igjen etablerer en forventning om at det er mindre fare for ondsinnede handlinger, industrispionasje, etc. motivert av geopolitiske konflikter. Fra et sikkerhetsperspektiv, er det på bakgrunn av det rådende trusselbildet gode grunner til å vurdere hvilke land man anskaffer produkter og tjenester fra.

Virksomheter kan komme i situasjoner hvor det er nødvendig eller sterkt ønsket for virksomheten å anskaffe produkter eller tjenester fra land som Norge ikke har sikkerhetssamarbeid med. Dette gjelder typisk der leverandørmarkedet er begrenset til slike land, eller der det er vesentlige forskjeller i leveringsbetingelser eller pris. Siden man da i praksis åpner opp for å anskaffe produkter og tjenester fra land man ikke har sikkerhetssamarbeid med, er det sikkerhetsmessig sett fordelaktig å gjennomføre en landrisikovurdering for de landene man antar at man vil få leverandørtilbud fra (dvs. i planleggingsfasen) eller for de landene man faktisk har fått leverandørtilbud fra (dvs. i anskaffelsesfasen). Merk at slike landrisikovurderinger også kan være nødvendig for underleverandører til potensielle tilbydere, dersom man ikke legger geografiske restriksjoner på hvor tilbydere kan benytte underleverandører fra. Landrisikovurderinger kan også være relevante å gjennomføre dersom man ser at en tilbyder som opererer virksomheten sin innenfor land som Norge har sikkerhetssamarbeid med, men hvor eierselskapet/-ene hører til utenfor slike land.

En landrisikovurdering vil på samme måte som en informasjonssikkerhetsrisikovurdering, ta utgangspunkt i den verdi eller kritikalitet det anskaffede produkt eller tjeneste har for virksomheten. Jo mer kritisk produktet eller tjenesten er eller vil bli for virksomheten, jo mer relevant er det med en landrisikovurdering før anskaffelse (og jo grundigere bør vurderingen være). I leverandørrelasjoner som pågår over tid, kan det også være relevant å gjennomføre landrisikovurdering underveis i avtaleforholdet, for slik å vurdere hvorvidt man bør avslutte eller endre leverandørrelasjonen eller om man bør iverksette tiltak for å redusere den risiko relasjonen utgjør for virksomheten. Selv om man kanskje ikke gjennomfører landrisikovurderinger for ethvert land en leverandør benytter underleverandører fra, bør virksomheten som minimum følge med på den geografiske lokasjonen til underleverandører så langt tilbake i leverandørkjeden som er relevant (mht. risiko) for den konkrete tjenesten eller produktet. Generelt sett, bør virksomheten dessuten overvåke eierskapet til sine mest kritiske leverandører.

Nasjonal sikkerhetsmyndighet (NSM) er et nasjonalt fagmiljø for motvirkning av sikkerhetstruende økonomisk virksomhet, og har på sine nettsider en anbefaling om landvurdering ved tjenesteutsetting som tar for seg fire sett med kriterier som bør inngå i slike vurderinger:

- Statlige styringsindikatorer

- Cybersikkerhetstilstanden
- IKT-infrastruktur og kompetanse
- Forretningsstabilitet

For hvert kriterium, lister NSM så opp en rekke åpent tilgjengelige indikatorer som virksomheten kan benytte for å vurdere statusen for det enkelte kriterium i det landet man vurderer. En landrisikovurdering er med andre ord en skjønnsmessig vurdering hvor man for det enkelte land blant annet vurderer de indikatorer NSM viser til, ser hva offisielle kilder uttaler om relevante trusler, undersøker om det foreligger konkrete saker som har avdekket uønskede forhold, etc.

Hvilke land som bør være gjenstand for landrisikovurdering vil til enhver tid endre seg, og virksomheten bør lese trusselvurderinger fra Politiets sikkerhetstjeneste (PST), NSM og Etterretningstjenesten for å ha kunnskap om relevante trusler. Selv om landene det gjelder ofte er gitt som følge av de rådende geopolitiske skillelinjer, kan det også oppstå enkelthendelser eller endringer som på kort sikt etablerer insentiver for stater å benytte leverandørrelasjoner som middel for å tilegne seg informasjon eller erfaring, for å skaffe seg makt eller pressmidler, eller for å kunne ha målrettede angrep på enkeltvirksomheter. NSM viser til konkrete eksempler på at stater benytter økonomiske virkemidler som investeringer i, og oppkjøp av, norske virksomheter for å blant annet få innsikt i sensitiv informasjon og teknologi av strategisk betydning. Slike praksiser utgjør ikke bare en trussel mot enkeltvirksomheter, men også mot den nasjonale sikkerheten. Virksomheten bør med andre ord være oppmerksomme på fordekte investeringer og oppkjøp fra andre land Norge ikke har et sikkerhetssamarbeid med. Slike økonomiske transaksjoner kan skje gjennom stråselskaper, flernasjonale investeringsselskaper, verdipapirfond eller komplekse selskapsstrukturer og kan dermed være vanskelig å avdekke.

Stater kan også benytte ikke-økonomiske virkemidler som cyber- og påvirkningsoperasjoner gjennom etablerte leverandørrelasjoner – rettet mot et hvilket som helst punkt nedover i leverandørkjeden eller verdikjeden – enten for å skade direkte eller for å etablere et pressmiddel til senere bruk.

Der landrisikovurderingen planlegges å gjøres etter publisering av konkurransegrunnlaget for å se om det i det hele tatt kommer tilbud fra land som bør være gjenstand for slike vurderinger, må virksomheten sørge for at det i konkurransegrunnlaget er hjemmel for å eventuelt forkaste et tilbud basert på resultatene fra en landrisikovurdering. Dette kan for eksempel gjøres ved å spesifisere et krav om at landrisikovurdering vil bli gjennomført for å verifisere sikkerhetsnivå og pålitelighet i leveransen av produktet/tjenesten. Når man så vurderer tilbud, må virksomheten basere seg på åpne og mest mulig objektive kilder.

Der virksomheten har foretatt en landrisikovurdering og vurdert leverandørlandet som akseptabelt, etablerer dette risiko som virksomheten må ta hensyn til i sin styring av informasjonssikkerhetsrisiko. For risiko relatert til leverandørland, vil denne kunne stamme fra blant annet:

- **Leverandørenes personell:** personer med tilgang til å påvirke informasjon og/eller system kan utsettes for utpressing via tredjepart, personens lojalitet kan være svekket av manglende nærhet til de som rammes av en ondsinnet handling.
- **Tap av kritisk informasjon:** manglende forståelse for konseptet «kraftsensitiv informasjon» og potensielle konsekvenser av slik informasjon på avveie.

- **Leverandørkjede**: komplekse kjeder med mange avhengigheter etablerer en større sårbarhetsflate. Manglende oversikt over leverandørkjeden.
- **Leveransepålitelighet**: kritiske komponenter og produkter nødvendige for virksomhetens kritiske driftsprosesser og hvor det ikke eksisterer mulige substitutter, er sårbare for ustabile rammevilkår for leverandør (politisk ustabilitet, kriminalitet, mangler i infrastruktur, mv.).
- **Komponenter**: produkt kan være bygget med mulighet for fremtidig inngang/angrep.
- **Drift & support**: mange produkter/systemer som anskaffes har lang levetid og skal driftes gjennom hele levetiden samtidig som leverandørkjeder og landrisiko kan endre seg over tid.

Vær oppmerksom på at anskaffelseslovgivningen har forbud mot diskriminering på grunnlag av nasjonalitet eller lokal tilhørighet innenfor EU/EØS.

Når det gjelder landrisikovurdering og vurdering av geografisk lokalisering av leverandørens personell, så finnes det noen eksterne kilder som kan bidra til å kartlegge og vurdere risiko:

- Kreditt- og betalingsrisiko etter OECDs risikoklassifisering: https://www.eksfin.no/no/landrisiko/
- Korrupsjon: https://www.transparency.org/en/cpi/2021/
- Politisk stabilitet: https://www.theglobaleconomy.com/economies/
- Lover og regler, overholdelse av inngåtte avtaler, tillit til politiet og domstolene: https://worldjusticeproject.org/rule-of-law-index/"
- Samfunnssikkerhet, nasjonal og internasjonale konfliktnivå: https://www.visionofhumanity.org/maps/#/
- Juridisk høyrisikoland: https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions.htmlHar
- Økonomisk eller sikkerhetsmessig samarbeid: https://www.nato.int/cps/en/natohq/nato_countries.htm

  https://european-union.europa.eu/principles-countries-history/country-profiles_en
- Overføring av personopplysninger til 3-parter, utenfor EU (adekvat beskyttelsesnivå): https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/overforing-av-personopplysninger-ut-av-eos/omrader-med-tilstrekkelig-beskyttelsesniva/
- Det europeiske personvernrådet (EDPB) har betalt for en ekstern studie av myndighetenes adgang til personopplysninger i Kina, India og Russland. Studien går gjennom relevant personvernlovverk i de tre landene og vurderer dette i lys av europeiske personvernregler. En del av funnene er overførbare til sikkerhet generelt. https://edpb.europa.eu/our-work-tools/our-documents/legal-study-external-provider/legal-study-government-access-data-third_en

8 VEDLEGG C – REVISJON OG KONTROLL AV LEVERANDØR

Omfanget av leveransen og leveransens kritikalitet er relevant for hvordan leverandør bør følges opp på sikkerhetsområdet. I noen avtaler har man avtalt at statusmøter eller rapportering på målbare KPI-er anses som tilstrekkelig. For andre leveranser er det behov for dypere innsikt i sikkerhetsarbeidet rundt hele eller deler av leveransen, gjennom utføring av revisjon eller eksempelvis penetrasjonstester.

Statusmøter:

Ofte kan det være hensiktsmessig med statusmøte med leverandør for å følge med på sikkerhetsarbeidet fremfor (eller i tillegg til) formaliserte revisjoner, og hyppigheten vil som oftest være avhengig av leveransens kritikalitet. Statusmøter kan eksempelvis brukes til å vedlikeholde leverandørrelasjonen, til å demonstrere sikkerhetsbehov, til å sjekke etterlevelse av sikkerhetskrav, og til å følge opp eventuelle tidligere avvik eller hendelser. Ofte har partene allerede avtalt å ha faste statusmøter knyttet til ytelse eller tjenestenivå, og man kan da la sikkerhetsaspektet være en del det samme statusmøtet. Stautsmøter bør ha en viss systematikk og formell form.

Elementer som bør på plass i forbindelse med statusmøte:

- Avtalerettslig grunnlag for statusmøte
- En invitasjon som sier noe om:
    - Formålet
    - Henvisning til krav som skal kontrolleres, eller skrive noe om hvilke typer spørsmål som kan komme

Praktisk gjennomføring av statusmøte:

- Sørg for å kalle inn de riktige deltakerne
- Send ut agenda i forkant slik at det er mulig for alle parter å forberede seg
- Utarbeid spørsmål i forkant, for å få leverandørene inn på det sporet du ønsker
- Følg opp krav i avtalen
- Styr tiden
- Avtal eventuell oppfølgingspunkter og tidspunkt for neste statusmøte

Forslag til tema/kontrollpunkter i statusmøte:

- Har leverandør gode rutiner for å installere sikkerhetsoppdateringer så fort som mulig? Er dette en automatisk eller manuell prosess?
- Har leverandør god kontroll på brukertilganger og administratorrettigheter?
- Følger leverandør *best practice* for passordregime?
- Følger leverandør *best practice* for sikker utvikling?
- Er det rutiner for å fase ut eldre IKT-produkter direkte eller indirekte relatert til leveransen?
- Har partene opplevd sikkerhetshendelser relevant for avtaleforholdet?

Revisjon:

Revisjon kan gjennomføres via spørreskjema, møte, eller kombinasjon av disse avhengig av hva som anses som hensiktsmessig for den konkrete leveranse. Grunnelementer som anbefales ved revisjon, uavhengig av hvor liten eller stor revisjonen er:

- En avtale eller et krav som tilsier at man har rett til å utføre en revisjon.
- En oppdragsbeskrivelse som sier noe om:
    - Oppdragsgiver
    - Formål
    - Utfører av revisjon
    - Metodikk for gjennomføring
    - Ønsket skriftlig dokumentasjon (logger, prosedyrer, rapporter, beskrivelser, etc.)
    - Estimert tidsplan
- Oppstartsmøte for gjennomgang av oppdragsbeskrivelsen. Kanskje ikke så relevant for små revisjoner, men kan være nyttig for alle parter ved større revisjoner.
- Intervju (spørreskjema eller muntlige intervju).
- Avslutningsmøte for å oppsummere revisjonen og belyse funn.
- Rapport/skriftlig tilbakemelding av funn og eventuelle oppfølgingspunkter.

Praktisk gjennomføring av revisjon:

- Sørg for at du involverer de riktige deltakerne.
- Ved møte, send agenda i forkant slik at det er mulig for alle parter å forberede seg.
- Sørg for at spørsmålene gjenspeiler kravene i avtalen/kravspesifikasjonen.
- Sett realistiske tidsfrister.
- Gi tilbakemelding til leverandør, og avtal eventuelle oppfølgingspunkter og eventuelt nytt møte.

Penetrasjonstesting:

Penetrasjonstesting er en utbredt metode for å følge opp og undersøke sikkerhetstilstanden hos leverandører eller i tjenester som leveres. Ved penetrasjonstesting forsøker man å bruke samme teknikker som en angriper ville gjort for å komme seg inn i det aktuelle systemet man tester. Penetrasjonstesting utføres oftest ved hjelp av en tredjepart som leverer slike tjenester. Penetrasjonstester kan brukes for å avdekke styrker ved det aktuelle systemet, men brukes i hovedsak for å avdekke svakheter og sårbarheter, samt for å avdekke om det er tilstrekkelig rutiner på plass for å detektere uønsket aktivitet. Der leverandør ikke utfører penetrasjonstesting på eget initiativ, bør virksomheten oppfordre til slik testing. Virksomheten skal alltid avklare med leverandør på forhånd dersom virksomheten selv ønsker å gjennomføre penetrasjonstesting. Vær oppmerksom på at en del leverandører vil kunne ønske å reservere seg mot å levere fra seg resultat fra penetrasjonstester for egne system da dette kan utgjøre en sikkerhetsrisiko for leverandøren selv.