Temarapport

Anskaffelse av datasentertjenester

november 2024

NSM

Nasjonal kommunikasjons-myndighet

NASJONAL SIKKERHETSMYNDIGHET

Nasjonal sikkerhetsmyndighet

Nasjonal sikkerhetsmyndighet (NSM) er Norges direktorat for nasjonal forebyggende sikkerhet. Tjenestens hovedoppgave er å bedre Norges evne til å beskytte seg mot spionasje, sabotasje, terror og sammensatte trusler. Gjennom rådgivning, kontrollaktiviteter, tilsyn, testing og forskning bidrar NSM til at virksomheter sikrer sivil og militær informasjon, systemer, objekter og infrastruktur med betydning for nasjonal sikkerhet. NSM er ansvarlig for et nasjonalt varslingssystem (VDI) som skal avdekke og varsle om cyberoperasjoner mot digital infrastruktur. NSM har også et nasjonalt ansvar for å koordinere håndteringen av alvorlige cyberoperasjoner.

Nasjonal kommunikasjons-myndighet

Nasjonal kommunikasjonsmyndighet

Nasjonal kommunikasjonsmyndighet (Nkom) er utøvende tilsyns- og forvaltningsmyndighet for post og elektronisk kommunikasjon (ekom) i Norge. Myndigheten har også tilsyns- og godkjenningsansvaret for sikkerhet i tillitstjenester. Innenfor elektronisk kommunikasjon jobber Nkom blant annet med markedsregulering, spektrumsregulering og sikkerhet i nett og tjenester. Nkom har ansvaret for å følge opp regelverket som fastslår at ekomsektoren skal ha et forsvarlig sikkerhetsnivå og en forsvarlig beredskap. Myndigheten har fått delegert ansvaret for oppfølging av sikkerhetsloven i egen sektor og har et eget responsmiljø for cyberhendelser (EkomCERT).

Med den nye ekomloven vil Nkom etter alt å dømme også få det regulatoriske ansvaret for sikkerhet i datasentre. Fra 1. januar 2024 er Nkom underlagt Digitaliserings- og forvaltningsdepartementet (DFD).

Forside: Colourbox

Sammendrag

Virksomheter bør gjøre tilstrekkelige sikkerhetsmessige vurderinger ved anskaffelse av datasentertjenester eller reforhandling av eksisterende avtaler. Denne rapporten skal bidra til en overordnet forståelse av hva et datasenter er, de viktigste delene i et datasenter og hvordan det driftes. Denne kunnskapen vil gi grunnlag for å gjøre bedre risikovurderinger og kravstilling, som igjen vil bidra til å oppnå et forsvarlig sikkerhetsnivå gjennom hele avtaleperioden. Kravene til en leverandør blir gjerne fastsatt i forkant av et kundeforhold. Det er derfor viktig at tilstrekkelige vurderinger gjøres før kontraktsinngåelse.

Rapporten gir ulike vurderingspunkter som virksomheten bør ta stilling til. Vurderingspunktene oppsummeres og utdypes videre i et eget regneark. Regnearket er lagd for praktisk bruk i anskaffelsessammenheng. Virksomheten avgjør selv hvilke momenter som er relevante for egne vurderinger.

Bakgrunn

I august 2021 lanserte Kommunal- og moderniseringsdepartementet under regjeringen Solberg en ny datasenterstrategi. Der det ble uttalt at Norge skal være et attraktivt land for datasenteretablering og at det skal tilrettelegges for en bærekraftig datasenterindustri.

Ansvaret for datasentersektoren er lagt til Digitaliserings- og forvaltningsdepartementet og Nasjonal kommunikasjonsmyndighet (Nkom). Nkom er tilsyns- og forvaltningsorgan innen sektoren for elektronisk kommunikasjon, og vil med ny ekomlov også ha ansvaret for oppfølging av sikkerheten i datasentre. Nkom er tildelt ansvar for sikkerhetsloven i egen sektor. Nasjonal sikkerhetsmyndighet (NSM) er tilsynsmyndighet og fagmyndighet innen forebyggende sikkerhet i henhold til sikkerhetsloven. Gjennom rådgivning, kontrollaktiviteter, tilsyn, testing og forskning bidrar NSM til at virksomheter sikrer sivil og militær informasjon, systemer, objekter og infrastruktur med betydning for nasjonal sikkerhet.

NSM ga i 2022 ut en rapport om norske datasentre og digital autonomi. I rapporten anbefalte NSM blant annet at det offentlige bør spesifisere krav til sikring av datasentre og at det bør etableres sektoransvar og regulering av næringen.

Både NSM og Nkom har registrert et økt behov for bistand og informasjon om sikkerhetsvurderinger i forbindelse med anskaffelser av datasentertjenester. Myndighetene har derfor utarbeidet denne rapporten med vurderingskriterier som er anvendelige for virksomheter i de fleste sektorer, og som kan benyttes som underlag i anbuds- og anskaffelsesprosesser.

Målgruppe

Denne rapporten er rettet mot IKT-, sikkerhets- og merkantilt personell som ønsker å få en kortfattet innføring i temaet datasenter, samt vurderer å tjenesteutsette datasenterdrift eller ønsker å forlenge eller reforhandle eksisterende kontrakter. Rapporten kan benyttes av både offentlige og private virksomheter i ulike sektorer. Rapporten kan også benyttes av ledere og andre interesserte for å øke forståelsen for datasenter og tilhørende tjenester. For enkelte virksomheter kan noen temaer oppfattes som mindre relevante, men det anbefales likevel å sette seg inn i innholdet.

Avgrensninger

Rapporten er ment som et første trinn i å hjelpe virksomheter med utfordringer relatert til sikkerhet i datasenteranskaffelser. Den har fokus på samlokasjondatasentre, og har til hensikt å gi en kort innføring i ulike aspekter relatert til dette. Rapporten tar opp temaer som er relevante for sikkerhetsstyring og for å kunne vurdere risiko og sårbarhet gjennom hele leveransekjeden.

I rapporten omtales de fysiske tjenestene som tilbys i tilknytning til datasentre. Den logiske delen av tjenesteleveransen (infrastruktur, plattformer og applikasjonstjenester) tilbys som regel av en annen part enn datasenteroperatøren. Dette blir ikke behandlet her. Datasentre som understøtter utvinning av kryptovaluta omfattes heller ikke rapporten. For mer informasjon om anskaffelse av logisk tjenesteleveranse henviser vi til andre veiledere og rapporter som er utarbeidet på dette feltet.

Rapporten er ikke tiltenkt brukt i vurderingen av egen virksomhets etterlevelse av regelverk. For samsvarsvurderinger opp imot for eksempel sikkerhetsloven eller sektorregelverk må virksomhetene se til egen veiledning.

NSM og Nkom ønsker å takke sentrale aktører som har bidratt med nyttige innspill og informasjon til rapporten. Disse aktørene inkluderer Norsk Datasenterindustri, de største datasenteroperatørene i Norge og Sigma2.

Innhold

Begrepsforklaring

Begrep	Forklaring
Ekomnett	Offentlig elektronisk kommunikasjonsnett eksternt til datasenteret.
Ekomtjeneste	Offentlig elektronisk kommunikasjonstjeneste levert i ekomnett.
Ekomtilknytning/konnektivitet	Forbindelse fra datasenteret til ekomnett.
Nett/nettverk	Brukes her om de interne nettverkene i datasenteret.
Meet-me room (MMR)	Tilkoblings- og utvekslingspunkt for/mellom ekomnett og nettverk.
SD-WAN	Software Defined Wide Area Network. Teknikk/tjeneste for å separere en virksomhets trafikk og sikre den ønsket tjenestekvalitet i et ekomnett.
IP-VPN	Internet Protocol Virtual Private Network. Teknikk/tjeneste for å separere og beskytte en virksomhets trafikk som går over et åpent ekomnett.
IaaS	Infrastructure as a Service. Tjenestekjøp av fysisk eller logisk infrastruktur (fysiske eller virtuelle servere) for lagring og prosessering av data.
PaaS	Platform as a Service. Kunde ivaretar programvare og data, mens tredjepart tar hånd om infrastrukturen og plattformen programvaren kjører på.
SaaS	Software as a Service. Infrastruktur, plattform og programvare tjenesteutsettes til en tredjepart. Kunde kjøper i praksis tilgang til en applikasjon.

Datasentre er en del av vår kritiske infrastruktur

I vårt digitaliserte samfunn er datasentre en svært viktig del av infrastrukturen. Datasentrene står sentralt i den digitale verdenen vi lever i. Der datautveksling og informasjonsoverføring skjer i et enormt tempo, er datasentrene selve navet i den digitale infrastrukturen. Det er i disse sentrene at data og informasjon lagres, behandles og distribueres. Dataene, informasjonen og tjenestene kan være helt avgjørende for enkeltpersoner, virksomheter og myndighetene.

For at samfunnet til enhver tid kan benytte seg av tjenestene som et datasenter understøtter, må mange datasentre tilby nær 100 % tilgjengelighet. Nedetid eller driftsavbrudd kan få alvorlige konsekvenser, fra økonomiske tap til forstyrrelser i tjenesteleveranse. I ytterste konsekvens kan det true nasjonal sikkerhet. Derfor er sikkerheten og påliteligheten til datasentre viktig å hensynta.

For å sikre at datasentre fungerer optimalt, må det tas forholdsregler for å beskytte dem mot farer og trusler som brann, strømbrudd, fysiske og digitale angrep og naturkatastrofer. Dette innebærer etablering av sikkerhetssystemer, redundant strømforsyning og kjølesystemer samt kontinuerlig overvåkning og vedlikehold.

I tillegg til fysisk og digital sikkerhet, er det også nødvendig med planlegging og samarbeid mellom ulike interessenter. Dette inkluderer myndigheter, datasenteroperatører og teknologiselskaper. Samarbeidet er avgjørende for å utvikle og ta i bruk effektive beredskapsplaner og krisehåndteringsstrategier. Et eksempel kan være samarbeid og samtrening mellom det lokale brannvesenet og datasenteroperatøren i tilfelle brann.

Enkelte datasentre har også en større rolle når det gjelder nasjonal autonomi og suverenitet, og er essensielle for å understøtte samfunnskritiske funksjoner. Å ha kontroll over datasentrenes lokalisering, drift og sikkerhet er avgjørende for å beskytte sensitive eller samfunnskritiske data og tjenester samt å redusere Norges avhengighet til andre land. Dette sikrer ikke bare nasjonal kontroll, men også at Norge kan opprettholde sin digitale infrastruktur uavhengig av eksterne forhold som hendelser og kriser i andre land.

Tjenestemodeller

I datasenternæringen og standardiseringsarbeid finnes ulike typer definisjoner på datasenter og ulike begreper for å benevne de forskjellige typene datasentre. Definisjonene og benevnelsene lagt til grunn i denne rapporten er generiske, og drar veksler på både lovverk og anerkjente standarder.

Et datasenter kan betraktes som et anlegg, del av anlegg eller gruppe av anlegg som brukes for å innplassere, tilkoble og drifte IT- og nettverksutstyr for datalagring, dataprosessering eller dataoverføring, og relaterte aktiviteter.

Overordnet kan man kategorisere datasentre som

- virksomhetsinterne datasenter
- virksomhetseksterne datasenter

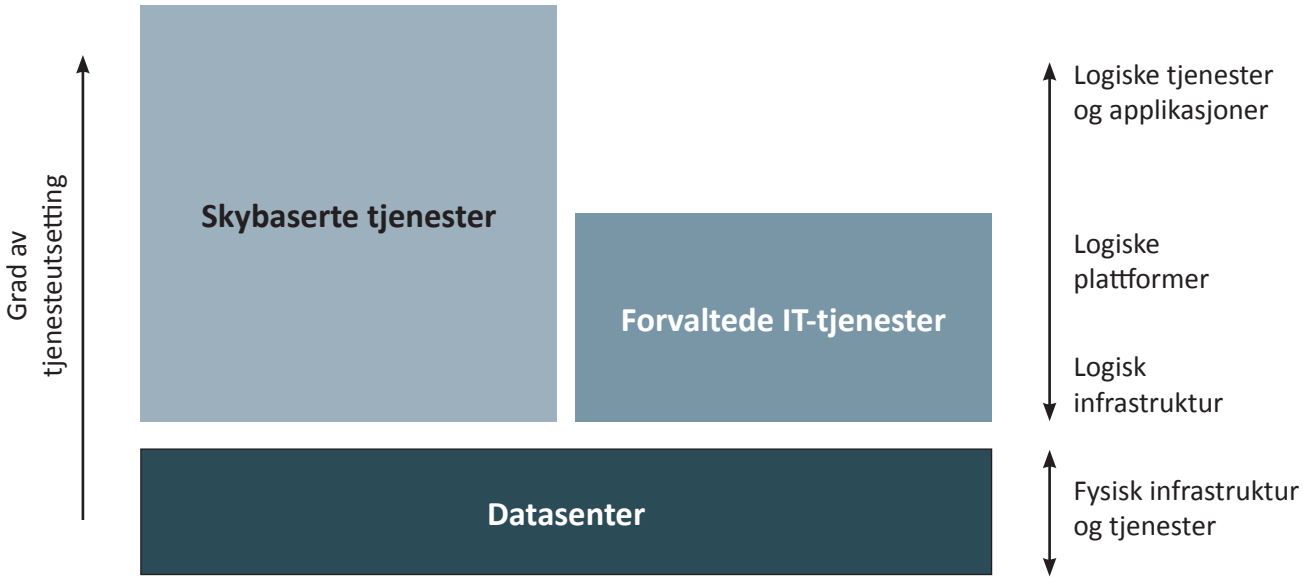
En datasenteroperatør er en aktør som drifter og leverer datasentertjenester. Når datasenteret er virksomhetsinternt er det virksomheten selv som eier datasenteret og er bruker av de tjenestene som det leverer. Normalt er virksomheten selv driftsoperatør, men det forekommer også at denne funksjonen tjenesteutsettes. Datasentre som er virksomhetseksterne, altså ikke eid eller driftet av virksomheten selv, har ulike drifts- og forvaltningsmodeller.

En vanlig form for leveranse av fysiske datasentertjenester omtales her som samlokasjonsdatasenter (eng: co-location datacenter). Kommersielle samlokasjonsdatasentre tilbyr vertskap for sine kunders datautstyr og servere. Tjenesteleveransen reguleres gjennom en avtale om tjenestenivå (service level agreement, SLA). Dette omfatter fysisk innplassering i datahall og sørger for tilgang til kraftforsyning og kjøling. Samlokasjonsdatasentre har videre ansvar for fysisk sikring og drift. Dette innebærer å etablere og ivareta fysiske barrierer og tilgangskontroll samt redundans på elektrisitet og kjøling i tilfelle uønskede hendelser skulle inntreffe.

Datasenteroperatøren er videre med på å tilrettelegge for konnektivitet (ekomtilkytning) til datasenteret ved å tilby innføringspunkter for fiberkabler og sette opp meet-me room (MMR), men det er ekomtilbyderne virksomhetene i hovedsak må forholde seg til for å sette opp konnektiviteten til omverdenen. Datasenteroperatøren kan i noen tilfeller også ha egen fiberinfrastruktur som tilbys til virksomheten for å sette opp konnektivitet. I slike tilfeller vil datasenteroperatøren også være en ekomtilbyder.

Samlokasjonsdatasentre gir samdriftsfordeler, men kan også utgjøre en viss sikkerhetsrisiko ved at flere aktører har fysisk tilgang til samme bygningsmasse og datarom. Sikkerhetsrisikoen avhenger blant annet av hvor mye kontroll og påvirkningsmulighet kunden har over sikkerhetsnivået, og vil variere mellom ulike samlokasjonsdatasentre og hvordan de er konstruert.

Enkelte kilder og litteratur definerer begrepene «forvaltet datasenter» (eng. co-hosting data center) og «skybasert datasenter» (eng. cloud based data center) som egne datasentertyper. Disse definisjonene mener Nkom og NSM er uheldige, da det bidrar til å utydeliggjøre skillet mellom de fysiske og logiske tjenesteleveransene fordi det blander sammen ren datasenterdrift med IT-tjenester som IaaS, PaaS og SaaS. De er likevel relevante å nevne, men da bør de betraktes som IT-tjenester og ikke datasentertjenester. Se Figur 1 for en grafisk fremstilling av forholdene.



Figur 1: Datasentertjenester ligger til grunn for forvaltede IT-tjenester (tradisjonell tjenesteutsetting) og skytjenester.

Innsamling av informasjon fra datasenteroperatører

I forbindelse med en anskaffelse er det vanlig å innhente informasjon og dokumentasjon fra mulige leverandører. Av ulike årsaker kan datasenteroperatører være tilbakeholdne med å utlevere informasjon om sine rutiner og anlegg. Fysiske møter med operatøren kan derfor være nyttig for å skaffe seg innsikt i områder som drift, sikkerhetsstyring og tjenestetilbud. Andre kilder til informasjon kan være via myndigheter, interesseorganisasjoner, referansekunder og nettsider. Tabell 1 viser et eksempel på en oversikt over hvilke informasjonstyper en datasenteroperatør deler under ulike forutsetninger.

Drift	Informasjonssikkerhet	Virksomhetskontinuitet
• Retningslinjer for hendelseshåndtering • Metode for risikovurdering og -håndtering • Retningslinjer for sikkerhet for leverandører • Sikkerhetsprosedyrer for leverandører	• Retningslinjer for klassifisering av informasjon • Retningslinjer for informasjonssikkerhet • Retningslinjer for «Bring Your Own Device (BOYD)»	• Retningslinjer for virksomhetskontinuitet
• Retningslinjer for tilgangskontroll • Lokal nødplan • Plan for forebyggende vedlikehold	• Operasjonsprosedyrer for informasjon og kommunikasjonsteknologi	
• Responsplan ved hendelser • Plan for risikohåndtering • Plan for øvelse og bevisstgjøring	• Retningslinjer for krav til passord • Risikovurderinger og risikohåndtering	• Beredskapsplaner • Plan for gjennoppretting

Deles med mulige kunder | Deles under avtale (NDA) | Deles ikke

Tabell 1: Eksempel på hvilke typer informasjon en datasenteroperatør er villig til å dele med mulige kunder, kunder som har underskrevet taushetserklæring og hva som ikke deles av datasenteroperatøren.

Innledende vurderinger

Verdivurdering

Før en virksomhet går i gang med å anskaffe datasentertjenester vil det være behov for å ha en oversikt over verdier og deres betydning for egen og andres virksomhet (kunder, leverandører etc.). Oversikten synliggjør konsekvenser dersom virksomheter mister kontrollen over verdiene og hvilken skade dette kan medføre. Den danner også grunnlag for eventuelle/nødvendige tiltak for å oppnå et forsvarlig sikkerhetsnivå. Sett fra en datasenterkundes ståsted er det først og fremst verdier i form av virksomhetens data, informasjon og systemer som ivaretas i datasenteret. Dersom virksomheten ikke har en slik oversikt, anbefales det å gjennomføre en verdikartlegging og verdivurdering før anskaffelsesfasen. Se til NSMs og Digitaliseringsdirektoratets veiledninger («Vurdering av risiko og «Orden i eget hus») for detaljer om verdivurdering. Når virksomheter har oversikt, vil dette bidra til å

- vite hva som kan tjenesteutsettes
- tydeliggjøre eksterne avhengigheter
- tydeliggjøre ansvarsforholdet mellom datasenteroperatør og virksomheten
- danne grunnlag for å stille krav til og iverksette sikkerhetstiltak

Datasenteroperatøren har ansvar og kontroll over lokasjon, bygning og datasenterets basistjenester. Dette innebærer også et ansvar for at kritiske leveranser til driften av datasenteret, som for eksempel reservedeler og drivstoff, blir ivaretatt. Kundens ansvar er å følge opp datasenteroperatøren og dens oppgaver samt å håndtere driften av egne servere og IT-systemer.

For å ivareta sitt ansvar og kontroll over tjenesteleveransen, kan en datasenteroperatør sette inn sikringstiltak som både dekker tilsiktede og utilsiktede hendelser. Dette omfatter blant annet

- brannsikkerhet
- personellsikkerhet
- objektsikkerhet og fysisk sikring
- forsyningskjedesikkerhet
- logisk sikring av datasenterets drifts- og styringssystemer (OT-systemer)

Disse sikringstiltakene settes inn for å beskytte selve leveransen av datasentertjenestene. Det bidrar også til å beskytte kundens tilgjengelighet til data, dataenes konfidensialitet og dataenes integritet. Det anbefales å gjøre en konkret vurdering av egne verdier og risiko opp imot sikkerhetsnivået i datasenteret, og ta høyde for det i en eventuell anskaffelse. Et godt designet og driftet datasenter med dokumentert oppetidshistorikk og kundereferanser, i kombinasjon med nøye vurderinger fra kunden, vil bidra til en robust driftsoperativ evne for begge parter.

Gjennomfør en verdikartlegging og verdivurdering.

Anbudsprosessen

Anbudsprosessen avhenger av hvilken type virksomhet man representerer. Offentlig kunde er i all hovedsak bundet til regelverket om offentlige anskaffelser, mens private virksomheter stiller friere.

Ulike datasenteroperatører tilbyr ulike prismodeller, fra enkle og oversiktlige modeller til mer kompliserte. Dette gjør at det kan være utfordrende å forstå og sammenligne tilbudene. For de mer kompliserte modellene kan det i tillegg være vanskelig å forutsi de langsiktige kostnadene. I en anbudsprosess vil det derfor være hensiktsmessig å stille krav til at tilbyderne skal sette opp kostnader på en slik måte at priser kan sammenlignes på tvers av operatørene og gjerne i en mal utarbeidet av virksomheten.

For å redusere klimaavtrykk og miljøbelastningen fra offentlig sektor ble det fra det fra 1. januar 2024 krav til at offentlige virksomheter skal vektlegge klima- og miljøhensyn med 30 %. Mange datasenteroperatører har et høyt fokus på klima- og miljøfremmende tiltak. Overskuddsvarme fra datasentre kan i mange tilfeller brukes til eksempelvis oppvarming av boliger, men det forutsetter nærhet til bebyggelse og infrastruktur som kan overføre energien.

I anbudsdokumentene kan det også være nyttig å ha med krav om at datasenteroperatøren skal veilede virksomheten i hvordan man skal benytte datasenteret for å oppnå best effektivitet. Dette kan for eksempel gjelde oppsett og plassering av serverrack eller valg av type maskinvare.

Vurder anbudsprosessens omfang og innhold

Kontinuitetsbehov

Fra et kontinuitetsperspektiv bør man også vurdere behovet for en beredskapsløsning som bidrar til å holde virksomheten og IT-tjenestene aktive dersom det skulle skje en uønsket hendelse. Dette kan innebære alt fra å etablere seg i flere datasentre som sameksisterer og ved nødvendighet kan operere autonomt, til datasentre som håndterer «enklere» løsninger for sikkerhetskopiering. Virksomhetens tidskrav ved en eventuell gjenoppretting av tjenester gir føringer for hvilken løsning som er best egnet.

Vurder virksomhetens kontinuitetsbehov.

Krav i kontrakt og leveransebeskrivelse

Leveransebeskrivelsen eller tjenestenivået som avtales mellom en virksomhet og datasenteroperatøren er som regel regulert i en tjenesteavtale. Denne delen av kontrakten beskrive forpliktelsene en datasenteroperatør påtar seg overfor kunden med hensyn til leveransens omfang, kvalitet, standarder (se tabell s. 25) som må etterleves og hvordan kravene skal verifiseres gjennom revisjoner. Praktiske og relevante måleparametre (key performance indicators, KPI) innen sikkerhet, drift, økonomi og bærekraft bør også inngå i disse dokumentene.

Om en tjeneste plutselig skulle falle bort bør kundens rettigheter være beskrevet. Ved et nettverksbrudd kan kunden for eksempel få dekket nettverkskostnadene for inneværende måned om tidsavbruddet overstiger en viss tid. Samtidig kan totalkostnadene for kunden være langt større i form av inntektstap og/eller skade på renommé. Det bør derfor avklares hvem som har erstatningsansvaret i slike tilfeller.

Ulike virksomheter har ulike krav til datasenteroperatøren. Som mulig kunde bør man derfor vurdere om datasenteroperatøren allerede tilfredsstiller virksomhetens sikkerhetsbehov eller om det må stilles ytterligere krav i avtalen. I enkelte sammenhenger vil en egen sikkerhetsavtale som kan endres hyppigere inkluderes i kontraktsdokumentene, i tillegg til tjenestenivådokumentet.

Virksomheter bør ha en klar exit-strategi dersom operatøren ikke overholder sin del av avtalen eller det skjer endringer som overstiger virksomhetens risikotoleranse. Med dette menes en klausul i kontrakten som kan fristille partene og at virksomheten har en plan for utflytting. Samtidig må man som kunde være klar over at det kan ta lang tid å flytte ut av et datasenter. Det kan ta opptil flere år avhengig av IT-tjenestenes tilgjengelighetskrav, systemets arkitektur og hvor tett koblingen til datasenterinfrastrukturen er. Som kunde bør man ha garantier i kontrakten for at man får tekniske hjelp fra operatøren ved utflytting, dersom det er nødvendig.

Vurder hva avtalen skal omfatte.

Relevante lover og regler

Virksomheten bør sette seg inn i hvilke lovkrav og forpliktelser den selv og datasenteroperatøren må forholde seg til. For virksomheten kan det være egne sektorspesifikke lover. For datasenteroperatøren kan det for eksempel være krav til forsvarlig drift og krav til at datasentervirksomheten er registrert i et nasjonalt register, slik ny ekomlov fra 1. januar 2025 legger opp til. Sikkerhetsloven vil også kunne pålegge utpekte operatører ytterligere plikter.

Kunder av datasenteroperatører kan også bli underlagt krav i den nye digitalsikkerhetsforskriften. I forskriften er det foreslått krav til virksomheter som tilbyr samfunnskritiske tjenester, blant annet krav til at sikkerhet følges opp med leverandører og underleverandører.

Virksomheten bør ha en oversikt over hvilke lovkrav datasenteroperatøren og virksomheten selv er underlagt.

Datasenterets plassering, struktur og oppbygging

Datasentre variere i både størrelse, kapasitet og hvilket kundesegment de retter seg mot, men de har også noen fellestrekk. I de kommende avsnittene finner man en kortfattet oversikt over de vanligste områdene og delsystemene et datasenter består av. Enkelte områder som omhandler administrasjon og drift er også beskrevet. I likhet med de foregående sidene er det også her inkludert et antall vurderingspunkter.

Colourbox

Geografiske forhold og fysisk plassering

Den geografiske plasseringen av et datasenter har mye å si for hvilke ytre påkjenninger bygget må stå imot. Avhengig av hvor i landet et datasenter er plassert, vil det være ulike faktorer som vil kunne påvirke tjenesteleveransen. Storm, flom, skred og skogbrann er typiske eksempler på hendelser som er knyttet til geografi. I tillegg kan uønskede hendelser knyttet til infrastruktur, industri og annen virksomhet i nærheten av datasenteret påvirke risikobildet. Eksempler på dette er flyplasser, drivstofflagre, vei og jernbane hvor konsekvensene av en hendelse ikke nødvendigvis er avgrenset til et mindre område.

Vurder datasenterets geografiske plassering.

Perimetersikring og soner

For å sikre forsvarlig drift og sikring av et datasenter er det vanlig å dele det inn i ulike soner. Soneinndeling og ulike sikringstiltak har betydning for tiden det tar for en trusselaktør å forsere datasenterets sikring. Datasenteret bør være konstruert etter prinsipper om balansert sikring og ha et positivt tidsregnskap. Balansert sikring betyr at de etablerte fysiske sikringstiltakene virker sammen og selvstendig, og ikke motvirker hverandre. Et positivt tidsregnskap vil si at det tar trusselaktør lengre tid å forsere sikringstiltakene enn tiden utrykningsstyrker bruker for å stoppe trusselaktøren. Tiltak som bidrar til helhetlig og balansert sikring av datasenteret kan på overordnet nivå grupperes i følgende kategorier:

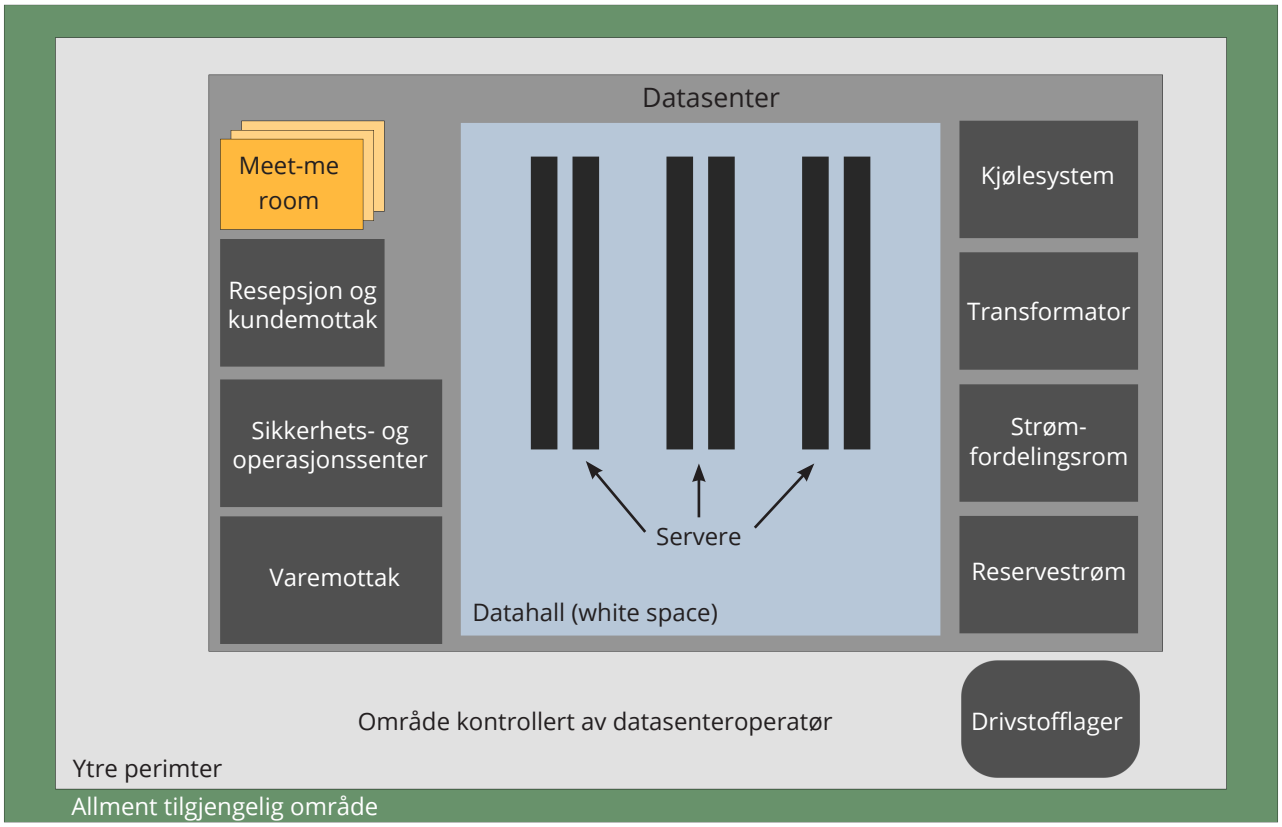
- forebyggende og avskrekkende (Plassering, barrierer, soner, sikkerhetskultur mm.)
- deteksjon og varsling (Kameraer, sensorer, publikum, ansatte, vakter mm.)
- forsinkende og gjenopprettende (Fysisk og elektronisk, beredskapsplaner mm.)

Ytre perimetre

Et moderne datasenteranlegg er sikret i flere lag. Det første er gjerne fysiske sikkerhetsbarrierer som har til hensikt å begrense kontakten med allmenheten og etablere et perimeter rundt selve datasenterbygningen. De ytterste barrierene er som oftest gjerder eller murer. For å komme inn til datasenterets ytre sone må personer og kjøretøy gjennom eksempelvis rotasjonsporter og kjøretøyssperrer. I tillegg til de fysiske barrierene sikres ofte de ytre perimeterne og datasenterbygningen med elektroniske tiltak som kameraovervåkning, adgangskontroll, belysning, radar og lyd. Stedlig vakthold er også vanlig å benytte. Figur 2 viser en skjematisk fremstilling av et datasenter.

Vurder datasenterets grunnsikring*.

*Grunnsikring
Innebærer at sikkerhetstiltakene rundt verdiene i bygget eller på eiendommen er på plass og er i daglig drift, slik at vi kan håndtere en trussel som kan oppstå uten forvarsel (Sikringshåndboka (2016), Forsvarsbygg).



Figur 2: Skjematisk oversikt over områder og systemer i et datasenter.

Inngangsparti og resepsjon

Etter å ha passert de ytre perimeterne er det vanlig å registrere besøket i en vaktpost eller resepsjon. Dette gjøres for at operatøren skal ha kontroll på hvem som er på besøk. Dette gjelder med hensyn til både sikkerhet (*security*) og HMS (*safety*). Etter en ID-sjekk får man utdelt adgangsrettigheter i henhold til oppdrag og avtale.

Ved vaktpost eller resepsjon er det òg vanlig å benytte slusedører (*mantrap*) som fysisk barriere mellom resepsjon og datasenterets indre områder. Samme prinsipp benyttes også i forbindelse med varemottaket.

Datasenteroperatøren kan også sette begrensninger på utstyr det er lov å ta med inn i datahallen. Eksempler på dette kan være utstyr med nettilkobling slik som mobiltelefoner og trådløse rutere eller lagringsmedier som minnepenner. Fotografering er som oftest forbudt.

Vurder datasenterets rutiner for besøk.

Datahall

Det er i datahallen at serverne fysisk innplasseres og kobles til nettverk, strøm og kjøling. Avhengig av hva datasenteroperatøren tilbyr, kan en datahall deles mellom ulike kunder hvor tilgangen til de ulike serverne begrenses av rackskap, være inndelt i ulike soner eller innplassert i egne bur. Sonene eller burene er fysisk adskilt fra hverandre og kan ha egen adgangskontroll driftet av datasenteroperatøren eller kunden selv. I enkelte samlokasjonsdatasentre har kunder mulighet til å leie egne etasjer eller bygge helt separate datahaller.

I samlokasjonsdatasentre er det viktig at datahallen har et høyt sikkerhetsnivå for å forhindre at personell kan gjøre endringer på andre kunders utstyr. Som et eksempel er fysisk usikrede nettverksutstyr eller servere i en datahall en enkel vei inn for aktører som vil gjøre skade. Det er derfor vanlig med utstrakt kameraovervåkning og tidsbegrenset tilgang (til datahallen) for at datasenteroperatøren skal ha oversikt og kontroll. Besøkende kan få utlevert besøksvester og utstyr som lokaliserer personer i sanntid inne i datahallen, og som dermed er med å redusere faren for at uvedkommende er i områder man ikke skal være.

Vurder sikringen og kontrollen datasenteroperatøren har over datahallen

■ Selv om en kunde ønsker å kontrollere tilgangen til egne områder selv, vil datasenter-operatøren i de fleste tilfeller kreve selvstendig tilgang. Dette er for å kunne håndtere en eventuell brann.

Meet-me room (MMR)

Meet-me room er et område i datasenteret hvor kunder og ekomtilbydere fysisk kan koble sammen IT-utstyr for å utveksle data over ulike ekomnett. Et slikt rom har to primærfunksjoner:

1. Innplassering av ekomutstyr eid av ekomtilbydere som muliggjør transport og distribusjon av virksomhetens datatrafikk inn og ut av datasenteret.
2. Sammenkobling av interne og ekomnett – kunde mot kunde, kunde mot ekomtilbyder og ekomtilbyder mot ekomtilbyder.

Tilgangen til et meet-me room må være strengt kontrollert og antall personer med selvstendig tilgang bør være på et minimum. Et datasenter har som regel flere slike rom som følge av sikkerhetskrav fra ulike kunder og/eller som følge av redundante føringsveier for ekomnett som føres til bygget fra ulike retninger. Meet-me room kan konstrueres på ulike måter, som blant annet avhenger av innretningen på datasenteret og ønsket sikkerhetsnivå. Dersom et rom deles av flere kunder er det vanlig å ha følgetjeneste fra operatøren. Dette skyldes at mange kunder og tilbydere kan ha kritisk nettverskutstyr plassert i et meet-me room, og gjelder selv om virksomheten har selvstendig adgang til andre deler av datasenteret.

Internt i datasenteret kan kabling legges opp på forskjellige måter. Virksomheten bør også undersøke hvordan den interne kablingen er lagt opp i datahallen, i grenseflaten mot et meet-me room og internt i sistnevnte. Risikoen for uønskede hendelser øker ved manglende oversikt eller struktur på kablingen. Se avsnittet under tabellen (s. 27) for standarder som omhandler oppsett og kabelstruktur.

Vurder sikringen og kontrollen datasenteroperatøren har over meet-me room.

Vurder hvordan intern kabling er lagt opp og strukturert i datahallen, og om det er risiko knyttet til utilsiktede og tilsiktede hendelser som berører den interne kablingen.

Datasenterinfrastruktur

For at et datasenter skal kunne levere tilfredsstillende tjenester er det helt avhengig av strøm, kjøling og ekomtilknytning. Under gis det en kort innføring i de ulike delsystemene.

Tilknyting til ekomnett

Datasentre forbindes til omverdenen ved hjelp av ekomnett. Ekomnettene består grovt sett av

- aksessnett, som er fiberaksesser og basestasjoner der kundene tilslutter seg ekomnettene
- regionalnett, som bærer ekomtrafikk i regioner mellom byer og tettsteder
- landsnett, som bærer ekomtrafikk på tvers av regioner samt inn og ut av landet

Ut over i ekomnettene avtar gradvis robustheten i nettverksstrukturen. Det betyr at landsnett og regionalnett har mer motstandsdyktighet mot utfall enn aksessnettene. Aksessnettene betjener lokal trafikk og består som oftest av stjernestrukturer. Dette betyr at fiberbrudd et sted kan være nok til å forårsake utfall på en eller flere basestasjoner og/eller lokale bredbåndsaksesser.

Ekomnettene kan ha redundans innebygd både på det fysiske laget (dvs. flere fiberkabler), det optiske laget (fiberoptisk nett) og på nettverks- og transportlaget (IP-nett). Se referansemodellen OSI for mer informasjon om emnet. Ønsker virksomheten ytterligere fysisk og/eller logisk redundans ut over det én ekomtilbyder kan tilby, er det mulig å kjøpe tilknytning fra flere ekomtilbydere.

Virksomheten bør vurdere hvordan tilknytningen til datasentrene realiseres samt den fysiske og logiske redundansen i tilknytningen. I dette ligger blant annet om det er flere fysisk adskilte fiberkabler og traseer inn i et datasenter samt hvilken type nettverksstruktur fiberkablene er tilknyttet. Videre bør virksomheten vurdere hvordan viktige kvalitetsparametere som kapasitet og konfidensialitet ivaretas. Vurder også om det er behov for tjenester som SD-WAN eller IP-VPN som garanterer en viss tjenestekvalitet, og om det er mulig å kjøpe tilknytning fra flere ekomtilbydere.

Disse valgene har betydning for motstandsdyktigheten mot ulike uønskede hendelser, både tilsiktede og utilsiktede, som rammer tilgjengelighet, konfidensialitet og integritet. Virksomheten kan ikke nyttegjøre seg av IT-systemene i datasenteret uten tilknytning til ekomnett. Det bør inngås en avtale om tjenestenivå med tilbyderen(e) av ekomnett som tydelig spesifiserer tjenestekvaliteten som forventes for ekom-tilknytningen til datasenteret og virksomhetens øvrige lokasjoner.

■ Autorisert virksomhet
All installasjon og vedlikehold av ekomnett skal være foretatt av en virksomhet som har tillatelse fra myndighetene. Dette gjelder uavhengig av om det er i ekomnettet utenfor datasenteret, i tilkoblingspunktet mellom ekomnettet og datasenterets nettverk, eller videre inn i datasenterets nettverk.

Myndigheten (Nkom) setter også krav til at det skal benyttes standarder eller tilsvarende ved bygging og etablering av ekomnett.

Vurder virksomhetens behov for redundans og diversitet på ekomtjenester

Vurder datasenteroperatørens arbeid med å sikre fiberinnføringer.

Strømforsyning

Hovedstrømforsyningen til samtlige datasentre i Norge er kraftnettet. Imidlertid varierer det om de er koblet til distribusjonsnettet (lokalt), det regionale nettet eller transmisjonsnettet (nasjonalt nivå, Statnett). Normalt forsynes et datasenter fra enten distribusjonsnettet eller det regionale nettet, men det forekommer også at de mest kraftkrevende sentrene forsynes fra transmisjonsnettet.

Distribusjonsnettene er bygd opp med strålestruktur/radiell struktur. Brudd i et distribusjonsnett fører derfor til at samtlige abonnenter etter bruddet mister strømmen. De regionale nettene og transmisjonsnettet er basert på ringstrukturer. Ringstrukturer vil på den andre siden gi større motstandsdyktighet mot enkeltbrudd, fordi transformatorene blir forsynt fra to kanter. Dermed vil forsyningssikkerheten frem til datasenterets transformator muligens være bedre sikret for de som er direkte tilkoblet regionale nett eller transmisjonsnettet enn via et distribusjonsnett. Kunder kan etterspørre dokumentasjon og statistikk fra datasenteroperatøren og Norges vassdrags- og energidirektorat (NVE) for å vurdere datasenterets robusthet mot strømbrudd.

Som sekundærkilde benyttes tradisjonelt dieselaggregater og batterier (avbruddsfri strømforsyning (UPS)) i kombinasjon. Ved bortfall av primærkilden skal batteriene overta kraftleveransen for en kortere periode for å hindre driftsavbrudd. Deretter vil aggregatene starte opp og forsyne datasenteret inntil primærkilden er tilbake. Om primærkilden uteblir over en lengre periode vil det bli nødvendig med drivstoffleveranser. I beredskapssituasjoner i samfunnet kan det være nødvendig å prioritere tilgangen til drivstoff. Vurderingene av hvor lenge datasenteret kan driftes på sekundærstrømforsyning bør ta høyde for dette.

Primær- og sekundærstrømkilde er to ulike systemer som kan ha redundans hver for seg. Avhengig av oppsett kan det være flere føringsveier som kommer inn fra kraftnettet, og i en del tilfeller kan strømmen distribueres i datasenteret gjennom uavhengige kretser. Det samme gjelder sekundærstrømforsyningen. Datasenteret kan altså ha to eller flere generatorer med uavhengige kretser som kan ta over for hverandre, gjerne kalt A- og B-mating.

■ Ikke alle applikasjoner og IT-systemer krever redundant strømtilførsel. Høyere krav til oppetid og tilgjengelighet påvirker kostnadsbildet. Gjør derfor en kost-nyttevurdering av hvilke applikasjoner og systemer som krever redundans. Vær oppmerksom på at sektorspesifikke krav likevel kan ha krav til redundans, selv om virksomhetens vurdering kommer frem til det motsatte.

Vurder datasenteroperatørens drifts- og vedlikeholdsrutiner av primær og sekundær strømforsyning.

Vurder både den fysiske, logiske og administrative sikringen av datasenterets strømforsyning.

Vurder primærforsyningens (kraftnettet) robusthet.

Energieffektivitetsindikatorer

I vurderingen av datasenteroperatørens arbeid med energieffektivisering er prestasjonsindikatoren *power usage effectiveness* (PUE) mye benyttet. PUE er et mål på hvor mye effekt i datasenteret som går bort til drift av andre systemer (kjøling) enn kun IT-infrastruktur (servere). Som et eksempel tilsvarer en PUE-faktor lik 1 at et datasenter kun forbruker strøm på IT-infrastrukturen. En PUE-faktor lik 2 vil si at datasenteret grovt sett forbruker like mye effekt på å kjøle ned IT-infrastrukturen som på å drifte den. For moderne datasentre vil en PUE-faktor mellom 1.1 og 1.4 være normalt. For kunder er det ønskelig at den er så lav som mulig da denne ofte inngår som grunnlag for å beregne driftskostnader som viderefaktureres kunden.

For å redusere klimagassutslipp, er det sentralt at virksomheter tar energieffektive valg i anskaffelser. Datasenternæringen jobber aktivt med gjenbruk av overskuddsenergi eller restvarme. I denne sammenheng gir prestasjonsindikatorene energy reuse effectiveness (ERE) og enery reuse factor (ERF) virksomheten verdifull innsikt. I motsetning til PUE inkluderer disse indikatorene gjenbruk av overskuddsenergi, som for eksempel oppvarming av boliger.

Kjøling

Sammen med intern nettverksinfrastruktur og strømtilførsel, utgjør også kjøling en vesentlig del av grunninfrastrukturen til et datasenter. Tradisjonelt har kjølesystemene benyttet seg av kald luft som kjølemedium i datahallen. Overskuddsvarmen har blitt frigjort via kjøletårn som utgjør den utvendige delen av kjølesystemet. Ved mangel på kjøling vil servere og annet IT-utstyr raskt bli overopphetet og i verste fall ødelegges. Det er derfor kritisk at vedlikehold av kjølesystemene og sikkerheten rundt slike systemer blir ivaretatt på en forsvarlig måte. For delene som er plassert på utsiden og i friluft er det spesielt viktig med tilstrekkelig sikkerhet, da disse delene er mer eksponert mot eksterne trussler enn de som står på innsiden.

I eldre datahaller benyttes ofte egne datagulv. Dette er gulv bestående av spesialmoduler i et rutemønster som står hevet over det eksisterende gulvet. Datagulvet holdes oppe av understøttende bein. Rommet som oppstår mellom det eksisterende gulvet og modulene benyttes ofte til å føre frem kabler. Det er også vanlig å benytte dette rommet som en ventilasjonskanal for kald luft til kjøling av server. I så tilfelle erstattes modulene i nærheten av rackene med perforerte versjoner for å føre luften opp. Nyere datasentre konstrueres ofte uten datagulv og med høyere takhøyde for å sikre bedre varmeavledning og luftsirkulasjon. Her føres kabler frem på kabelbroer i himlingen.

Nye IKT-teknologier krever også modernisering av kjølesystemene. Tradisjonelt har det vært vanlig med et effektforbruk mellom 5-15kW per rackskap, og for disse nivåene har luftkjøling vært tilstrekkelig. Behovet for økt datakraft og bruk av grafikkprosessorer (GPU), til blant annet trening av AI-modeller, gjør at det ikke er uvanlig med et effektnivå på to- til tresifret antall kW. Dette krever andre kjølemetoder som vannkjøling. Eksempler på vannkjøling kan være direkte på komponenter (direct liquid cooling, DLC) eller nedsenket i kar (immersion cooling), og av disse to metodene er førstnevnte mest vanlig.

Vurder både den fysiske, logiske og administrative sikringen av datasenterets kjølesystem.

Vurder datasenteroperatørens drifts- og vedlikeholdsrutiner av kjølesystemet.

Kontrollsystemer

Infrastruktur som strøm, kjøling, interne nettverk, brannvarslingssystemer og fysiske sikkerhetssystemer er nødvendige for å ivareta sikker drift og forvaltning av et datasenter. For å oppnå en effektiv og sammenhengende drift er disse ofte integrert med hverandre i et eget nettverk uavhengig av kundene, og styres og monitoreres gjennom et felles kontrollsystem. En slik sammenkobling av fysiske og logiske enheter omtales gjerne som operasjonell teknologi (OT), og gir mulighet for en helhetlig administrasjon og overvåkning av den tekniske tilstanden i datasenteret. Disse nettverkene og systemene er av kritisk verdi og må derfor sikres tilstrekkelig både mot eksterne og interne trusler. Uautorisert tilgang til et datasenters internnettverk og kontrollsystem kan føre til store tap både for datasenteroperatør og kunder.

Til forskjell fra rene IT-systemer vil de fysiske komponentene (kjøleutstyr, brannalarm etc.) i et OT-system ha vesentlig lengre levetid enn servere og nettverksutstyr. Fra et cybersikkerhetsperspektiv kan dette føre til at de er utdaterte lenge før de fysisk slutter å fungere. Virksomheten bør derfor vurdere å innhente informasjon om hvordan datasenteroperatøren forvalter slike systemer, og om det benyttes prinsipper og standarder for risikostyring for IT-systemer. Se standarder som ISA/IEC 62443 for relevant informasjon.

Vurder datasenteroperatørens arbeid med sikring av OT-systemer.

Annen sikring

Brannsikring

Brannsikring er viktig for å unngå eller begrense konsekvensene av en brann. Mangel på tiltak øker risikoen for tap av både datasenteroperatørens og kunders verdier.

For å redusere faren for brann finnes det både defensive og aktive sikringstiltak. De defensive tiltakene omfatter den bygningsmessige strukturen som for eksempel bruk av brannhemmende materialer, oppdeling i ulike brannceller, bruk av materialer med lav avgassing og sikring av drivstofforsyning til strømaggregater. Aktive tiltak består blant annet av deteksjonssystemer som røyk-, varme- og CO2-detektorer, og reaksjonssystemer som lyd og lys.

Inne i datahallen benytter datasenteroperatørene i hovedsak tørrslukkingssystemer som bruker ikke-reagerende gass som slukkemiddel. I motsetning til vann leder ikke gassen strøm, krever ikke opprydning og ødelegger ikke infrastrukturen eller verdiene i et datasenter. Gassene som kan benyttes er blant annet karbondioksid, nitrogen eller argon. Ved tilløp til brann pumpes

slukkegassen ut i rommet gjennom et distribusjonssystem. Slukkeanlegg med aerosol benyttes også i datasentre.

Det er òg vanlig at datasenterets ulike delsystemer er sikret med ulike slukkeanlegg. Som nevnt over er datahallen ofte sikret med ikke-reagerende gass, men i rom hvor for eksempel aggregater og diesel oppbevares vil sprinkleranlegg være en bedre og billigere løsning. I rom og arealer hvor mennesker oppholder seg er det lite egnet å benytte slukkesystemer med gass som slukkemiddel. I stedet benyttes det som oftest tradisjonelle sprinkleranlegg.

Vurder datasenteroperatørens rutiner og dokumentasjon på at slukkesystemet er forsvarlig sikret og vedlikeholdt.

Sikring mot elektromagnetiske sårbarheter

Enkelte IT-systemer har så høy verdi for brukeren at det også krever sikring mot andre typer trusler enn det et typisk datasenter er sikret mot. Et eksempel på slike trusler er elektromagnetiske pulser (EMP). Pulsene kjennetegnes ved at de har høy intensitet og er kortvarige. De kan være menneskeskapt eller som følge av naturlige fenomener. Eksempler på menneskeskapte pulser er elektromagnetiske våpen som mikrobølgevåpen (RFW) eller atomladninger som detoneres høyt oppe i atmosfæren (HEMP). Solstormer og lyn er eksempler på naturlige fenomener.

Konsekvensen av slike pulser er ødeleggelse av elektroniske komponenter. Dette kan igjen påvirke samfunnet og individer ved at IT-systemer stopper å fungere og på den måten forårsake større skader.

TEMPEST er òg et elektromagnetisk fenomen, men behandles ikke videre her.

Vurder behovet for sikring mot elektromagnetiske sårbarheter.

Colourbox

Administrativ sikkerhet, drift og personell

Forsvarlig, stabil og sikker datasenterdrift krever at datasenteroperatøren har fordelt roller og ansvar, og gjennomfører nødvendige aktiviteter og prosesser. Driftsansvarlig, sikkerhetsansvarlig og kapasitetsansvarlig er roller kunden kan forvente hos en operatør. Beredskapsøvelser, test av aggregater eller loggføring av endringer er alle eksempler på aktiviteter og prosesser. Både roller og oppgaver bør være strukturert og dokumentert i et styringssystem, som kan benyttes i revisjonsarbeid og oppfølging av avtaler.

Enkeltpersoner kan være tillagt flere roller. For eksempel kan drifts- og sikkerhetsansvaret tillegges samme person.

Roller

Overordnet forvaltning

Funksjonene i denne kategorien inkluderer ledelse, økonomi og kunde- og markedskontakt. Oppgavene spenner fra å utarbeide og oppdatere de strategiske føringene og dokumentene basert på etterspørsel og markedet, til regnskap og økonomiforvaltning. Kunderelaterte oppgaver går blant annet ut på å følge opp avtaler og påse at avtalt tjenestenivå blir overholdt.

Sikkerhet

Sikkerhetsfunksjonen har som oppgave å påse at både datasenterets og kundenes verdier er forsvarlig sikret. Dette innebærer blant annet å utarbeide og oppdatere sikkerhetsrutiner, gjennomføre trussel- og risikovurderinger samt drift av sikkerhetssenter og sikkerhetsoppfølging av personell.

Myndighetskontakt og etterlevelse av krav

Denne funksjonen sørger for at prosesser, oppgaver og dokumentasjon relatert til krav fra myndighetene blir utført. I tillegg følger denne funksjonen opp etterlevelse av krav i relevante standarder og eventuelle sertifiseringer.

Vedlikehold

Vedlikehold går ut på å holde oversikt over, opprettholde og utbedre eksisterende delsystemer. Dette inkluderer delsystemene strømforsyning (primær og sekundær), kjøling, areal, sikkerhet og IKT-infrastruktur relatert til driften av datasenteret. Sammen med sikkerhetsfunksjonen må vedlikeholdsfunksjonen ta høyde for datasenterets beredskap og blant annet kunne planlegge for reservedeler og -komponenter. For å sikre nødvendig vedlikehold og kapasitet er det viktig at datasenteroperatøren har tilstrekkelig og hurtig tilgang til vedlikeholdspersonell.

Kapasitetsplanlegging

Kapasitetsplanleggingsfunksjonen sørger for å planlegge for fremtidige investeringer i datasenterinfrastrukturen. Dette gjøres med utgangspunkt i gapet mellom hvordan anlegget og delsystemene i dag er dimensjonert, og hvordan de må dimensjoneres for å dekke de fremtidige behovene.

Overvåkning og optimalisering

Personell i denne funksjonen sørger for overvåkning av datasenterdriften og påser at datasenteret opererer innenfor akseptable grenser. Denne funksjonen har også som oppgave å analysere driftsdata relatert til de ulike systemene og eventuelt optimalisere og justere systemene. Dette gjøres blant annet for å redusere datasenterets energiforbruk, CO2-avtrykk og sikre stabil drift. Sistnevnte er kritisk for datasenterets oppetid og tilgjengelighet.

Vurder hvordan operatøren har fordelt roller og ansvar, og om dette er forankret i et styringssystem.

Eierskapsstruktur og finansiell status

Informasjon om eierskapsstruktur og finansiell status kan brukes i vurderingen av om det er risiko knyttet til endringer i tjenestetilbudet frem i tid, eller om det vil foreligge en sikkerhetsrisiko ved å velge en gitt operatør. Dersom operatører har eiere med hovedsete utenfor Norge kan det være vanskelig å kartlegge de fullstendige eierskapsstrukturene, da disse kan være lange og kompliserte.

Finansiell status kan ha betydning for fremtidig drift. Dersom datasenteroperatøren har en uforsvarlig drift eller eiersiden mangler investeringsvilje, kan dette blant annet påvirke den driftsoperative evnen i den forstand at nødvendige oppdateringer i infrastrukturen ikke blir gjennomført. Tjenesteomfanget kan også bli påvirket.

Finansiell status kan videre påvirke eierskapet ved at attraktive datasenteroperatører kan være aktuelle for oppkjøp. Nye eiere kan ha andre mål og prioriteringer som nødvendigvis ikke sammenfaller med virksomhetens mål og prioriteringer. Det er derfor viktig å være bevisst og ta høyde for slike eventuelle endringer.

Når det gjelder forretningsmodell bør virksomheten undersøke hva operatøren i utgangspunktet har spesialisert seg på. Er det en ren datasenteroperatør, eller driver operatøren også innenfor andre forretningsområder? Det kan også være en fordel å undersøke i hvilket omfang operatøren drifter datasentre. Stordrift kan bety høyere grad av profesjonalisering og mer stabil drift. Det viktigste er at virksomheten undersøker at operatøren har tilstrekkelig grad av kompetanse til å drifte datasentre. Erfaringer fra andre kunder kan være verdifullt i disse vurderingene.

Dersom det vurderes som relevant for å ivareta sikkerheten i tjenesteutsettingen, bør virksomheten også undersøke eierskapet til underleverandører av datasenteroperatøren som for eksempel entreprenører og vaktselskap.

Vurder de forretningsmessige sidene ved datasenteroperatøren og dens underleverandører.

Andre datasentertjenester

I tillegg til å tilby areal, strøm, nettverk og kjøling, kan datasenteroperatører tilby andre relevante og nyttige tjenester. Dette kan romme alt fra å motta og driftsette nytt IT-utstyr til ulike drifts-, sikkerhets- og overvåkingstjenester i det fysiske og logiske domenet. Hensikten er å være kundens forlengede arm i datasenteret.

For datasenteroperatører som tilbyr tjenester utover de grunnleggende datasentertjenestene faller disse ofte inn under kategoriene IMACD-tjenester, *remote hands*-tjenester eller *smart/ intelligent hands*-tjenester. Hvilke tilleggstjenester som faktisk faller inn under de ulike kategoriene avhenger av operatørens kategorisering. En grov tommelfingerregel er at tjenester som kategoriseres som *smart hands* ansees å kunne løse mer komplekse oppgaver enn *remote hands*- og IMACD-tjenester. Kunder bør være oppmerksom på at datasenteroperatører kan benytte *smart hands* eller *remote hands* som samlebetegnelse for samtlige av tjenestene de tilbyr. Under følger en kort beskrivelse av disse tilleggstjenestene.

IMACD – Install, Move, Add, Change og Dispose

IMACD er først og fremst rettet mot håndtering av maskinvare. Dette inkluderer installasjon, flytting, enkel endring i serveroppsett eller serverkonfigurering, avhending av IT-utstyr og koordinering av transport til og fra datasenterlokasjonen. Tjenesten kan også omfatte dokumentasjon av nevnte oppgaver.

Remote hands

Remote hands er en samlebetegnelse over tjenester som en datasenteroperatør kan levere. De ligner i enkelte tilfeller på IMACD-tjenester. I tillegg kan enkelte operatører tilby tjenester som omstart av IT-utstyr, kabling, sjekk av statuslys på IT-utstyr eller følgetjeneste ved besøk av eksterne. Enkelte datasenteroperatører tilbyr kunden å følge servicepersonellet via videolink.

Smart hands og intelligent hands

Dette er tjenester som går utover enkel support og inkluderer mer komplekse oppgaver knyttet til installasjon, konfigurering, drift, feilsøking og -retting og avhending av servere og nettverksutstyr. Andre eksempler er oppsett av brannmur, sikkerhetskopiering og design av datasenterløsning tilpasset kundens behov. *Smart hands*-tjenester kan òg inkludere teknisk personell med dypere IT-teknisk kompetanse, og som vil kunne bistå i forbindelse med uønskede hendelser som for eksempel ved driftsavbrudd i kundens IT-system.

Avhengig av tjeneste- og prismodell kan datasenteroperatørene ta betalt for de nevnte tjenestene på ulike måter. Dette kan for eksempel være gjennom et løpende abonnement eller som enkeltbetalinger. Noen tjenester kan være inkludert i tilbudet, mens de mer avanserte kjøpes av kunden etter behov. Tjenestene kan tilbys uavhengig av tidspunkt på døgnet og gjennom hele året.

Vurder bruken av og risikoen forbundet med tilleggstjenester.

Om tilgjengelighet og pålitelighet

I datasentersektoren er det vanlig å ha et bevisst forhold til begrepet oppetid. Opptid er hvor stor andel av tiden over en tidsperiode, eksempelvis gjennom et år, et datasenter leverer de avtalte tjenestene uten opphold. Begrepet nedetid er da det motsatte, altså driftsavbrudd. Informasjonen man får fra datasenteroperatøren om tekniske systemer, oppbygning og administrasjon, er nyttig for å vurdere datasenterets tilgjengelighet og pålitelighet.

Om en datasenteroperatør kan garantere en oppetid på 99,99% gjennom et år, tilsvarer det et totalt driftsavbrudd på omtrent 53 minutter i løpet av 365 dager. Oppetiden sier derimot ikke noe om hvor ofte et driftsavbrudd skjer, ei heller noe om hvor lang tid det tar å gjenopprette til samme tilstanden som før avbruddet. Et strømavbrudd på bare noen tidels sekunder kan påvirke kundene i datasenteret og IT-systemene deres negativt. Og gitt at det for eksempel tar 30 minutter å gjenopprette en virksomhets tjenester, vil man da ikke behøve mer enn to driftsavbrudd i datasenteret før tiden det tar å gjenopprette egne tjenester overgår datasenterets 53 minutter nedetid.

Derfor er det ikke bare krav til tilgjengelighet som er viktig å kreve, men også krav til pålitelighet. Pålitelighet handler om hvor driftssikkert datasenteret er, altså i hvilken grad delsystemene fungerer slik de skal både individuelt og sammen.

I overnevnte avsnitt er det først og fremst tilgang til strøm som er beskrevet. Dersom man har driftsavbrudd i for eksempel kjølesystemet er det som regel noe bedre tid til å unngå driftsstans fordi serverne i seg selv har en toleranse på driftstemperatur. Men med inntoget av ny teknologi, som har en høyere effekttetthet (power density) per rack enn det man tradisjonelt har sett, vil tiden man har til å forhindre en driftsstans som følge av overoppheting gå betraktelig ned.

Vurder tilgjengeligheten og påliteligheten til datasenteret.

Standarder

Det eksisterer mange ulike standarder som datasenteroperatørene kan velge å sertifisere seg etter, eller som kunder krever at de er i overenstemmelse med. Standardene omfatter områder som design og drift av datasenter, cybersikkerhet, bærekraft og miljø. Å opprettholde sertifiseringer er både tids- og kostnadskrevende, be derfor om oppdatert dokumentasjon på datasenterets og operatørens sertifiseringer. Det kan være hensiktsmessig å benytte standarder, eller deler av dem, som utgangspunkt for kravstilling og kontrakt. Under presenteres de mest brukte standardene per 2024.

Undersøk hvilke standarder datasenteroperatøren er sertifisert etter.

Standard	Beskrivelse
ISO 9001	Ledelsessystem for kvalitet. Denne standarden angir kravene til hva et kvalitetsledelsesystem bør inneholde, slik at virksomheter kan styre prosesser eller aktiviteter for å kunne levere varer og/eller tjenester som tilfredsstiller kundens krav til kvalitet.
ISO 14001	Ledelsessystem for miljø. Denne standarden angir anerkjente metoder for systematisk miljøledelse og skal bidra til at virksomheter forbedrer sin miljøprestasjon.
ISO 20000	Ledelsessystem for å sikre kvalitet på levering av IT-tjenester. Kan benyttes av kunder som behøver en ensartet tilnærming til livsløpet til en tjeneste.
ISO 27001	Ledelsessystem for informasjonssikkerhet. Denne standarden angir kravene til etablering, implementering, vedlikehold og kontinuerlig forbedring av et ledelsessystem for informasjonssikkerhet.
ISO 45001	Ledelsessystem for arbeidsmiljø.
ISO/IEC 22237	En helhetlig standard som tar for seg krav og anbefalinger for planlegging, bygging og forvaltning av datasentre. ISO 22237 deler datasentre inn i ulike klasser etter tilgjengelighet, sikkerhet og energieffektivitet. EN 50600 er det europeiske motstykke til denne standarden.
ISO 30134 (i sammenheng med ISO/IEC 22237)	Standarden inneholder ulike KPIer for å forbedre driften av datasentre.
ISAE 3402/SOC 1	En standard til nytte for tjenesteleverandører som skal forsikre kunder om forsvarlig internkontroll på det finansielle området. Benyttes mest i USA, men også internasjonalt anerkjent.
NEK EN 50600	En helhetlig standard som tar for seg krav og anbefalinger for planlegging, bygging og forvaltning av datasentre. EN 50600 deler datasentre inn i ulike klasser etter tilgjengelighet, sikkerhet og energieffektivitet. ISO/IEC 22237 er det internasjonale motstykke til denne standarden.
Tier Standard (Uptime Institute)	En kommersiell standard og sertifiseringsordning levert av Uptime Institute. Standarden deler datasentre inn i ulike klasser etter pålitelighet, tilgjengelighet og oppetid.

I tillegg kan sektorspesifikke standarder som PCI/DSS for finanssektoren, Normen for helsesektoren og TIA 942 for telekom-sektoren være relevante som underlag for kravstilling ved anskaffelse av datasentertjenester. Det er også standarder som NEK 339, NEK EN 50173 og NEK EN 50174 som gir føringer for kabelinstallasjon i blant annet i datasentre.

Klassifisering av datasentre etter pålitelighet og tilgjengelighet

Oversikten på forrige side viser at det er flere standarder som deler inn datasentre i ulike klasser basert på hvor høy grad av pålitelighet og tilgjengelighet de har. De mest kjente er tilgjengelighetsklassene i EN 50600, ISO/IEC 22237 og Tier-klassene fra Uptime Institute. Forskjellen mellom disse er ikke veldig store, men det er likevel enkelte ting som er verdt å bemerke.

- De europeiske og internasjonale standardene er utarbeidet av faggrupper satt sammen av representanter fra ulike organisasjoner, virksomheter og fagmiljøer.
- De europeiske og internasjonale standardene er ikke kommersielt rettet.

Fellestrekkene i de ulike nivåene i overnevnte standarder kan oppsummeres som følger:

Nivå 1 – Basisnivå uten redundans

Består kun av enkle, ikke-redundante føringsveier for strøm og kjøling og har heller ingen redundans for produksjon av strøm og kjøling. Både planlagte og ikke-planlagte aktiviteter vil påvirke IT-infrastrukturen. Det betyr blant annet at det ikke er mulig å gjennomføre vedlikehold på systemene uten at dette påvirker oppetiden.

Nivå 2 – Redundant kapasitet

Datasentre på dette nivået har kun enkle, ikke-redundante føringsveier for strøm og kjøling, men i motsetning til nivå 1 har denne klassen et krav til reservekomponenter for strømproduksjon, UPS og kjøling. Både planlagte og ikke-planlagte hendelser kan påvirke IT-infrastrukturen, spesielt dersom føringsveiene for strøm og kjøling blir påvirket negativt. En feil i reservekapasiteten kan påvirke IT-infrastrukturen, mens en feil i føringsveiene for strøm og kjøling vil påvirke (ingen redundans). I likhet med nivå 1 vil det heller ikke være mulig å gjennomføre vedlikehold uten at dette påvirker oppetiden til IT-infrastrukturen.

Nivå 3 – Vedlikehold uten opphold

Nivå 3 har krav til flere føringsveier for strøm og kjøling (for strømdistribusjon er det kun krav til én aktiv føringsvei til enhver tid). I tillegg er det krav til reservekomponenter for strømproduksjon, UPS og kjøling. Datasentre med denne klassifiseringen kan likevel påvirkes negativt av ikke-planlagte hendelser, men det er mulig å drifte IT-strukturen via andre føringsveier og reservekomponenter ved planlagt vedlikehold. Mange av de norske datasentrene er per 2024 dimensjonert for dette nivået.

Nivå 4 – Feiltollerant

For datasentre med klassifisering nivå 4 er alle føringsveier og reservekomponenter redundante. Det er også krav til at samtlige føringsveier er aktive frem til IT-infrastrukturen. IT-infrastruktur må være tilkoblet to feiltollerante strømkilder. Komplementære systemer og føringsveier må være fysisk isolert fra hverandre slik at feil ikke forplanter seg. Nivå 4 datasentre skal ikke påvirkes av hverken planlagte eller ikke-planlagte hendelser. Samtidig drift og vedlikehold er mulig ved å benytte redundant kapasitet.

Colourbox

Blank

NSM

Nasjonal kommunikasjons-myndighet

Postboks 814
1306 Sandvika

Tlf: 67864000
www.nsm.no
U-24/01412

Postboks 93
4791 Lillesand

Tlf: 22 82 46 00
www.nkom.no