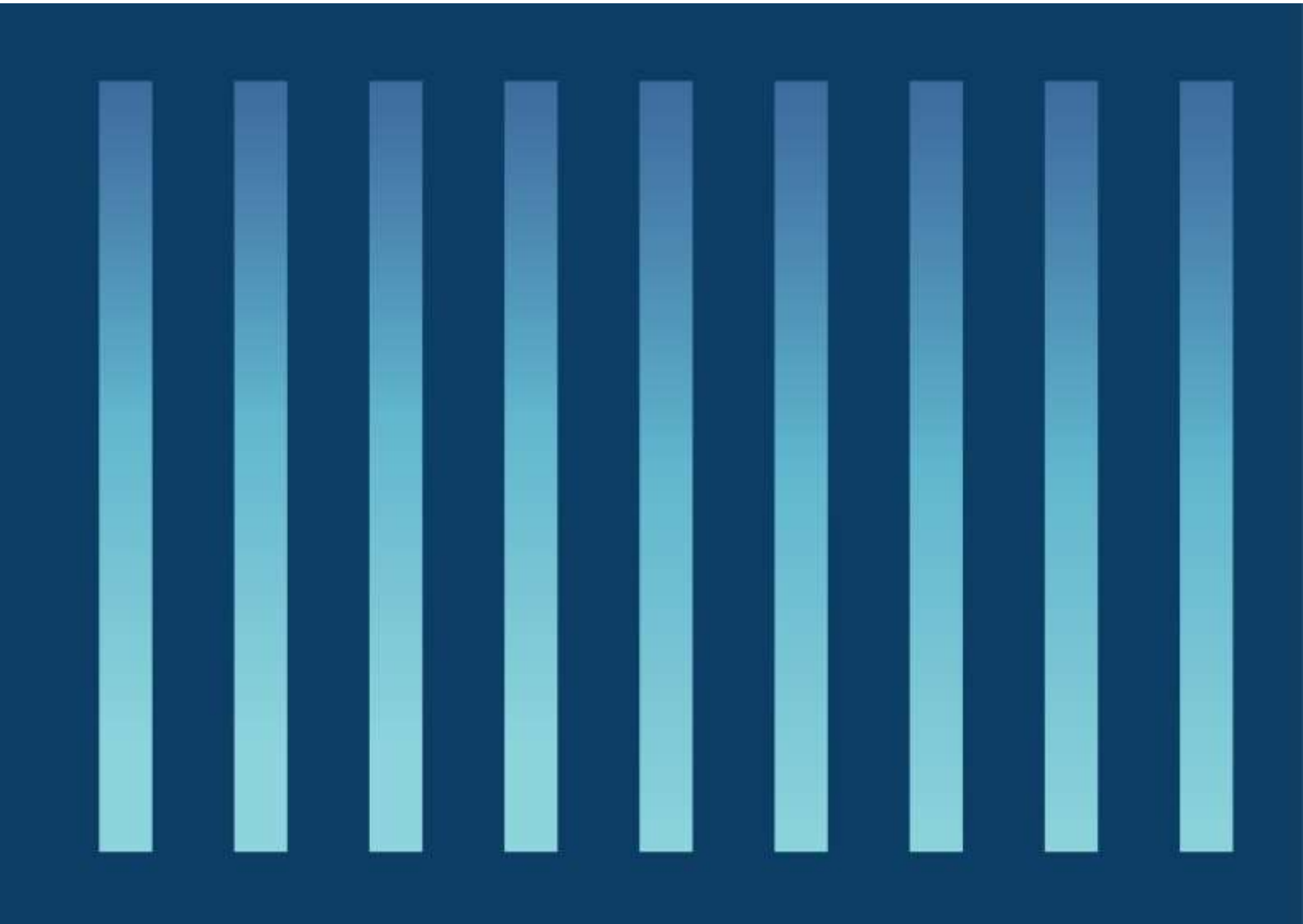
NASJONAL
SIKKERHETSMYNDIGHET

Norske datasenter og digital autonomi

Fire sikkerhetsfaglige anbefalinger ved datasenter

Versjon: 17.01.2022



Sammendrag

Datasentrene er produksjonsfabrikken for våre digitale tjenester, altså der tjenestene prosesseres og lagres. Dette gjelder både for private og offentlige virksomheter. I dagens digitaliserte samfunn er virksomheter avhengig av datasentrene, hvor et bortfall av produksjonsfabrikken vil kunne skape store utfordringer både for virksomhetene selv og deres kunder. Virksomhetene og samfunnet bør derfor vurdere nøye hvordan de realiserer sine tjenester med hensyn til sikkerhet, tilgjengelighet og robusthet.

I denne rapporten gir NSM fire anbefalinger som bør vurderes ved samfunnets bruk av datasentre:

- Anbefaling 1: De funksjonene samfunnet er mest avhengig av bør leveres fra datasentre i Norge.
- Anbefaling 2: Nasjonal digital infrastruktur bør kartlegges.
- Anbefaling 3: Det offentlige bør spesifisere krav til sikring av datasentre.
- Anbefaling 4: Etablere sektoransvar og regulering for datasentre.

INNHOLD

1. Bakgrunn og hensikt

NSM har over tid løftet problemstillinger ved bruk av skytjenester lokalisert i utlandet, spesielt for bruk av samfunnskritiske tjenester og funksjoner.[1] En økende nasjonal avhengighet til utenlandske skytjenesteleverandører skaper bekymring. Bruk av skytjenester bør, for noen virksomheter, vurderes opp mot nasjonal kontroll og krisespennet (fred, krise og krig). Vurderingene bør se om det er behov for at skytjenester leveres fra datasenter i Norge.

Datasentre er produksjonsfabrikkene for de digitale tjenestene, altså der tjenestene prosesseres og lagres. Dette gjelder både for private og offentlige virksomheter. I dagens digitaliserte samfunn er virksomheter helt avhengige av datasentre. Dette inkluderer prosessering og lagring i skytjenester, sosiale medier, mobile nettverk og alle varianter av IKT- og OT-systemer. Flertallet av app-ene på våre mobiltelefoner må ha tjenester levert fra datasenter for å fungere.

Hensikten med rapporten er å øke forståelsen for, og gi noen anbefalinger til, datasentre sin viktige og sentrale rolle og funksjon i vår nasjonale digitale infrastruktur. I forståelsen inngår ikke bare hvilke muligheter datasentrene gir oss, men også hvilke trusler og sårbarheter de eksponeres for og hva det kan medføre for samfunnet. I verste fall kan disse truslene føre til stabilitets- og tilgjengelighetsutfordringer til viktige systemer og tjenester, som igjen påvirker samfunnets evne til å levere kritiske funksjoner.

Nasjonale datasentre er viktige faktorer innen energibruk, næringspolitikk og 5G. Dette kommer blant annet til uttrykk i stortingsmelding Meld. St. 28 (2020-2021) *Vår felles digitale grunnmur.* Viktigheten av å ha datasenter med digitale tjenester levert fra Norge understrekes også i den nasjonale strategien om datasenter *Norske datasenter - berekraftige, digitale kraftsenter (2021)*.

2. Avgrensning og målgruppe

I denne rapporten, om ikke annet nevnes, brukes begrepet datasenter generelt om «alle» typer, størrelser og bruksområder både nasjonalt og internasjonalt. Det er forsøkt avgrenset til selve datasentrene og ikke de tjenester som blir levert fra datasentrene (skytjenester m.m.).

I hovedsak fokuserer denne rapporten på datasentre som leverer tjenester og funksjoner vårt samfunn er avhengig av.[2]

Målgruppen for denne rapporten er departementer og eiere av kritisk digital infrastruktur, sekundært de virksomheter som er avhengige av digitale løsninger levert fra datasentre.

3. Hva er et datasenter?

Det finnes flere definisjoner og mange meninger om hva et datasenter er, men de fleste ser ut til å enes om at det er en installasjon hvor de digitale tjenestene produseres, det vil si prosesseres og lagres. Størrelsen på en slik installasjon kan variere fra et rom med et fåtall rack (utstyrsskap) til store haller med hundrevis av utstyrsskap. I disse skapene innplasseres servere, samt nettverks- og lagringsutstyr.

Et datasenters grunninfrastruktur vil være det som på engelsk kalles «facilities». Dette omfatter selve bygningen med sikringsbarrierer, adgangskontroll og hvor strøm og kjøling distribueres til de enkelte

[1] Se kap 3 i *Helhetlig digitalt risikobilde 2020*, NSM.

[2] Se rapport «Samfunnets kritiske funksjoner» (KIKS2), DSB (2016)

hallene. I tillegg inngår bredbånd som ofte termineres i et såkalt «meet-me room» klar for videre intern distribusjon. Nevnte grunninfrastruktur vil normalt være robust konstruert med redundans og nødbaserte («fallback») løsninger.

Noen av de største globale sky-leverandørene tilbyr også tjenesten DCaaS (Data Center as a Service) som muliggjør etablering av virtuelle datasentre, hvor selve produksjonsressursene kan være lokalisert flere fysiske steder. Ved hjelp av SDDC (Software Defined Data Center) kan virksomheten realisere hybride arkitekturer som integrerer tjenester fra flere skyleverandører med eget utstyr på egen lokasjon (on-premises). Bruken av slike løsninger ser vi øker i volum både hos private og offentlige virksomheter, noe som også bidrar til at flere tjenester og infrastruktur blir lokalisert i de samme fysiske datasentrene.

Hensikten med et datasenter er sikker, stabil og kostnadseffektiv skalaproduksjon som i stor grad baserer seg på gjenbruk, det vil si en deler på fellestjenester for å redusere produksjonskostnadene.

4. Typer av datasenter

Datasentre som benyttes av norske brukere finnes i mange varianter og størrelser både nasjonalt og internasjonalt. En kan imidlertid dele dem inn i to klasser; virksomhetsinterne og kommersielle, og sistnevnte kan igjen være av tre hovedtyper; colocation, hyperscale, og edge.

A) Virksomhetsinternt datasenter

Et virksomhetsinternt datasenter er dedikert for virksomheten selv eller for kunder av virksomheten. I denne definisjonen inngår virksomheter i både offentlig og privat sektor, samt kommersielle aktører som ivaretar datasenteret på vegne av virksomheten. Forsvaret og Telenor er eksempler på virksomheter som har virksomhetsinterne datasentre.

Et virksomhetsinternt datasenter kan realiseres og driftes på forskjellige måter. Selve datasenteret kan for eksempel etableres hos en kommersiell aktør i et colocation datasenter og driftes av en ekstern profesjonell datasenteroperatør. Virksomheten kan i denne modellen også innplassere og drifte løsninger for kunder av virksomheten selv.

Virksomhetsinterne datasentre antas å ha en viktig rolle for tjenester relatert til samfunnskritisk infrastruktur og samfunnskritiske funksjoner. Størrelsen på disse datasentrene er ofte på nivå med hva colocation-aktører tilbyr.

B) Kommersielt datasenter

Kommersielle datasentre drives av en profesjonell aktør som tilbyr datasenter med produkter og tjenester i flere nivå i det åpne markedet. Disse aktørene kan i realiteten tilby alt hva en kunde etterspør av tjenester enten av dem selv eller ved bruk av samarbeidspartnere.

Av kommersielle datasenter nevner vi i det følgende tre ulike varianter: colocation, hyperscale og edge.

1) Colocation datasenter

Et colocation datasenter («serverhotell» eller «samlokaliseringsdatasenter») tilhører en virksomhet hvor forretningsformål er utleie av lokaler/plass til kundens eget utstyr, kraft og kjøling til kunder. Inkludert i dette ligger adgangskontroll og fysisk sikkerhet, samt tilgang til bredbåndstjenester. I tillegg kan virksomhetene tilby en rekke andre tjenester tilpasset kundens behov.

Antall kunder og størrelsen på det de leier ut varierer, men forretningsintensjonen er å gjøre det enklere og billigere for kundene å skalere etter behov. De største sentrene kan ha over hundre kunder og ha flere tusen kvadratmeter areal for utleie.

2) Hyperscale datasenter

Et hyperscale datasenter[3] («stort dedikert datasenter») er større anlegg som ofte er designet for, og eid av, virksomheter med ekstreme krav til skalerbare og robuste tjenester. Slike datasentre stiller strenge krav til robuste og redundante leveranser av kraft og bredbånd, samt at det selvfølgelig skal være bærekraftig når det gjelder miljøutslipp.

3) Edge datasenter

Edge datasenter er betegnelsen på mindre datasentre som etableres desentralt for å ivareta tjenester med krav til lokal prosessering, lagring, latens og sikkerhet. Edge datasenter karakteriseres ved at de etableres lokalt og hvor virksomhetene har behov for hurtig respons, men det kan også være andre tjenester som genererer behovet, eksempelvis behov for lokale tjenester, sikkerhet og en eventuell utnyttelse av muligheten som etablering av private nettverk kan gi for virksomheter. Bakgrunnen for navnet er det engelske ordet «edge», som betyr «kant», og peker på at datasentrene plasseres i «kanten» av nettverket. Det forventes etablering av flere edge datasenter som en mulig konsekvens av utbyggingen av 5G.

5. Aktører i bransjen

Den kommersielle datasenterbransjen består av aktører som tilbyr infrastruktur og tjenester i flere nivå, fra utleie av lokaler til totalleveranse av IT-tjenester. Aktørene innenfor datasenter og datasenterbransjen opererer med basis i forskjellige forretningsmodeller og innretter seg i stor grad mot ulike kundesegmenter både nasjonalt og ikke minst internasjonalt. De tilbyr tjenester og infrastruktur både innenfor det kommersielle og det virksomhetsinterne markedet.

I det virksomhetsinterne markedet er et viktig forretningsområde å levere komplette tjenesteleveranser til kundene. Dette inkluderer datasentre, nettverk, plattform- og applikasjonsdrift, tilgangstjenester med mer. For noen innebærer dette drift og forvaltning av en virksomhets komplette IT-infrastruktur. Selve datasentrene leier de ofte av kommersielle colocation-aktører.

De kommersielle aktørene kan være alt fra sikkerhetsbevisste aktører som håndterer mye kritisk infrastruktur, til aktører med færre ressurser og lavere potensiale til å etablere sikre infrastrukturer.

Hvem eier så datasenteraktørene? I dag er ikke bransjen underlagt noen sektorer eller særegne lovverk. Det vil si at det kun er vanlige krav til forretningsvirksomhet som kan regulere datasenteraktøren.

I Norge er ikke datasentre særskilt regulert, så her vil det være de enkelte kundenes krav som gjelder, og som de kommersielle operatørene bør oppfylle ved kontraktsinngåelse. Et eventuelt unntak er om datasenteret underlegges sikkerhetsloven eller sektorvise lover, forskrifter og krav.

[3] Det er vanlig å benevne de aktører som eier og driver hyperscale datasentre for «hyperscalere». Det er de aller største globale aktørene som Google, Microsoft og Amazon som har denne betegnelsen.

6. Datasenterets rolle i vår nasjonale digitale infrastruktur

I et digitalisert samfunn som Norge utgjør ekom-infrastrukturen og datasentre fundamentet i vår nasjonale digitale infrastruktur: Ekom for transport av alle typer digitalt innhold og datasenter for innplassering av alle typer IKT-plattformer og tjenester. For at alt dette skal fungere er det nødvendig med en sikker og stabil kraftforsyning med høy kapasitet, noe som gjør at muligheten for kraftforsyning bør inkluderes og tas hensyn til ved planlegging av datasentre og lokalisering av disse nasjonalt.

Med ekom-infrastrukturen menes her den infrastrukturen som utgjør transport- og aksess-laget både innenlands og mot utlandet, samt de tjenestene som skal til for at et datasenter skal fungere.

Det er i dag sivile aktører som bygger infrastrukturen til ekom og datasentre. Dette gjøres ut ifra kommersielle strategier og resultatkrav som ikke nødvendigvis er forenlig med at samfunnets sikkerhetsbehov ivaretas. En slik utvikling kan redusere virksomhetens muligheter for beredskapsalternativer ved at alt produseres i de samme datasentrene og transporteres over de samme ekom-løsningene.

Dersom det oppstår nedetid i vår nasjonale digitale infrastruktur vil overliggende tjenester berøres om ikke infrastrukturen i tilstrekkelig grad har hensyntatt redundans, robusthet og sikkerhet. Med overliggende tjenester menes de tjenester og plattformer som har avhengigheter til den nasjonale infrastrukturen, eksempelvis mobiltjenester, Internett-tilgang, TV-distribusjon, radio-distribusjon (DAB), Forsvarets ulike nettverkstjenester og nødnett-tjenestene.

7. Datasenterets rolle i den norske beredskapen

Store deler av samfunnets beredskap er i dag basert på vår nasjonale digitale infrastruktur.

Digitale løsninger som er sentrale i beredskap og krisehåndtering, bør kunne tåle flere samtidige hendelser. De bør være mer robuste og tilgjengelige enn vanlige kommersielle løsninger, da de skal fungere i situasjoner hvor mye annet er utilgjengelig. Det bør etableres fysisk og logisk redundans i underliggende infrastruktur, i datasentrene og i den enkelte digitale løsning for å sikre en høy grad av tillit til leveransene. I planlegging av beredskapen bør det derfor legges vekt på hvor de digitale løsningene leveres fra, altså fra hvilke datasentre, slik at alternative produksjonskapasiteter er etablerte og tilgjengelige. Mangelfulle alternative løsninger for infrastrukturområdet kan føre til større konsekvenser for samfunnet ved nedetid.

Militær- og sivil sektor vil i økende grad benytte felles digital infrastruktur og tjenester vil kjøpes fra de samme kommersielle aktørene. Dette gjør at militær og sivil sektor deler de digitale sårbarhetene, noe som øker totalforsvarets behov for alternativer i form av infrastruktur og tjenester. Hvis Forsvaret i større grad baserer seg på sivil infrastruktur, må denne vurderes og sikres i henhold til Forsvarets behov i hele krisespennet. I tillegg kommer betraktninger rundt folkeretten som ikke utdypes nærmere her.

8. Trusler og sårbarheter i et datasenter

Truslene mot og sårbarhetene i et datasenter vil, med noen unntak, være de samme som vi kjenner fra digital sikkerhet. I et datasenter vil nivået på risikoen bestemmes av verdien av den produksjonen som utføres og de konsekvensene som oppstår om en hendelse skulle inntreffe.

Dersom vi tenker oss et eksempel hvor banktjenestene i Norge produseres i noen få datasentre, så er det naturlig å tenke seg at disse datasentrene er kritiske for det norske samfunn. Kan samfunnet stole på at disse produksjonsstedene gir god nok redundans? Klarer disse datasentrene å opprettholde tjenestenivået ved flere samtidige hendelser? Det blir fort snakk om økonomi, og hvem som skal betale for denne sikkerheten. I dag er det virksomhetene selv som gjør vurderingen og tar kostnaden.

Selv om dette er et tenkt scenario så ser NSM flere eksempler på konsentrasjon av kritiske digitale tjenester i et fåtall datasentre. Dette skjer innenfor både offentlige og private virksomheter og innen de fleste sektorer.

Konsentrasjonen av verdier i datasentre øker konsekvensene av en potensiell innsider plassert hos datasenteraktøren. Dette henger selvsagt sammen med til hvilken grad det er etablert tilstrekkelige autorisasjonsskiller mellom ulike kunder, eller kunde og datasenteraktøren.

Insiderrisiko henger også til dels sammen med problemstillinger knyttet til eierskapsutfordringer. Risikoen kan endres/økes avhengig av forhold på datasenteraktørens eierside. Eksempelvis kan økonomien i eierselskapet påvirke risikoappetitt. Videre kan nasjonal tilknytning ha en betydning. Er vi like villige til å plassere våre digitale produksjonsfabrikker i øst som i vest?

Datasenter vil ofte være av typen «lights out» hvor det kun er tilstedeværelse av dedikert datasenterpersonell for å montere og reparere utstyr fysisk. Hensikten er å unngå feilsituasjoner knyttet til arbeid i hallene. Dette gjør at konfigurering og overvåkning av grunninfrastrukturen utføres via fjernarbeid, noe som krever dedikerte administrasjonssystemer. Disse lokaliseres normalt i egne sikkerhetssoner og med egne adgangssystemer. Dersom en trusselaktør får tilgang til disse, vil aktøren ha store muligheter for å utføre sine uønskede aktiviteter. Denne sårbarheten vil kunne øke om datasenteret også tilbyr server, lagring og nettverk og eventuelt andre tjenester, hvor administrasjonssystemene er plassert i tidligere nevnte sikkerhetssone.

Tilveksten av skytjenester har bidratt til standardiserte arkitekturer som kan skape mer robusthet og skalerbarhet. Dette gjelder spesielt de store globale skyleverandørene, som har brukt milliarder av kroner på å lage et distribuert nettverk av datasentre og "tilgjengelighetssoner", sammen med programvareverktøy som lar kundene replikere data, slik at tjenester ved en feilhendelse automatisk kobles til en reserveløsning. For de mindre datasenteraktørene vil bildet være et helt annet, da nevnte sikkerhetstiltak krever store investeringer, kompetanse, og ikke minst betalende kunder.

9. Anbefaling 1: De funksjonene samfunnet er mest avhengig av bør leveres fra datasentre i Norge.

Vi har behov for datasentre i Norge for å sikre det norske samfunnets digitale autonomi. Det offentlige Norge benytter seg i økende grad av IKT-tjenester levert fra datasentre som er lokalisert og driftet utenfor Norge. Flere sektorer og virksomheter ønsker å benytte disse også til samfunnskritiske funksjoner. Sikkerhetsloven avgrenser ikke mot bruk av utenlandske datasentre, men kritikaliteten vil gi føringer.

Dersom datasentre med tjenester hadde vært lokalisert i Norge, hatt norske eiere, og administrert og driftet fra Norge, kunne de i større grad vært benyttet til samfunnskritiske funksjoner og skjermingsverdig informasjon av betydning for nasjonale sikkerhetsinteresser.

NSM mener de funksjonene samfunnet er mest avhengig av bør kunne leveres fra datasentre i Norge, eller funksjonene må kunne re-etableres i tide, for å kunne gi tilstrekkelig ytelse i fred, krise eller krig.

Hvorvidt samfunnskritiske funksjoner kan plasseres utenfor Norge må vurderes mot gjeldene lovverk. En utflytting må også risikovurderes med tanke på en eventuelt reetablering i Norge.

10. Anbefaling 2: Nasjonal digital infrastruktur bør kartlegges

Ved å analysere dagens tjenesteleveranser til offentlige og sentrale funksjoner, ser vi at disse leveres fra et fåtall datasentre (eks. bank-tjenester). Dette tilsier at en konsentrasjon av verdier kan samles i de samme datasentrene. Hvis vi antar at våre digitale samfunnskritiske funksjoner blir levert fra et fåtall datasentre utgjør dette en nasjonal sårbarhet. Slike datasentre antas også å være attraktive mål for sabotasje.

NSM mener det bør gjennomføres en kartlegging av hvor (i hvilke datasentre med avhengigheter) kritiske samfunnsfunksjoner produseres.

Kartleggingen vil avdekke om sektorer og deres redundans kan være mer konsentrert i få datasentre enn den enkelte brukeren eller sektoren kan få oversikt over. Kartleggingen må være periodisk. Kartleggingen bør omfatte datasentre både i og utenfor Norge. For norske datasentre bør kartleggingen inkludere avhengigheter til hvilke ekom-nettverk og kraftleveranser som forsyner datasentrene. De to sistnevnte har Nkom og NVE oversikter over, men det er koblingen mellom alle tre som eksponerer sårbarheten i et nasjonalt, digitalt infrastruktur perspektiv. Det er også relevant å høre bakgrunnen for de virksomheter som benytter utenlandske datasentre, og hva som skal til for at de skal kunne benytte norske datasentre.

11. Anbefaling 3: Det offentlige bør spesifisere krav til sikring av datasentre

Datasenteraktører kan være alt fra sikkerhetsbevisste aktører som håndterer kritisk infrastruktur, til aktører med færre ressurser og muligheter til å etablere sikre infrastrukturer. For å øke sannsynligheten for datasenteraktører har innført gode sikkerhetstiltak og -rutiner bør datasenteret og aktøren være sertifisert i henhold til anerkjente, internasjonale standarder. Dette kan for eksempel være sertifisering etter EN 50600 og ISO 27001. Anerkjente sikkerhetsstandarder, veiledninger og beste praksiser bør i tillegg benyttes for å etablere gode sikkerhetstiltak. Logiske styringssystemer med tilhørende infrastruktur eksempelvis DCIM (DataCenter Infrastructure Management system) anbefales vurdert opp mot *NSMs grunnprinsipper for IKT-sikkerhet.*

Dersom en trusselaktør har fysisk tilgang til en server eller annet utstyr, så er den å anse som tapt eller kompromittert. Hvis datasentrene ikke er forsvarlig sikret og tilstrekkelig robuste, vil øvrige sikkerhetstiltak ha liten effekt.

NSM mener det offentlige bør spesifisere krav til fysisk og logisk sikring av datasentre og krav til personell med tilgang, inkludert underleverandører.

12. Anbefaling 4: Etablere sektoransvar og regulering for datasentre

Datasenterbransjen består av aktører som tilbyr infrastruktur og tjenester på flere nivåer, fra utleiere av lokaler til de aktører som håndterer og leverer «alt» en virksomhet måtte ønske. Noen større

virksomheter besitter eller leier datasentre for intern bruk. Under gjeldende regelverk stilles det få eller ingen særskilte krav til sikkerhet i datasentre. Imidlertid kan noen tjenester og informasjonssystemer som innplasseres være underlagt og regulert av lovverk. Med tanke på at operatørene av datasentre i tillegg til fysisk sikring har ansvaret for leveranse av grunnleggende infrastrukturtjenester som strøm, kjøling og bredbånd, er dette å anse som svært sårbart.

I den nasjonale datasenterstrategien foreslås det at *«datasenter blir vurderte for relevant og formålstenleg regulering i ekomregelverket, for å følge opp den samla risikoen og sårbarheita hos ein datasenteraktør, som samlar og driftar aktivitet frå fleire ulike verksemder».* Regjeringa vil at datasenter blir vurdert for regulering i ekomlovverket og andre relevante lovverk for å ivareta digital sikkerhet og nasjonale sikkerhetsinteresser.

I gjeldende strategi er det ønskelig at Norge gjennom EØS-avtalen blir en del av EUs indre marked, også for datasentertjenester. Dette er et argument for at bransjen underlegges et sektorlovverk, da EUs ulike strategidokumenter stiller klare krav til datasenteraktørene.

Lovregulering av datasenter må komme på plass. Reguleringen bør blant annet omfatte krav til sikkerhet, krav til oversikt og vurdering av verdier plassert i datasenter og krav til flytting av ulike typer data og tjenester fra virksomheten til datasenter og imellom datasentre.

Dersom datasentre leverer funksjoner som er avgjørende for nasjonal sikkerhet, så skal disse underlegges sikkerhetsloven og gis et forsvarlig sikkerhetsnivå. Her må departementene og virksomheter i større grad være bevisst, verdivurdere og eventuelt utpeke datasentre som skjermingsverdige.

Flere aktører i bransjen tilbyr leie av infrastruktur som kan leveres fra nasjonale og internasjonale skyplattformer eller som dedikert infrastruktur. Dersom utstyret/tjenestene benyttes til kriminell eller terrorlignende aktiviteter, er det svært utfordrende å spore da det ikke er noe registreringskrav av hvem som leier og hva det eventuelt skal benyttes til. Det er heller ingen krav til eller registrering av eierne til datasentre utover det som kreves som byggherre.

En slik situasjon skaper utfordringer ved hendelseshåndtering og etterforskning. Den nye datasenterstrategien nevner at tiltak nå blir diskutert på EU-nivå, og at det er viktig at Norge deltar i dette arbeidet.

Det bør vurderes å pålegge en registreringsplikt for datasenteraktører.

13. Økt krav til lokalisering og sikker aksess

Norge bør stimulere den forventede fremveksten av regionale og lokale datasentre som følger av 5G Edge Computing (Multi-access Edge Computing). Dette er datasentre bestående av distribuerte regionale og lokale datasentre. Skytjenester levert fra slike «edge compute» datasentre kan kalles «distribuert skytjeneste». Denne distribuerte skyen kan bidra til at Norge har nødvendig datakraft (lokalt tilgjengelig, redundant og autonom) når krisen rammer og de lange linjene til fjerntliggende datasentre svikter.

Det er mindre viktig om det er det offentlige, telekom-operatører og deres partnere, eller operatører av dagens skytjenester som eier og drifter disse lokale datasentrene. Det viktige er at de er distribuerte utover landet der brukerne er, og ikke fjerntliggende/sentraliserte slik de kan være med dagens datasentre. Et viktig moment er altså ikke privateid fremfor offentlig eid, men trygghet for at virksomhetene og brukerne har tilgang til sine data og programmer under alle omstendigheter.

Et bortfall av datasenter vil skape store utfordringer for mange virksomheter, og vil kunne få store konsekvenser for samfunnets evne til å levere digitale tjenester. Det er derfor viktig at arbeidet med digitalisering av samfunnet inkluderer bevissthet på verdien av sikre og robuste datasentre i Norge.