Innholdsfortegnelse

Introduksjon

I en verden som stadig blir mer digitalisert er lagring og prosessering av data i offentlig sky et mer agilt, tidsbesparende, sikkert, miljøvennlig og kostnadseffektivt enn andre alternativer.

Det er et klart behov for offentlig sektor å digitalisere seg raskere. Utfordringer, bekymringer, tvetydighet og mangel på kunnskap rundt lovgivning og tekniske løsninger har ført til at digitalisering i offentlig sektor gått noe saktere enn andre sektorer. Samtidig ser vi at aktører som "knekker koden" kan ta ledende posisjoner innenfor digitalisering, og Norge er et land som kan skryte av ledende fagmiljøer og løsninger som plasserer oss som en av de ledende nasjonene innenfor digitalisering. Den desentraliserte organiseringer vi har i Norge tillater både større aktører å innovere, og kan samtidig skape noen utfordringer for de mindre aktørene som ikke har tilsvarende ressurser.

Bruk av offentlig sky krever en interdisiplinær tilnærming over både det juridiske og det tekniske domenet. Juridiske tiltak kan ikke løse alle tekniske utfordringer, og tekniske tiltak kan ikke løse alle juridiske utfordringer - men vår påstand er at man kan nå en tilstrekkelig grad av risikoreduksjon gjennom forståelse og avveininger på tvers av domenene.

Derfor ønsker vi å legge til rette for et åpent samarbeide i å utvikle malverk som skal fasilitere for bruk av skytjenester i offentlig sektor. Vi gjør dette i en "open-source ånd", og inviterer alle interesserte parter i å bidra. Microsoft og noen utvalgte partnere og domeneeksperter har tatt på seg å lede an i dette arbeidet, men vi er til slutt avhengig av en åpen og konstruktiv debatt og bidrag fra langt flere enn kjerneteamet for å kunne lage løsninger som vil bli allment akseptert.

Målet for dette prosjektet er å kunne gi forslag til holistiske arkitekturer som dekker 80-90% av de bruksområdene vi ser i offentlig sektor. Referansearkitekturene vil ta utgangspunkt i klassifisering av data og krav til tilgjengelighet for å gi anbefalinger i henhold til teknologivalg og plassering av data og applikasjoner på tvers av offentlig sky og hybride løsninger (on-premise).

Helt konkret er målet å levere både referansearkitekturer og verktøy for raskt å kunne bygge såkalte "landingssoner" for ulike risiko og/eller klassifiseringsdomener for bruk av IaaS og PaaS tjenester.[1]

Dette prosjektet vil også ha verdi for privat næringsliv i regulerte industrier, eller som ønsker å klassifisere data og risiko på samme måte, og spesielt for aktører som arbeider eller leverer inn til offentlig sektor.

[1] Vi tar ikke med SaaS-tjenester i dette prosjektet, da ansvarsforholdet er annerledes og dermed er det behov for en noe annerledes diskusjon, samt at det allerede er ganske god forståelse av hva dette betyr og hvordan det må håndteres i markedet.

Felles utfordringer for offentlig

- Teknisk gjeld
- Mangel på ressurser (Personell)
- Mangel på kompetanse
- IT Support
- Utdaterte systemer (Og da usikre eller lite fleksbile systemer)
- Sikkerhet & Forensic
- Mangel på alternativer
- Tradisjonell sonemodell/IT infrastruktur vs moderne sky-miljø
- Mangel på standardisering (duplikater av fellestjenester, mangel på tjenestekataloger++)
- GDPR & Data Governance
- Kommunesammenslåing
- Kost
- Tilknytting til Helsenett

Risikovurderinger (list vanlige risikoelementer som diskuteres og hvordan det kan begrenses/minimaliseres).

- Brudd på fiberkabler (Datasenter eller hel region)
- Strømbrudd (Datasenter)
- Tjeneste(r) går ned (oppgradering, patching)
- Leverandør går konkurs
- Ikke tilgjengelig kapasitet
- Myndigheter ber om innsyn
- Hacker(e) får tilgang (Storage, compute)
- Korrupt ansatt (internt)
- Korrupt ansatt (vendor/tredjepart)
- Korrupt ansatt (skyleverandør)
- Myndigheter klarer å digital tilgang til datasentere
- Fysisk tilgang til utstyr
- FISA 702

Landingssoner

Landingssoner i Azure består av flere abonnementer i satt opp på en skalerbar måte og som samtidig ivaretar sikkerhet og tilhørende tjenester som nettverk og identitet.

Landingssoner muliggjør migrering, modernisering og innovasjon i stor-skala i Azure.

Sonene som etableres tar høyde for alle plattformressurser som er nødvendig for å understøtte en bedrift's applikasjons-portefølje og differensierer ikke mellom infrastruktur som tjeneste og plattform som en tjeneste.

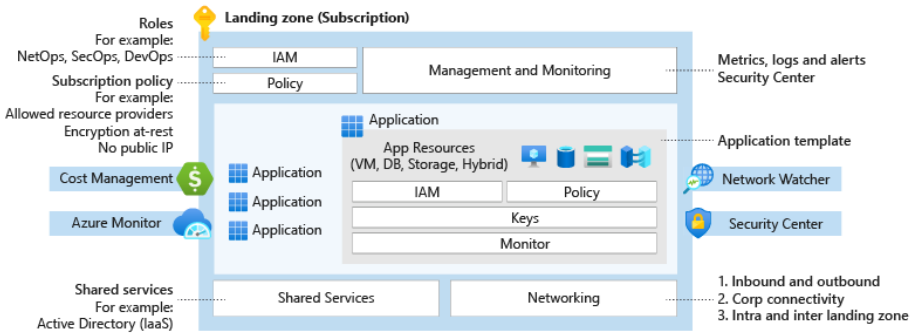

Figure 1: Landingssone

Tilgjengelighet (SLA)

- Høy tilgjengelighet (E.g - Konsumenttjeneste) 99.99 eller 99.95% oppetid. Noe nedetid (minutter) per år aksetabelt. Redundante server(e) og lagringskopier - men ikke på tvers av datasentere.
- Meget høy tilgjengelighet (e.g. pasientsystem) 99.99% eller høyere. Redundante servere og kopier av data på tvers av datasentere (med mer enn 10 km avstand).
- Unntakssituasjon (Disaster scenario) En hel region går ned og blir utilgjengelig.
- Fullstendig suverenitet/autonomitet (autonomity/soveriginity) Skyleverandør går konkurs, Norge mister all kommunikasjon med omverden, systemer som må fungere uavhengig av skyleverandør.

Gjenopprettingspunkt (RPO)

Tradisjonell sonemodell

Hva er sky?

Hva er et datasenter

I informasjonsteknologiens spede barndom var det en gjengs oppfattning at verden kun ville trenge et begrenset antall datamaskiner. Vi kan kalle dette "stormaskinens tidsalder", og de fleste som benyttet en datamaskin jobbet gjennom en terminal som gav tilgang til data og regnekraft som befant seg i en sentral datamaskin. Disse stormaskinene befant seg typisk i datarommet til en organisasjon eller bedrift - en fysisk sikret lokasjon hvor kun autorisert personnel hadde tilgang.

Etterhvert som avhengigheten til datasystemer økte, ble det satt større og større krav til fysisk sikring og redundans for slike datarom, og det ble etterhvert både vanskelig, upraktisk og ulønnsomt å etterleve disse kravene for hver enkelt organisasjon og bedrift. Samtidig fikk vi ny og raskere nettverksteknologi som gjorde det mulig å flytte både stormaskiner, servere og data lengre unna brukerne. Dette la grunnlaget for en ny industri: datasenterindustrien.

Idag er datasenterindustrien en sentral komponent i vår digitale infrastruktur. Dedikerte datasenterleverandører leverer redundante tilkoblinger til nettverk- og elektrisitetsnett, nød-aggregater som holder datasenteret igang selv gjennom lange perioder med strømbrudd, og strenge tiltak for fysisk sikring slik som perimetersikring kombinert med videoovervåking og døgkontinuerlig bemanning.

I dag vil de aller fleste organisasjoner velge å benytte en profesjonell datasenterleverandør fremfor å bygge sitt eget datarom.

Hva er så sky, og hvordan skiller skyleverandører seg fra datasenterleverandører?

Idag bærer stort sett alle rundt på både mere regnekraft og lagringsplass en vi trenger. (Faktisk har en moderne smarttelefon mer regnekraft enn hele land hadde tilgang til for bare tiår siden. TODO: Kilde) På samme måte har de fleste datarom mer regnekraft og lagringsplass enn organisasjonen som eier det trenger. Vi overdimensjonerer systemene våre for å kunne ta unna for perioder med intens bruk - tenk 8-timers arbeidsdag for de fleste organisasjoner og bedrifter, black-friday og julehandel for varehandelen, og frist for innlevering av skattemeldingen for alle norske borgere. Dette fører til at vi har mange enkeltsiloer av overdimensjonerte systemer - dette er både dyrt og har store miljøimplikasjoner. Datasenterindustrien er i ferd med å bli en av verdens mest energikrevende bransjer. (TODO: Kilde)

Med skyteknologi så endres måten man kan kjøpe regnekraft og lagringsplass seg dramatisk. Organisasjoner kan nå kjøpe bare det de har behov for, når de har behov for det. En bedrift i varehandelen kan skalere opp før black-friday, og ned igjen etterpå. De kan til og med designe systemet sitt slik at det autoskalerer med bruk. Finn.no har for eksempel XX% av besøkene sine innenfor lunsj-perioden på hverdagene (TODO: Kilde). Resten av tiden trenger de bare en

brøkdel av regnekraften - som så kan frigis av skyleverandøren og selges til andre kunder, for eksempel forskningsorganisasjoner som kjører store jobber som ikke er tidskritiske - og derfor kan kjøpe kapasitet rimeligere, siden deres jobber kan aktivieres når det er mindre behov i markedet. Store skyleverandører vil også flytte om på workloads for kunder, slik at servere, racks, eller til og med hele datasentre kan skrus av for å spare energi i perioder med lav etterspørsel.

En annen forskjell på en datasenterleverandør og en skyleverandør er tjenestespekteret. Mens en datasenterleverandør er som en avansert utleier av fysisk plass, er en skyleverandør også en programvare- og driftsleverandør av hundrevis av avanserte tjenester som gjør det mulig å bygge digitale systemer raskere og bedre.

...

Fysisk og logisk sikring av datasentre

Ansvarsmodellen for offentlig sky

Klassifisering

- Ikke sensitivt (Ikke PII)
- Sensitivt (PII mm.)
- Begrenset (Sikkerhetsloven)
- Konfidensielt (Sikkerhetsloven)
- Hemmelig (Sikkerhetsloven)
- Strengt hemmelig (Sikkerhetsloven)

Klassifisering av data

Risikoklassifisering av systemer

Referansearkitektur

Rent overordnet kan man se på en ende-til-ende arkitektur - hvor vi tenker bør skille på hva som lovmessig må ligge i egne datasentere (lovmessig reguleringer/krav) og hvordan vi bør klassifisere applikasjoner.

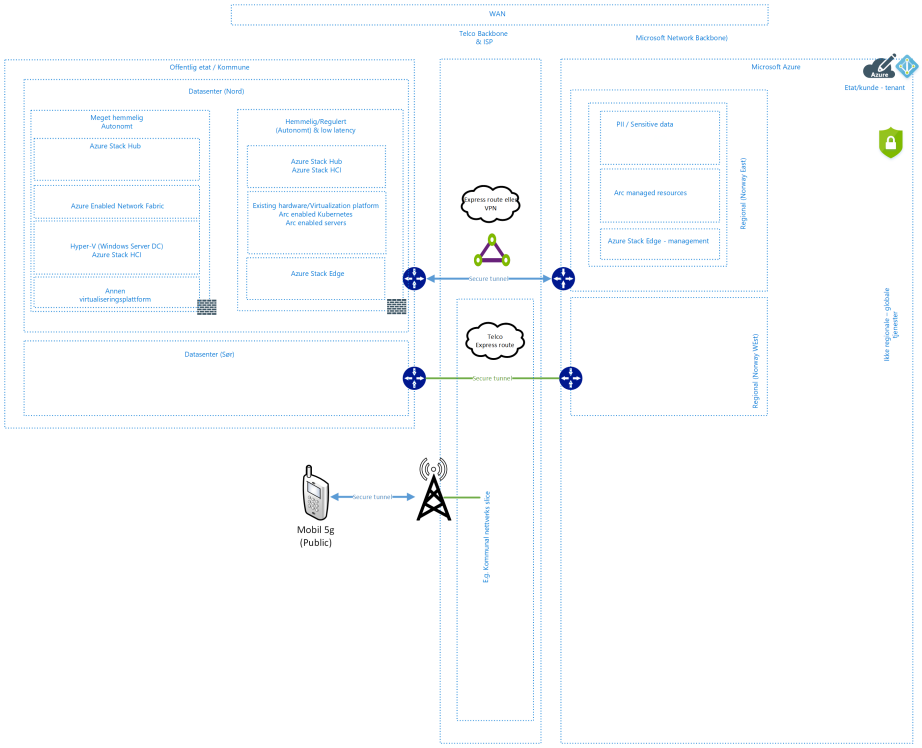

Figure 2: High-level

Klassifiseringmatrise for applikasjoner

Her er et forsøk på hvordan vi kan tenke rundt klassifisering/skille av applikasjoner:

- Publikumstjeneste/Applikasjon (Internet exposed)
- Intern applikasjon (interne ansatte)
- PII
- Ikke PII
- Ikke sammfunnskritisk (tåler noe nedetid)
- Sammfunnskritisk - delte tjenester (nasjonale)

Sammfunnskritiske tjenester som må kjøre og være tilgjengelig som er delt på tvers av lokasjoner/uavhengig av lokasjon.

Sluttbrukere/systemer bruker internet (VPN eller MPLS).

- Sammfunnskritiske - lokale tjenster (edge) Sammfunnskritiske tjenester må fungere i nødssituasjon hvor deler faller ut og tåler lite/eller ingen nedetid eller er svært sensitive til latens.

Sluttbrukere/systemer befinner seg lokalt (e.g. et sykehus/sykebil) mm.

- Særskilte lover (hvor public cloud gjør det umulig)

On-premises

Dette er servere (virtualisert eller bare-metal) du har i dine egne datasentere hvor du kan drifte deler av applikasjonsporteføljen.

Nettverk

Du kan sikkert knytte ditt kontor til Azure ved hjelp av f.eks Site-to-Site VPN eller Azure Express Route.

Dersom det er behov for svært mange klienter tilknyttet et virtuelt nettverk og/eller det er mange kontorer som skal tilknyttes - så bør man vurdere å kombinere dette med Azure Virtual WAN.

Sikring av nettverk

I Azure finnes det mange aspekter av nettverkssikkerhet. På mange måter kan man designe en nettverkstopolgi som ligner et tradisjonelt datasenter med segmentering mm.

Man kan sikre trafikkflyt og nettverk i Azure med blant annet NSGs (Network security groups), Application Security groups, Brannmurer (Azure Firewall - eller tredjeparter slik som Barracuda, BigIp/F5 mm.).

I tillegg bør du basere sikkerhetsmodellen din på en "Zero Trust" modell (Se Zero trust in Azure her).

Tekniske komponenter for sikring og compliance

- Azure Datasenter sikring
- Customer Lockbox
- Confidential computing
- Azure Policy
- Customer managed Keys (Kryptering og Bring-Your-Own-Key)
- Azure Dedicated HSM
- Azure ARC
- Azure Dedicated Hosts

Utvalgte sikkerhetselementer

- Security baseline
- Security baseline (Azure Stack Edge)
- Security baseline (Azure Stack HCI)
- Azure Active Directory : Conditional access
- Azure Active Directory : Privileged identity management (PIM)
- Microsoft Defender for Cloud
- Azure DDOS Protection

Krisesituasjoner

I en særskilt krisesituasjon bør vi stille oss følgende spørsmål:

- Hvor lang tid tar det før ditt eget utstyr begynner å feile?
- Hvilke 'skjulte' avhengigheter har dine systemer?
- Hvordan skal sluttbrukere nå applikasjoner som er eksponert på internett? (DNS/Sertifikater mm.)

Særskilte norske krav (som man bør ta stilling til)

- Arkivloven: *"Arkivloven inneholder ingen bestemmelser som direkte regulerer lagring av arkiv i skytjenester, og er i utgangspunktet ikke til hinder for bruk av slike løsninger. Det følger likevel av arkivloven § 9 b at arkivmateriale ikke kan «førast ut or landet, dersom dette ikkje representerer ein naudsynt del av den forvaltningsmessige eller rettslege bruken av dokumenta." Når det er lagt til grunn at den fysiske lagringsplassen avgjør hvor data er å finne, følger det naturlig av denne bestemmelsen at overføring av arkivmateriale til servere i utlandet bryter med forbudet mot å føre arkiv ut av landet."*
- [Bokføringsloven]
- [Sikkerhetsloven]
- [NKOM]
- [NSM]

Datacenters in Norway

- 2 datasentere i Norge
- Datalagring i Azure
- Availability Zones in Norway
- Mission Critical workloads in Norway

Rapporter, audit, innsyn

Klareringssenter inneholder hundrevis av rapporter, innsyn og tredjepart audits for Microsoft sine tjenester i sky. Her kan du finne alt fra linker rundt overholdelse av regler og standarder, personvern, datainnsyn mm.

Alternativt kan du også gå inn her for å finne rapporter direkte: https://servicetrust.microsoft.com/ ## Schrems-II - EU Data Boundry - EU Data Boundry - FAQ

GDPR

Som kunde opprettholder du eierskap til kundedata – innhold, personlige kundedata og andre data du leverer til lagring og drifting i Azure-tjenestene. Du har også kontroll over eventuelle andre geografiske områder der du bestemmer deg for å rulle ut løsningene eller replikere dataene dine.

Der en tjenestes funksjonalitet krever global datareplikering, er detaljene tilgjengelige her.

Linker

- Protecting privacy in Microsoft Azure
- Microsoft EU Data Boundary
- Trusted Cloud
- Datalagring i Azure
- Microsoft Azure SOC Rapporter
- Online Services Terms for Microsoft Azure

Verktøy

- Azure Advisor
- Microsoft Defender for Cloud
- Azure Policy
- Azure Optimization Engine