Malverk for bruk av Sky i Offentlig Sektor

Introduksjon - Formål

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.

Hva som kan forventes

- Referanse arkitektur(er)
- Blueprints og maler for deployment
- PDF/Whitepaper (bygges automatisk basert på Github)
- Artikler, linker og enkelte tekser til juridiske vurderinger for å addressere GDPR/Schrems-II/mm.

Bidrag

Dette er et samarbeid mellom Microsoft, annerkjente tjenestelevandører og offentlige instanser for å utforme retningslinjer, maler og arkitektur for applikasjoner på Microsoft sine skyplattformer (Azure, Microsoft 365, Power Platform mm).

Bidra gjerne med innhold direkte gjennom pull requests, eller lag issues rundt konkrete utfordringer/problemstillinger. Vi ønsker en åpen og bred diskusjon slik at dette prosjektet kan bidra til å komme raskere frem til akseptabel løsningsforslag for de mest relevante utfordringene for offentlig sektor.

Disclaimer

Dette arbeidet er ikke offisielt sertifisert materiale og har ikke gjennomgått juridiske vurderinger. Dette er et frivillig samarbeid av flere aktører for å bidra med forslag til hvordan offentlig sektor kan ta i bruk skytjenester, men den ultimate juridiske og tekniske vurderingen må fortsatt gjøres ihht gjeldende lover og regler for hver instans som benytter materiale fra dette prosjektet.

Bidragsytere

- Microsoft (Harald S. Fianbakken, Christopher Frenning, Henry Hagnäs)
- Crayon (Jan Egil Ring)
- Sopra Steria (Marius Sandbu)
- ..

Innholdsfortegnelse

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.

...

Klassifisering

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

Tilgjengelighet

- 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.