Oppgave A1:

Cloud computing teknologier muliggjør det for brukere å aksessere sky data og tillater brukere lagring av data og tilpasse applikasjoner, og aksessere ressurser og tjenester gjennom internett (i en sky). Dette kan blant annet aksesseres via en mobiltelefon eller en laptop og muliggjør det for en bedrift eller en organisasjon å lagre og administrere store mengder av data i skyplattformen istedenfor at det gjøres lokalt. Cloud teknologier kan bidra til en organisasjon med å spare penger. Eksempler på cloud teknologier er som virtualisering, IAAS, PAAS, SAAS.

Virtualisering er en teknologi som har som formål å skape et virtuelt miljø som ved bruk av hypervisorer muliggjør det for å kjøre flere servere i en server. Hypervisorer sørger for at de virtuelle miljøene ikke forstyrrer hverandre og sørger for at hvert operativt system har tilgang på ressursene fra den fysiske hardwaren.

Det finnes ulike typer for virtualisering som for eksempel en OS virtualisering som tillater maskinen å kjøre flere operativsystemer samtidig ved hjelp av en programvare som VMware eller VirtualBox. Andre eksempler er applikasjons-virtualisering som gir brukeren til serverens applikasjon via internett. Dette gir brukere mulighet til å kjøre applikasjonen uten å laste den ned lokalt for at den skal kunne kjøres. Det finnes i tillegg noe som heter Desktop virtualisering. Denne lar brukere lage sin egen virtuelle skrivebord og aksessere og gir brukerne mulighet til å aksessere via en nettleser. Dette gir brukerne tilgang en virtuell arbeidsplass som gir økt fleksibilitet. (Bisht, 2022)

Videre har skyen en SAAS (Software As A Service) tjeneste, som er en teknologi som tilbys av en skyleverandør til brukere. SAAS er en ferdig applikasjon som oftest er satt sammen av IAAS og PAAS plattformer som brukere kan aksessere via en web-browser fra enheter som har internettilgang som mobiltelefoner og pc. Brukere eller organisasjoner som benytter seg av SAAS får tilgang til ressurser i applikasjonen tilbyr og må i tillegg betale for å benytte seg av denne løsning. Det kan være at forbrukeren benytter seg av en applikasjon for mailtjenester som Gmail, eller at de vil benytte seg av en provider som tilbyr applikasjoner for å skape eller redigere dokumenter som Microsofts Office produktene som Word, Powerpoint, Excel i skyen eksempler på SAAS applikasjoner i skyen. Brukere kan lage og lagre dokumentene direkte i skyen istedenfor at det gjøres lokalt på maskinen. Provideren har ansvaret for å vedlikeholde infrastrukturen som patching og oppdatere hvis nødvendig, imens brukeren har ansvaret for å sikre dataen som implementeres i skyen. (Bigcommerce, 2022)

PAAS (Platform As A Service) er en cloud teknologi operere som en plattform brukere kan benytte seg av for å utvikle applikasjoner eller webservere, men som også kan brukes til å teste og kjøre applikasjoner og programkoder. En forbruker kan implementere applikasjonen sin i skyen hvis ønskelig, men den må tilpasses for å kunne kjøre. Eksempler på leverandører som driver PAAS er Apache Stratos, Openshift og Heroku. (Bigcommerce, 2022)

PAAS tilbyr ressurser som bedrifter eller forbrukere trenger for utviklingen og krever at bruker betaler for ressursene med (Pay As You Go) for å benytte seg av PAAS plattformen. Dette gir brukeren mulighet å skalere opp eller ned på ressursene etter behov. Noen PAAS leverandør tilbyr kun ressurser for applikasjonsutvikling, imens andre kan tilby kunden infrastruktur og ressursene den trenger for applikasjonsutvikling. I likhet med SAAS kan brukere aksessere PAAS via en nettleser. Leverandøren eller provideren i PAAS er ansvarlig

for å håndtere den underliggende infrastrukturen, brukeren er kun ansvarlig for å for å sikre dataen og applikasjonen de utvikler eller implementerer i skyen.

IAAS (Infrastruktur As A Service) er en teknologi som tilbyr brukeren ressurser fra infrastrukturen som erstatter den lokale datasenter infrastrukturen. Ressurser som tilbys er innen nettverk, lagring og datahåndtering over internett. Eksempler på ressurser en bruker kan få tilgang til er blant annet servere, virtuelle maskiner og brannmurer. IAAS gir mulighet for brukeren å administrere nettverkstilgangen i skyen. Forbrukeren har i likhet med de andre teknologiene ikke et ansvar for å administrere den underliggende infrastrukturen. Og IAAS tar i bruk betaling for brukere eller kunder som benytter seg av de ressursene som tilbys med (Pay AS You Go), og kan når som helst skalere opp eller ned på ressursene etter behov. Eksempler på IAAS er Amazons AWS og Microsoft Azure. (Bigcommerce, 2022)

Risikoen organisasjonene står ovenfor er at hackere prøver å få uautoriserte tilgang til plattformen får å tilgang til sensitiv data og ressurser tilknyttet til organisasjonene. Hvis skyplattformen ikke benytter seg av riktig sikkerhetsmekanismer, kan dette medføre til økt risiko for datainnbrudd som kan gi store konsekvenser for bedriften selv. De mest populære skyplattformene er GCP, Azure og AWS. Sikkerhetsrisikoen er ulik for de tre skyplattformene siden de tilbyr ulike sikkerhetsmekanismer som multifaktorisering (to trinns faktorisering) som kan bidra med å sikre kundenes kontoer på plattformen mot brute force angrep. (James Arlen, Cloud Security Alliance's Security Guidance for Critical Areas Of Focus, 2021)

Andre sikkerhetsmekanismer skyplattformene kan ta i bruk er autorisering. Ved å implementere denne mekanismen vil dette kunne bidrar bedriften med å gi brukere kun tilgang til spesifikke tjenester på serveren som minimerer risikoen for datatap. Hvis dataen i skyen er ukryptert kan det øke risikoen for at dataen faller hos angriper. Dette inkluderer bedrifts data og kundedata. Ukryptert data er årsaken til at dataen faller hos angriper.

Kryptering er en metode som gjør dataen uleselig for angriperen. Det finnes ulike metoder for å kryptere dataen og skyplattformen kan benytte seg av krypteringsmetoder slik som Symmetrisk (bruker en privat fellesnøkkel som brukes til å dekryptere og kryptere dataen) og asymmetrisk (Bruker en private og public key for å kryptere og dekryptere dataen) RSA krypteringsmetodene. Noen krypteringsalgoritmer er designet for å gjøre krypteringen mer komplisert for hackere å knekke. For et selskap kan det være vanskelig å detektere sårbarhetene i applikasjonen. Leverandørene tilbyr verktøy som selskapet kan benytte seg av for sårbarhetsscanning. Jevnlig sårbarhetsscanning kan bidra med å detektere sårbarhetene i skyplattformen og videre minimere risikoen for cyberangrep. (Andrew Froehlich, 2021)

Oppgave A2:

Migrering til skyen hjelper selskapet med å blant annet spare penger. Anta at selskapet brukte on premise servere for lagring av data og selskapets ressurser, grunnet betaling for å vedlikeholde. On premise servere har en begrenset mengde med lagring, men når de flytter til skyen, har de ubegrenset plass og ressurser som kan hjelpe selskapet med å vokse raskt og gir dem fleksibiliteten til å skalere opp eller ned på ressursene sine basert på deres behov. I skyen betaler selskapet bare for infrastrukturen og ressursene de bruker .

Når en bedrift migrerer til skyen, velger de hovedsakelig mellom tre cloud typer: Public, private og hybrid sky. Hvilke typer de velger avhenger av hva de skal bruke skyen til. Public

skyen er en cloud teknologi som drives av selskaper som har til hensikt å levere tjenester / services som skal være offentlig tilgjengelig eller til en spesifikk organisasjon.

Selskapet driver med forretning innen utvikling av programvare moduler, (IOT noder code snippets) og GCP integrasjon. Public cloud velger selskapet dersom de øsker å selge applikasjonene eller kodene til kundene sine. For at de skal drive en forretning er det viktig at de gjør ressursene og applikasjonen sine offentlig tilgjengelig for kunder. De kan bruke public cloud for å motta henvendelser og ordre fra kunder. Skyen kan i tillegg brukes til betaling og lagring kundedata og annen bedriftsdata. Bedriften kan bruke public cloud til å gjøre produktene sine offentlig tilgjengelig som kan bidra kunden med å velge hvilke produkter de ønsker å kjøpe som kan være en fordel for den økonomiske veksten i selskapet. Denne skytypen kan bidra selskapet med å håndtere mange kunder og gi dem de etterspurte tjenestene de trenger.

Med hensyn til 100 ansatte, hvis selskapet benytter seg av public skyen har de et redusert ansvar for håndtering av den underliggende infrastrukturen som patching og oppdatere operativ systemet. Fordi provideren er ansvarlig for det meste i skyen inkludert ansvaret for kundene i bedriften og mye mer. I offentlig sky er ansvaret fordelt mellom leverandører og forbrukeren. Leverandøren har ansvaret for håndtering av den underliggende infrastrukturen, imens selskapet er ansvarlig for å sikre dataen, applikasjonene og alt annet av ressurser de implementerer i skyen. Når de migrere til public skyen må de velge mellom skytjenestene IAAS, PAAS eller SAAS.

En stor eller et medium selskap vil prioritere IAAS tilnærmingen dersom de ønsker å benytte seg av ressursene provideren tilbyr innen nettverk, lagring og databehandling. Større selskaper er villige til å betale for ekstra ressurser eller tjenester som overlater provideren mer ansvar som håndtering av database eller data. Og for å øke sikkerheten eller betale for en tjeneste som forbedrer backup av data. PAAS benyttes av selskaper som klarer å lage eller utvikle applikasjoner som klarer å kjøre eller at de tilpasse seg i skyen. Mindre bedrifter benytter seg av SAAS løsningen.

Dette er et selskap som driver som driver med utvikling, og i dette tilfelle vil det være gunstig å benytte seg av PAAS tilnærmingen. PAAS er en skyplattform som tilbyr alle ressursene en utvikler trenger for kode og programvare utvikling. Men PAAS bruker (Pay As You Go) betalingsmetoden som gir økt skalerbarhet og gir selskapet mulighet til å skalere opp eller ned i ressursene sine etter behov. I PAAS har selskapet ikke et ansvar for administrering av den underliggende infrastrukturen og har kun ansvar for å sikre data, applikasjoner og ressursene de migrerer til skyen. Selskapet har 100 ansatte på starten så de vil mest sannsynlig ikke bruke så mange ressurser for utvikling av produktene sine. Men etter hvert som de vokser med 4000 ansatte vil det være sannsynlig at de øker på ressursene.

En private sky er dedikert til en bruker eller en organisasjon. Selskapet benytter seg av private skyen for utvikling og har i tillegg on-prem servere. Det er flere årsaker til at selskapet benytter seg av denne typen. Det kan være fordi de øsker å ha full kontroll over infrastrukturen eller at de ikke ønsker at kildekoden til applikasjonene de utvikler offentliggjøres, og ønsker isolert tilgang til skytjenesten. En annen ting kan være at de ønsker å ha ressursene sine og konfidensiell data atskilt fra offentligheten. (James Arlen, Cloud Security Alliance's Security Guidance for Critical Areas Of Focus, 2021)

Ulempen med privat skyen er at selskapet har et ansvar for infrastrukturen og alt annet i systemet som patching av operativsystemet og vedlikehold av tjenestene og et sikkerhetsansvar og de må betale for de ressursene de trenger. Administreringen kan medføre et stort ansvar og stjele mye av tiden til bedriften som de heller kunne ha benyttet til å konsentrere seg med å håndtere business data og annet business relatert jobb. Å drive en private sky er mer kostbart fordi det koster å administrere infrastrukturen og ressursene i skyen. Det krever blant annet flere ansatte for at det skal kunne drives, bedriften må ha ansatte til å patche og konfigurere og administrere cloud infrastrukturen. Selskapet må investere mer penger for å vedlikeholde tjenestene og serverne sine. Med public sky tilnærmingen så ligger ansvaret fordelt mellom leverandøren og forbrukeren. Dette gjør at selskapet slipper å investere mye tid på vedlikehold som bidrar med å spare dem tid. Dette gjør at de kan konsentrere seg om å administrere forretningsdata og annet forretningsrelatert arbeid som kan være til fordel for forretningsvekst. Public cloud er en billigere tilnærming med tanke på at selskapet ikke trenger å investere mye penger på å vedlikeholde on prem serverne sine når de migrere til skyen, siden infrastrukturen er leverandørens ansvar.

Selskapet ser ut til å ha behov for både public og private skyen. I dette tilfelle så anbefales det at de benytter seg av hybrid sky. Hybrid skyer er et skymiljø som er kombinert av en private og en offentlig sky. Det kan også bestå av et eller flere private eller offentlige skyer. Med hybrid cloud har bedriften tilgang på ressurser i offentlige og private skyer, hybride skyer bidrar med økt sikkerhet. Bedriften kan ved bruk av hybrid sky velge om de vil lokalisere dataen i offentlig sky eller privat sky, eller begge.

Hybrid cloud gir bedriften mer fleksibilitet med arbeidsoppgavene sine i cloud. Hybrid består av som regel en public og en privat cloud. De kan bruke public for computingen og private for resten. Hvis en bedrift bruker private cloud for det meste av datahåndteringen kan de benytte seg av public som en backup lokasjon for lagring av data hvis de blir utsatt for overflow. Hybrid sky gjør det enklere for selskapet å administrere konfidensielle data . Public har et lavt nivå av sikkerhet,så i stedet for å lagre sensitive data i public. Kan selskapet lagre konfidensielle data i den private skyen, noe som gjør at selskapet kan gi begrenset tilgang til dataene som kan være en fordel når de vokser med 4000 ansatte. Dette hjelper selskapet fra uautorisert tilgang til data. Hvis selskapet utsettes for et angrep i public skyen , kan selskapet enkelt overføre data til den private skyen for å beskytte den. (James Arlen, Cloud Security Alliance's Security Guidance for Critical Areas Of Focus, 2021).

Public skyen kan selskapet benytte seg av til å utvikle applikasjoner ved bruk av ressursene PAAS tilbyr og deretter gjøre disse tilgjengelig for kjøp til kundene . Selskaper kan bruke public cloud til å redusere kostnadene, siden det er kostbart å drive en private skytype. Selskapet kan benytte seg av public skyen for lokalisering av data som sparer dem penger med tanke på at vedlikehold administreres av provideren, her trengs det ingen dedikerte eller kloke ansatte for vedlikehold som er en fordel som bidrar til sparing.

Hvis utviklerne mangler noen ressurser i private skyen kan de bruke public for utviklingen av programvare og IOT kode snippets. Dersom de ønsker at code snippets ikke skal være offentlig tilgjengelig kan det være en fordel å lagre dem i private skyen. Eller om de ønsker å utvikle en programvare i et isolert miljø velger de også private tilnærmingen. Hybrid skyen betaler man også for ressursene man har behov for akkurat som i offentlig sky. Sammenliknet med privat sky så er hybride skyer mindre komplekst og billige i tillegg. Med

denne sky typen sikrer selskapet at tjenesten og innholdet er tilgjengelig for kundene og samtidig bidrar det selskapet med å sikre konfidensielle data. Dette kan bidra til at bedriften vokser.

Oppgave A.2.2:

Hva slags angrep selskapet utsettes for avhenger av hvilken type sky de bruker. Nevnte i forrige oppgave at selskapet benytter seg av private sky for at utviklere skal kunne utføre arbeidsoppgavene sine. Og det ble anbefalt at selskapet bør benytte seg av hybrid tilnærmingen for sine forretningsfordeler.

Før utvidelsen har selskapet 100 ansatte. Med få ansatte i selskapet vil de stå i fare for å bli utsatt for cyber trusler som kan gi forretningen konsekvenser. Hvis selskapet benytter seg av hybrid skyen og ikke har implementerer riktige sikkerhetsprotokoller, kan dette øke risikoen for at de utsettes for angrep. Vi vet at hybrid skyen består av en public og en private sky. I public er det tre hovedleverandører som selskapet velger mellom. Eksempler er Google GCP, Microsoft Azure og Amazon AWS. Disse tre leverandørene leverer ulike mengder og typer av sikkerhetsprotokoller som kan bidra til økt sikkerhet i skyplattformen.

Feilkonfigurering i skyen kan medføre til at selskapet utsettes for angrep som datatap og gi angriperen uautorisert tilgang til serveren. Hvis selskapet for eksempel ikke konfigurerer databaseserveren i skyen ordentlig kan dette medføre til at konfidensiell data om bedriften og kundene blir offentlig tilgjengelig som videre medfører til en datalekkasje. Feilkonfigurering kan også gi angriperen full kontroll over systemet. Og hvis dette skjer kan dette forårsake til at kundene mister tilliten til å benytte seg av selskapets skytjeneste som kan medføre at selskapet mister kunder. Dette kan påvirke selskapets vekst og videre føre til et økonomisk tap.

Lock in er en trussel som selskapet kan utsettes for hvis de ikke velger den riktige skyleverandøren. Lock in er en metode leverandører benytter seg av for å forhindre forbrukere å bytte leverandør. Hvis selskapet ikke kan administrere sikkerheten på skyen kan dette gi en konsekvens for dem hvis leverandøren leverer dårlig sikkerhet. Dette kan videre medføre til at bedriften blir tvunget til å overføre til en annen leverandør som er bedre på sikkerhet som kan være kostbart dersom leverandøren benytter seg av Lock in metodene for å forhindre at det skjer. Hvis selskapet utsettes for Lock-in blir kan dette føre til at de blir sittende fast med en leverandør med dårlige sikkerhetsprotokoller. Dette vil utsette selskapet for sikkerhetsbrudd som gjør den sårbar som øker risikoen for angrep som DDOS og datatap. (Daniele Catteddu, 2009)

Styring:

Når bedriften migrere til skyen så håndterer provideren for det meste av sikkerheten i infrastrukturen. Dette kan blant annet påvirke sikkerheten, hvis for eksempel bedriften benytter seg av en skyplattform som ikke tilbyr nok sikkerhetskomponenter, kan dette medføre til at de utsettes for cyberangrep og data innbrudd som gjør at sensitive data og kunde opplysninger faller hos angriper. Sikkerheten i applikasjonen er bedre når bedriften tar ansvaret for sikkerheten fordi de kan selv implementere de sikkerhetsmekanismene som er nødvendig for å sikre alt av dataen de har implementert i skyen inklusivt data om kundene og ansatte som benytter seg av applikasjonen. (Daniele Catteddu, 2009)

Usikker API:

API (Application Program Interface) er en enkel måte å kommunisere med klienten på, og tillater brukere å tilpasse skytjenesteopplevelsene sine. Grensesnittet kan aksesseres av angriperen gjennom skytjenesten som ligger offentlig tilgjengelig. Hvis selskapet ikke har sikret grensesnittet sitt ordentlig i skyplattformen kan dette være en trusselfaktor og medføre til at hackere får uautorisert tilgang til selskapets ressurser og sensitive data om brukerne. Hvis selskapet blir berørt av en hacker angrep kan dette føre til at angriperen misbruker konfidensielle dataen til noe ondsinnet som å lekke det ut på nettet.

Etter utvidelsen er det antatt at selskapet vokser med 4000 ansatte. En bedrift med mange ansatte er ettertraktet blant hackere fordi selskapet har mye data som angripere kan misbruke til noe ondsinnet. (www.checkpoint.com, 2021)

DOS angrep:

Selskapet bruker skyen til å lagre store mengder av data og bruker skyen til å kjøre og utvikle applikasjonene sine. DOS angrep er når systemet mottar for mange forespørsler som overlapper nettverk. Hvis de utsettes for DOS (Denial Of Service) angrep kan utelukke brukere fra serveren eller forstyrre skytjenesten som kan i verste fall medføre til datatap. En angriper utfører et slikt angrep ofte rettet mot store selskaper og kan i noen tilfeller kreve penger fra selskapet dersom de ønsker å aksessere tjenesten. (Cruz, 2022)

Datatap:

Videre er datatap er også en også risikofaktor som kan gi kunden konsekvenser hvis angripere bryter seg inn i plattformen og stjeler sensitive data til kunden. De kan misbruke disse opplysningene til noe ondsinnet det kan være at de bruker disse opplysningene til å utføre uønskede transaksjoner. Hvis de finner kortopplysninger, kan vedkommende bruke dette til å utføre pengeoverføringer til seg selv. (security risks of cloud computing, 2021)

Malware angrep:

Selskaper kan i tillegg til DOS angrep også bli utsatt for malware angrep. Malware kan utsette skyplattformen i fare ved å infisere miljøet med skadelig kode som kan distrahere systemet eller ødelegge den. Angripere kan ved å legge inn lenker inn i skytjenesten spre malware. Dette kan resultere til at bedriften og kundene utsettes for å laste malware lokalt på maskinene sine utilsiktet, dette kan ødelegge maskinen og i verste fall forstyrre dem. Hvis skymiljøet utsettes for et malware angrep kan dette resultere til nedstenging av serveren. Hvis dette er en vedvarende situasjon vil bedriften på denne måten miste kunden som kan påvirke dem økonomisk og videre medføre til at alt av ressurser og konfidensiell data går tapt om dette problemet ikke fikses.

Phishing angrep:

For at angripere skal få tilgang til skytjenesten benytter de seg av phishing metoder for å kunne få autorisert tilgang til tjenesten. Phishing angrep er en metode angripere eller svindlere bruker for å manipulere brukere til å oppgi sensitiv informasjon om dem selv via SMS, telefonsamtaler eller epost. Det kan være at ansatte for eksempel blir manipulert til å oppgi brukernavnet og passordet til skytjenesten. Dette er en trussel for selskapet fordi det kan gi hackeren tilgang til sensitive data om kundedata og annet data i bedriften. Angriperen kan i verste fall bruke dette angrepet til å spre malware til andre de andre brukerne på

tjenesten. Angriperen som utfører et slikt angrep, kan over tid ta full kontroll over systemet og utføre ondsinnede handlinger som å utføre modifikasjoner i tjenesten. Dette kan medføre også stjeling av bankkort opplysninger.

Insider angrep:

Siden selskapet ikke har kontroll på den underliggende infrastrukturen i skyplattformen kan de ikke styre sikkerheten som gjør det vanskelig å detektere en insider angrep så lenge angriperen ikke utfører mistenkelige aktiviteter på tjenesten. Insider angrep gir en angriper autorisert tilgang til tjenesten og kan utføres av en ondsinnet aktør eller en ansatte som jobber der. Dette gir dem tilgang til selskapets ressurser og data og medfører til stjeling av sensitiv data og forretningshemmeligheter. (Cruz, 2022)

Oppgave A.2.3

Sikkerhetskontroller er et sett med kontrollere i skyen som skal bidra til å forhindre miljøet mot angrep og andre sårbarheter i skyens infrastruktur. Etter utvidelsen har selskapet råd til å leie eller kjøpe de beste sikkerhetskontrollene leverandørene tilbyr. For et selskap med mange ansatte kan det være en fordel å benytte seg av gode sikkerhetskontroller som kan beskytte applikasjonene, data og ressursene de implementerer i skyen.

IAM:

IAM er en sikkerhetskontroll som selskapet kan benytte seg av. IAM (Identity Access Management) kan selskapet bruke for å kontrollere hvem som har autorisasjon til dataen. Det kan de gjøre ved å administrere privilegiene til de ulike brukerne på tjenesten. Det er viktig at selskapet sørger for at det er ingen andre enn administrator har tilgang til bedriftsdata og sensitive ressurser. I tillegg kan de benytte seg av multifaktorisering autentisering som kan brukes for å sikre kontoer og API mot uautorisert tilgang til skyens data. (Sandra Gittlen, u.d.)

Monitorering:

Monitorering er en annen sikkerhetskontroll som selskapet kan bruke. Dette skal kunne bidra med å overvåke prosessene og brukeraktivitetene i applikasjonen. Hvis en angriper forsøker å bryte seg inn på en konto eller misbruker de rettighetene som ble utdelt, kan bedriften blokkere tilgangen til brukene hvis de oppdager mistenkelig aktivitet som gjør at angriperen mister rettigheter til å benytte seg av tjenesten. De kan i tillegg bruke monitorerings-vertøy for slette brukeren som kan minimere risikoen for at en angriper utfører ondsinnede handlinger på skyplattformen.

SIEM er et monitorerings-vertøy som selskapet kan benytte seg av. SIEM (Security Information Event Management) gir brukerne en full innsikt over organisasjonen informasjonssikkerhet. Den varsler om systemet blir utsatt for sikkerhetsbrudd eller sikkerhetshendelser. Mange SIEM systemer består av et dashbord som varsler alt av aktivitet i systemet som for eksempel sikkerhetsproblemer Dette vil kunne bidra til å sikre applikasjonen mot uautorisert tilgang og detektere insider angrep. I tillegg bidra til å detektere DOS og malware angrep.

Data recovery (Backup): Ved å implementere data recovery kan dette forhindre selskapet med at dataen går tapt i skyen. Det kan de gjøre ved å ta backup av dataen sin som kan være

til fordel hvis selskapets ansatte ved feil sletter data i skytjenesten. Hvis skyplattformen utsettes for et angrep og angriperen har sabotert hele miljøet kan backup være en nødløsning dersom selskapet ikke ønsker at dataen skal gå tapt. Hvis skytjenesten er serveren, er nede og selskapet trenger å aksessere data fortløpende kan det være også en fordel med backup løsninger. Backup kan forhindre selskapet med å miste dataene sine i skyen.

Sårbarhetshåndtering: Sårbarhetshåndtering kan være en fordel som kan hjelpe selskapet med å detektere sårbarheter i skytjenesten. Å finne sårbarheter i infrastrukturen kan være tungvint å utføre manuelt. For å detektere sårbarheter i skyen eller i applikasjonene selskapet utvikler kan de utføre en penetrasjonstesting av applikasjonen eller benytte seg av verktøy for deteksjon av sårbarheter. Selskapet kan benytte seg av sårbarhet verktøy leverandørene tilbyr som kan bidra til å detektere sårbarheter. Verktøyene kan rapportere selskapet dersom den trenger å patche, oppdatere eller om systemet har noen porter åpne. Dette kan bidra til å minimere DOS og malware angrep på skytjenesten.

Trening: Etter hvert som selskapet vokser kan risikoen for cyberangrep være en trusselfaktor dersom selskapet eller ansatte ikke opplæres til hvordan de skal opptre i skyen. Dette kan medføre til at ansatte utsettes for blant annet phishing angrep som kan føre til datainnbrudd og spredning av malware. Dette kan gi selskapet store konsekvenser og derfor er viktig at ansatte opplæres til å unngå phishing angrep når de benytter seg av skyplattformen. På grunn av mange ansatte krever det mye menneskelige ressurser for å kunne utføre opplæringen og selskapet må i tillegg investere penger på å opplære ansatte til fordi de ikke har den kunnskapen de trenger for opplæringen. De må leie inn dyktige mennesker som kan undervise ansatte og leie inn lokaler dersom de ikke har en selv. Videre må de kjøpe inn nødvendige utstyr og programmene som trengs for å utføre treningen. Og etter hvert som selskapet vokser så må de også investere penger på å trene opp nye ansatte, derfor kan kontinuerlig trening være en fordel for å styrke informasjonssikkerheten blant ansatte. Ansatte kan ved uhell sende sensitive opplysninger til feil mottaker eller benytte seg av svakt passord. Treningen vil hjelpe ansatte med å styrke bevisstheten og informasjonssikkerheten sin på skytjenesten. Når informasjonssikkerheten styrkes blant ansatte, minker risikoen for at selskapet utsettes for phishing angrep, malware, datainnbrudd og angripere får uautorisert tilgang. Kontinuerlig treningsprogram for ansatte er en dyr implementasjon siden det krever at selskapet må investere mye penger for at det skal utføres. (Spencer, 2021)

Task A.2.4:

Selv etter utvidelsen antas det at selskapet ha behov for private skyen. Som nevnt tidligere kan det være en fordel å benytte seg av private skyen for lagring av konfidensiell data. Hvis selskapet utsettes for datainnbrudd kan det være en stor ulempe hvis de har implementert alt av data og ressurser i public cloud. Private cloud har et bedre sikkerhetsnivå og selskapet kan ved å implementere sikkerhetskontroller som autorisering, gi datatilgang til ansatte som har autorisasjon til det bidrar med å sikre konfidensiell data. Private cloud kan være en bra for selskapet og nå som de har vokst med 4000 ansatte, så har nok penger til å benytte seg av den private skyen. Hvis de ønsker å utvikle applikasjonene sine i et isolert miljø og ikke ønsker å lagre sensitive kildekoder i skyen kan det være en fordel å ha private sky. Dette er årsaken til at selskapet kan ha et behov for private skyen.

A.4 (GCP activities):

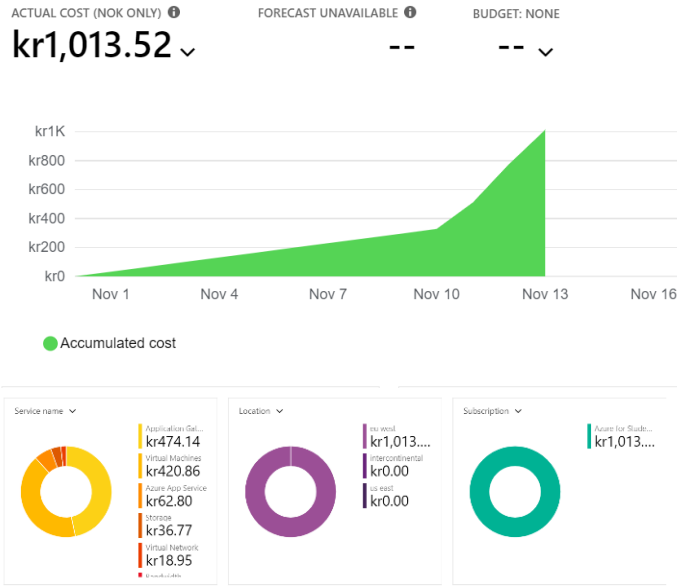
Activity	Type	Date started	Date finished	Score	Passed
Cloud Network Security with Cloud IDS and VM-Series	Lab	8 days ago	8 days ago	100.0/100.0	✓
Networking 101	Lab	8 days ago	8 days ago	100.0/100.0	✓
Build a Serverless App with Cloud Run that Creates PDF Files	Lab	8 days ago	8 days ago	100.0/100.0	✓
Service Accounts and Roles: Fundamentals	Lab	Oct 31, 2022	Oct 31, 2022	100.0/100.0	✓
Kubernetes Engine: Qwik Start	Lab	Oct 31, 2022	Oct 31, 2022	100.0/100.0	✓
Setting up a Private Kubernetes Cluster	Lab	Oct 31, 2022	Oct 31, 2022	100.0/100.0	✓
Ensure Access & Identity in Google Cloud: Challenge Lab	Lab	Oct 21, 2022	Oct 21, 2022	100.0/100.0	✓
Setting up a Private Kubernetes Cluster	Lab	Oct 21, 2022	Oct 21, 2022	0.0/100.0	
Setting up a Private Kubernetes Cluster	Lab	Oct 21, 2022	Oct 21, 2022	70.0/100.0	
User Authentication: Identity-Aware Proxy	Lab	Oct 14, 2022	Oct 14, 2022	100.0/100.0	✓
VPC Network Peering	Lab	Oct 14, 2022	Oct 14, 2022	100.0/100.0	✓
VPC Network Peering	Lab	Oct 14, 2022	Oct 14, 2022	38.0/100.0	
Getting Started with Cloud KMS	Lab	Oct 7, 2022	Oct 7, 2022	100.0/100.0	✓
User Authentication: Identity-Aware Proxy	Lab	Oct 7, 2022	Oct 7, 2022	100.0/100.0	✓
Service Accounts and Roles: Fundamentals	Lab	Oct 7, 2022	Oct 7, 2022	60.0/100.0	
Google Apps Script: Access Google Sheets, Maps & Gmail in 4 Lines of Code	Lab	Oct 7, 2022	Oct 7, 2022	100.0/100.0	✓
Introduction to APIs in Google	Lab	Oct 7, 2022	Oct 7, 2022	100.0/100.0	✓
IAM Custom Roles	Lab	Sep 30, 2022	Sep 30, 2022	100.0/100.0	✓
Cloud IAM: Qwik Start	Lab	Sep 30, 2022	Sep 30, 2022	100.0/100.0	✓
Set Up Network and HTTP Load Balancers	Lab	Sep 23, 2022	Sep 23, 2022	100.0/100.0	✓
Kubernetes Engine: Qwik Start	Lab	Sep 23, 2022	Sep 23, 2022	100.0/100.0	✓
Kubernetes Engine: Qwik Start	Lab	Sep 23, 2022	Sep 23, 2022	0.0/100.0	
Getting Started with Cloud Shell and gcloud	Lab	Sep 23, 2022	Sep 23, 2022	100.0/100.0	✓
Introduction to Docker	Lab	Sep 16, 2022	Sep 16, 2022	100.0/100.0	✓
Compute Engine: Qwik Start - Windows	Lab	Sep 9, 2022	Sep 9, 2022	100.0/100.0	✓

1 - 25 of 27

Activity	Type	Date started	Date finished	Score	Passed
Creating a Virtual Machine	Lab	Sep 2, 2022	Sep 2, 2022	100.0/100.0	✓
A Tour of Google Cloud Hands-on Labs	Lab	Sep 2, 2022	Sep 2, 2022	100.0/100.0	✓

26 - 27 of 27

A.3 (Azure Cost Analysis):



(Hele B oppgaven ble utført i Ubuntu VM-en)

Oppgave B.1

Vedlegg 1 (Ubuntu er lastet ned på VirtualBox)

B.2 a)

```
usah002@usah002-VirtualBox:~$ cat /proc/cpuinfo
processor       : 0
vendor_id       : GenuineIntel
cpu family      : 6
model           : 140
model name      : 11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz
stepping        : 1
cpu MHz         : 2419.196
cache size      : 8192 KB
physical id     : 0
siblings        : 2
core id         : 0
cpu cores       : 2
apicid          : 0
initial apicid  : 0
fpu             : yes
fpu_exception   : yes
cpuid level     : 22
wp              : yes
flags           : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse
 nonstop_tsc cpuid tsc_known_freq pni pclmulqdq ssse3 cx16 pcid sse4_1 sse4_2 x2apic movbe popcnt aes xsave avx
ase avx2 invpcid rdseed clflushopt md_clear flush_l1d arch_capabilities
bugs            : spectre_v1 spectre_v2 spec_store_bypass swapgs
bogomips        : 4838.39
```

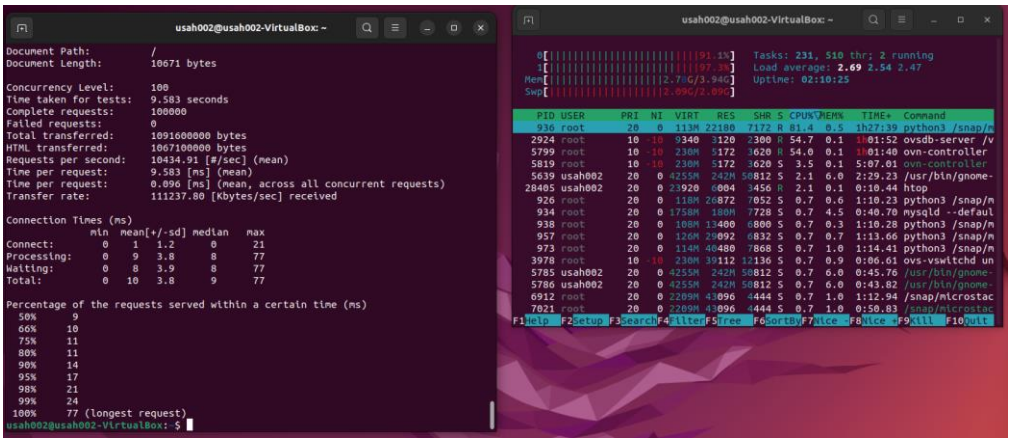
(Vedlegg 2 : bruker kommandoen «cat /proc/cpuinfo» og finner (cpu cores) antall CPU-er =2 på ubuntu og bogomips = 4838.39)

```
usah002@usah002-VirtualBox:~$ nmap localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-18 11:35 CET
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000073s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
80/tcp    open  http
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
631/tcp   open  ipp
3306/tcp  open  mysql
5000/tcp  open  upnp
10002/tcp open  documentum
```

B.2 b)

(Vedlegg 3: Laster ned nmap med kommandoen «sudo apt install nmap» og deretter kjører jeg «nmap localhost» og finner åpne porter»)

Oppgave B.3



(Vedlegg4: Laster ned nginx med kommandoen «sudo apt install nginx» og Etter å ha kjørt kommandoen «ab -n 100000 -c 100 localhost/» på den ene terminalen og utfører benchmark. Får opp den høyeste CPU loads med kommandoen «htop» som er 81.4 % maks grensen er 100% CPU load. htop ble lastet ned med kommandoen «sudo apt install htop».

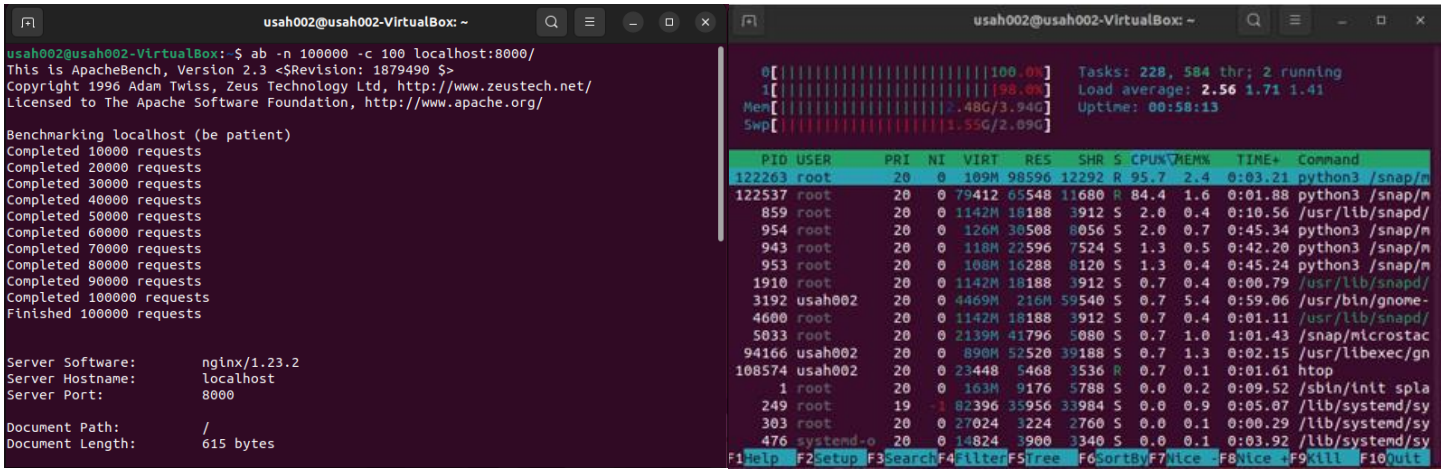
Oppgave B.4

(Vedlegg 5: Laster ned docker.io «sudo apt-get install docker.io»)

```
usah002@usah002-VirtualBox:~$ sudo apt-get install docker.io
[sudo] passord for usah002:
Leser pakkelister ... Ferdig
Skaper oversikt over avhengighetsforhold ... Ferdig
Leser tilstandsinformasjon ... Ferdig
Du har allerede nyeste versjon av docker.io (20.10.12-0ubuntu4).
Følgende pakker ble automatisk installert og er ikke lenger påkrevet:
  libpython2-stdlib libpython2.7-minimal libpython2.7-stdlib
  python-pkg-resources python-setuptools python2 python2-minimal python2.7
  python2.7-minimal
Bruk «sudo apt autoremove» for å fjerne dem.
0 oppgraderte, 0 nylig installerte, 0 å fjerne og 139 ikke oppgradert.
```

```
usah002@usah002-VirtualBox:~$ sudo docker run -d -p 8000:80 nginx
[sudo] passord for usah002:
a9e187a2d63698fd9d2f94259b42aa262c3bb87c63270ff9a3799fc285e3d256
usah002@usah002-VirtualBox:~$ sudo docker ps
CONTAINER ID   IMAGE     COMMAND                  CREATED          STATUS
   PORTS                                   NAMES
a9e187a2d636   nginx     "/docker-entrypoint.…"   26 seconds ago   Up 26 seconds
   0.0.0.0:8000->80/tcp, :::8000->80/tcp   pedantic_blackburn
```

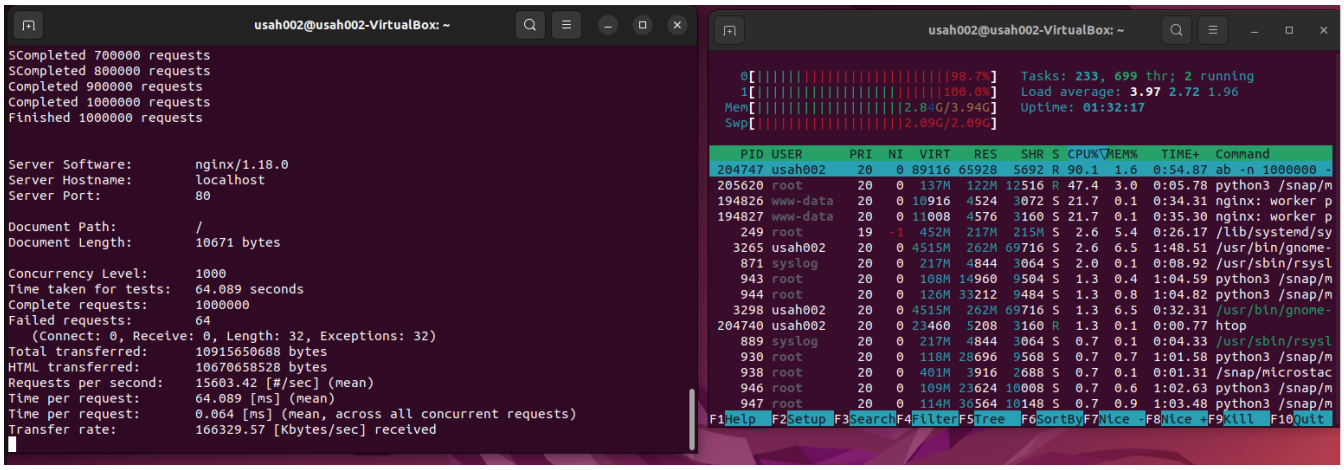
(Vedlegg 6: Starter nginx i docker med kommandoen: «sudo docker run -d -p 80 nginx»)



(Vedlegg 7: Sammenliknet med resultatene fra forrige oppgave er system load mye høyere her når vi kjører eksperimentet mot nginx i docker.)

Oppgave B.5

(Vedlegg 8: Kjører kommandoen : «ab -n 1000000 -c 1000 localhost/» mot serveren og får følgende resultat:)



Bibliografi

Andrew Froehlich, S. S. (2021, 02). *Tech Target*. Hentet fra cloud security : https://www.techtarget.com/searchsecurity/definition/cloud-security

Bigcommerce. (2022). Hentet fra SaaS vs. PaaS vs. IaaS: What You Need to Know: https://www.bigcommerce.com/articles/ecommerce/saas-vs-paas-vs-iaas/#the-3-types-of-cloud-computing-service-models-explained

Bisht, N. (2022, June). *GeeksforGeeks*. Hentet fra Virtualization in Cloud and Types: https://www.geeksforgeeks.org/virtualization-cloud-computing-types/

Cruz, S. (2022, June 15). *horangi.com*. Hentet fra cloud computing security threats to watch for: https://www.horangi.com/blog/7-cloud-computing-security-threats-to-watch-for

Daniele Catteddu, G. H. (2009). *Benefits, risks and recommendations for information security.* Athens: The European Network and Information Security Agency (ENISA) .

James Arlen, R. M. (2021). I R. M. James Arlen, *Cloud Security Alliance's Security Guidance for Critical Areas Of Focus* (ss. 131-132). Washington D.C : Cloud Security Alliance .

James Arlen, R. M. (2021). I R. M. James Arlen, *Cloud Security Alliance's Security Guidance for Critical Areas Of Focus* (s. 32). Washington D.C: Cloud Security Alliance.

James Arlen, R. M. (2021). I R. M. James Arlen, *Cloud Security Alliance's Security Guidance for Critical Areas Of Focus* (ss. 31-32). Washington D.C: Cloud Security Alliance.

paloaltonetworks. (2022). Hentet fra What is a denial of service attack (DoS): https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos#:~:text=A%20Denial%2Dof%2DService%20(,information%20that%20triggers%20a%20crash.

Sandra Gittlen, L. R. (u.d.). *Techtarget*. Hentet fra identity access management IAM system: https://www.techtarget.com/searchsecurity/definition/identity-access-management-IAM-system

security risks of cloud computing. (2021). Hentet fra https://www.javatpoint.com/security-risks-of-cloud-computing

Spencer, A. (2021, December 07). *What's the cost of training employees*. Hentet fra bizlibrary: https://www.bizlibrary.com/blog/training-programs/cost-of-training-employees/

www.checkpoint.com. (2021). Hentet fra Top 15 Cloud Security Issues, Threats and Concerns : https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/