FAKULTET FOR INFORMASJONSTEKNOLOGI OG ELEKTROTEKNIKK

INFT2504 SKYTJENESTER SOM ARBEIDSFLATE

20.09

Forfatter
Elias Rudsbråten

Innholdsfortegnelse

1 Oppgave 1 - Teoretisk perspektiv (50%) 1

1.1 Skybaserte Utrullings- og Tjenestemodeller 1

1.2 Evolusjonen av 'as-a-Service' Konsepter 2

1.3 Onboarding-prosess i Bedrifter 3

1.3.1 Lag en bruker 3

1.3.2 Passord 3

1.3.3 Roller 4

1.3.4 Grupper 4

2 Diskusjon og refleksjon 5

2.1 Teoretisk 5

2.1.1 Passord og MFA 5

2.1.2 Brukers rettigheter 5

2.2 Praktisk 5

2.3 Min følelse 6

Referanser 7

1 Oppgave 1 - Teoretisk perspektiv (50%)

1.1 Skybaserte Utrullings- og Tjenestemodeller

Problemstilling: Forståelsen av skyarkitekturer inkluderer flere utrullingsmodeller og tjenestemodeller. Kan du identifisere og differensiere mellom utrullingsmodellene som ofte benyttes i skyen? Videre, hva er de underliggende fordelene og potensielle begrensningene ved å velge en utrullingsmodell over en annen?

Offentlig sky er en av de tre utrullingsmodellene som er tilbudt av tredjepartsleverandører og gir alle muligheten til å bruke produktet. Produktet kan være gratis eller solgt ved etterspørsel, som Skystark hvor de tilbyr å leie RTX 4090 grafikk kort fra deres servere dersom du skulle ønske å spille Cyberpunk på ultra innstillinger. Når man er ferdig kan man enkelt avsluttet abonnementet, og dette viser til den skalerbare og kostnadseffektive delen av modellen.

Selvom man ikke eier og har full kontroll over infrastrukturen/eiendelen så slipper man de negative delene. Siden du distribuerer kostnadene for ressursene med flere kunder blir de større utgiftene mindre. Skulle noe gå ned er det ikke lengre du som må betale for reparasjonen, men tjenestetilbyderen som står med alt ansvaret.

For særegne bedrifter som må opprettholde en viss standard eller regelverk når det kommer til sikkerhet er offentlig sky ikke lengre en mulighet. Det er her privat sky er enn bedre løsning for kunden.

Privat sky, imotsetning til en offentlig sky, er dedikert til én enkelt organisasjon hvor alle ressursene i skyen er kun tilgjengelig til bedriften som styrer den. Dette pålegger bedriften å ha fult ansvar for infrastrukturen og kostnaden det tar å bygge den, men også vedlikeholdet det kreves dersom feil skulle oppstå. Ved en slik løsning bytter man kostnadeffektivitet og lav vedlikeholdskrav mot bedre kontroll over sine systemer og sikkerhetenheten man implementerer.

Vi må også nevne tidsbruket og ressursene som kreves for å bygge en slik privat sky. Før man kan flytte over alt opp til skyen vil bedriften måtte kunne sikre seg ved å implementere sikkerhetsregler og et robust miljø hvor de ansatte skal jobbe. En slik oppgave krever oftest at man leier inn konsulenter for å forsikre at oppsettet er oppimot ”best-practise”, noe som kan være svært kostbart, spesielt med opprettholdelse av infrastrukturen vil dette øke budsjettet.

Hybrid sky slår sammen de to konseptene vi nå har snakket om for å øke fleksibiliteten og redusere kostnadene. Ved denne løsningen kan vi plassere sikkerhetssensitive data i en privat sky og andre tjenester eller data i en den lokale. Slik senker vi kostnaden for den private delen ettersom det ikke kreves like stor infrastruktur, og fleksibilitet øker ved å flytte data mellom de to strukturene.

Men en slik smart løsning kommer med negative konsekvenser. Det kan være vanskelig å holde orden på hva som er innholdssenstivt av data, og vite hvor den er lokalisert og i hvilke sky den skal plasseres. Det er derfor viktig å lage en forstårlig struktur tidlig i starten av implementeringen.

1.2 Evolusjonen av 'as-a-Service' Konsepter

Problemstilling: Den teknologiske landskapet har utvidet seg til å inkludere "as-a-Service" paradigmet, spesielt gjennom Anything-as-a-Service (XaaS). Hvordan har denne utviklingen endret måten tjenester leveres på til bedrifter? Diskuter rollen til IaaS, PaaS og SaaS i denne konteksten og gi eksempler på scenarier der én tjenestemodell ville være mer hensiktsmessig enn de andre.

Enhver bedrift har sitt eget behov ettersom hva det er de produserer eller tilbyr. Anything-as-a-Service har gjort det enklere for bedrifter å kunne velge de ressursene og tjenestene som de krever som en tjeneste gjennom skyen.

For en organisasjon som har et robust IT-personal og hvor det kreves tilgjengelighet til maskinvaren, vil infrastructure as a service være en god investering. Tjenesteforsørgeren vil være ansvarlig for selve utstyret og kunden for den daglige driften, men det er også mulig å finne en leverandør som håndterer driftingen også. Har man en som driver med reverseengineering og malware analyse vil det være kritisk å endre på operativsystemene og ha virtuelle maskiner tilgjengelig, og IaaS vil da være en god løsning.

PaaS tilbyr operativsystem og mange av de nødvendige verktøyene for å bygge og distributere sitt produkt. For andre bedrifter er det ikke viktig å vite hva som kjører på datamaskinen deres, så lenge de har verktøyene til å gjøre jobben sin. Dette kan være programmere som vil enkelt deployere en app eller teste redundansen for en nettside.

Software as a service er med på å gi brukeren lettest tilgang til tjenesten de har lyst til å bruke. Det er ingenting som trengs å laste ned eller konfigureres, så lenge man har internett og eventuelt betaler for tjenesten har man tilgang. Overleaf som jeg bruker til å skrive denne oppgaven eller Zoom for å se på forelesning tilbyr SaaS til meg som jeg bruker uten å måtte tenke på noen form for infrastruktur.

1.3 Onboarding-prosess i Bedrifter

Problemstilling: Ansatte i en organisasjon går gjennom en rekke trinn fra de starter til de slutter. Beskriv prosedyrene som er knyttet til onboarding av nyansatte, med fokus på gruppetilhørighet, MFA og passordoppsett. Du kan supplere med et flytdiagram for å visualisere prosessen og ansvarlige for hvert trinn.

1.3.1 Lag en bruker

Når den ansatte skal få tildelt bruker i azure AD miljøet er det en rekke steg som må utføres før brukeren kan ta i bruk tjenestene som følger med.

I admin senteret velger man å opprette en ny bruker hvor man skriver inn den nye ansatte sin standard informasjon.

- Fullt navn
- Navn som skal vises i Azure-AD
- Og brukernavn samt domene.

1.3.2 Passord

Her får man også muligheten til å automatisk opprette ett passord, så lenge riktig policyer for passordkrav er satt kan dette muliggjøres.

For passordkrav er det vanlig å tro at man skal kreve avanserte passord ved bruk av !"%/()*-" og passordlengde på 16-20. Dette er best-practise for enkelt mennesket, men vi må ta i betraktning at mennesker er late og har ikke alltid sikkerhet som første prioritet. Jeg velger å følge microsoft sin passord guideline for administratorer.

- Maintain an 8-character minimum length requirement
- Don't require character composition requirements. For example, *&(^%$
- Don't require mandatory periodic password resets for user accounts
- Ban common passwords, to keep the most vulnerable passwords out of your system
- Educate your users to not reuse their organization passwords for non-work related purposes
- Enforce registration for multi-factor authentication
- Enable risk based multi-factor authentication challenges

Figure 1: Password guideline

Videre ønsker vi at den ansatte skal få et engangs passord ved første innlogging. Når brukeren logger seg inn vil de ble tvunget til å bytte passord ved hjelp av MFA noe vi har administrert i brukerens passordprofil. Det er ikke ønsket at de får tilsendt passord til email dersom brukeren sin email konto har blitt kompromittert og trusselaktør har tilgang til passordet kan dette ha store konsekvenser for bedriften.

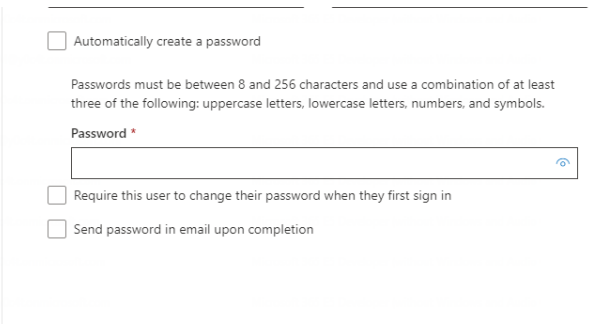

Figure 2: Password settings.

Skulle brukeren ha glemt passord er det viktig at man har lagt til mobiltelefon nummer på brukeren slik at man aktivere "self-service password reset" gjennom **MFA**. Brukeren kan da logge seg inn på mail, få en engangskode på sms og sette eget passord. Viktig da at krav til passordet er satt av IT-administrator på forhånd. Ved denne framgangsmåten unngår vi å sende passord ukryptert data over epost. Det er god praksis å gi password reset for grupper hvor det ikke er sensitiv data, og heller la administratorer måtte ha flere steg for passord tilbakestilling.

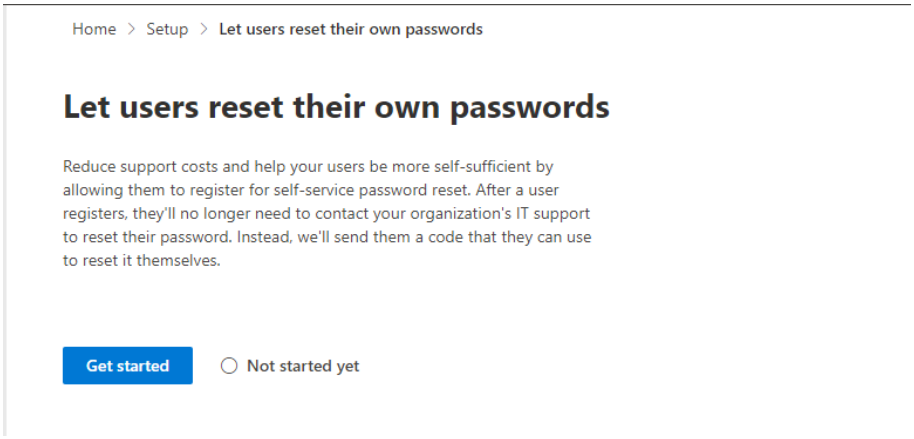

Figure 3: Enabling users to reset their own password.

1.3.3 Roller

For en ny ansatt vil man tildele en rolle som reflekterer arbeidet de skal gjøre for bedriften. Dette er en vurdering man må velge med sikkerhet slik at de får rettigheten som de trenger for å utføre arbeidet sitt, men som heller ikke gir de tilgang til ressurser som kan være skadelig for sikkerheten i bedriften.

1.3.4 Grupper

I en bedrift med mange ansatte er det viktig å kunne tildele de spesifikke gruppene med regelsett og ressurser som kun er nødvendig for oppgavene de har. Dette sparer tid ved at vi slipper å konfigurere hver enkelt og øker sikkerheten og oversikt når alle brukere innen én gruppe har de samme rettighetene.

Ved tildeling av gruppe må den ansatte få enten en sikkerhet- eller Microsoft 365 gruppe. For de fleste ansatte vil M365-gruppe være det riktige valg.

- Sikkerhetsgruppe: Den ansatte trenger nettverks- og tilgangkontroll. F.eks: IT-administrator.
- M365-gruppe: Den ansatte trenger kun tilgang til kommunikasjonsverktøy som Onedrive eller Microsoft Teams. F.eks: Systemutvikler/HR.

Videre må gruppen ha informasjon som:

- **Navn**, hvor det gjerne reflekterer gruppens bakgrunn.
- **Beskrivelse**, hvor man utdyper hva gruppen er ment for.
- **Medlems type**
  - **Tildelt medlemskap** hvor admin plasserer den ansatte i en gruppe (lite effektivt).
  - **Dynamisk** hvor ansatte legges automatisk med i gruppen basert på nøkkelord som ”developer”.

Basert på hva den nye ansatte har som oppgave for bedriften vil man kunne enkelt automatisere tildelingen av grupper. En oversiktlig AD øker sikkerheten i AD, og sparer administratorer for mye arbeid.

2 Diskusjon og refleksjon

2.1 Teoretisk

2.1.1 Passord og MFA

Med henhold til sikkerhet er MFA kritisk for å opprett holde en sikker AD, men føler at passord burde ha en høyere standard enn det Microsoft selv mener. Personlig ville jeg ha funnet en løsning for alle ansatte å bruke en passordbehandling tjeneste som Bitwarden eller 1Password slik at man kan øke passord krav uten at det blir et problem for de ansatte.

Selvom MFA er en av de viktigste sikkerhetsmekanisme man kan implementere, er det fortsatt viktig å poengtere at trusselaktører kan omgå det. Det kan være hensiktsmessig å implementere policies rundt dette ved å bestemme hvor og når MFA tokens skal være gyldige.

2.1.2 Brukers rettigheter

For å forsikre nettverket er det viktig å minimisere hva ansatte kan ta i bruk på bedriftens nettverk/maskiner. Dette vil å bannlyse visse nettsider eller tjenester som; personlig email og sosiale medier (mulig mer nettverks enn infrastruktur relatert).

2.2 Praktisk

Implementasjoner jeg kunne tenkt å hatt med:

- Roller for brukere
- Opprettet en kontinuerlig logging av alle brukere
- Key vault for passord

Hva jeg kunne ha gjort bedre:

- For å lage brukere ville jeg ha lagret dataen og brukt dem som objekter med å lage et hash table.
- En mer definert password policy med krav til flere tegn og variasjon.
- Laget en mer fleksibel lisensierings funksjon
- Lagt til flere feil sjekker i koden

2.3 Min følelse

Jeg hoppet litt fram og tilbake med teoretisk og praktisk jobbing. Jeg slet først litt med å skrive 1.3 oppgaven og følte det var godt å jobbe med litt praktisk, men dette funket ganske greit. Deretter skulle jeg gjort det litt mer klart over forklaringene mine i 1.1 og 1.2, men jeg følte at det var viktig å begrunne hva de forskjellige løsningene fører til.

Referanser

(2023). URL: ssa-ls03_AzureAD-M365.
(2023). URL: ssa-ls01_Introduksjon%20til%20sky.
(2023). URL: ssa-ls02-Kjernefunksjoner%20i%20M365.
Overview of Microsoft Graph (2023). URL: https://learn.microsoft.com/en-us/graph/overview.