FAKULTET FOR INFORMASJONSTEKNOLOGI OG ELEKTROTEKNIKK

INFT2504 SKYTJENESTER SOM ARBEIDSFLATE

29.10.2023

Forfatter
Elias Rudsbråten

Innhold

1 Oppgave 1 – Caseoppgave - Teori (70 %)

1.1 Oppgavetekst

Bedriften CyberDyne Systemes skal starte sin skyreise ved å starte med Microsoft 365. De ansatte skal naturligvis ha sine egne private adresser. Bedriften består av følgende avdelinger: - HR – for demoformål: 2 ansatte - IT – for demoformål: 2 ansatte - Developer – for demoformål: 2 ansatte

Bedriften skal ha en felles gruppe for hver av avdelingene med Teams-rom SharePoint site, samt en felles gruppe for alle ansatte. Alle i bedriften skal kunne booke følgende møterom: - Tank - Genisys

Som alltid er det viktig å tenke sikkerhet, både om en er on-prem og i sky. Ta stilling til hvilke sikkerhetstiltak, som et minimum, som bør vurderes/implementeres for bedriften i M365. Vis gjerne med noen print screen der det er hensiktsmessig og gir merverdi til besvarelsen

1.2 Problemstilling:

For at CyberDyne systems skal oppnå en høy standard for sin sikkerhet vil vi starte med de viktigste og mest standard tiltakene først. Vi må tenke på de forskjellige trusselen som står ovenfor M365 miljøet deres som phising, ransomware og man-in-the-middle angrep, og deretter jobbe får i minimere risikoen for at de skal inntreffe.

1.3 Besvarelse

Bruk av robuste sikkerhetstiltak i Microsoft 365 kan være avgjørende for at en bedrifts data skal være sikker og at ingen konfidensiell informasjon skal lekkes til det offentlige. Oppgaven vil sette fokus på de grunnleggende sikkerhetstiltakene som CyberDyne Systems bør implementere i sin skyløsning.

Sikkerhet i M365

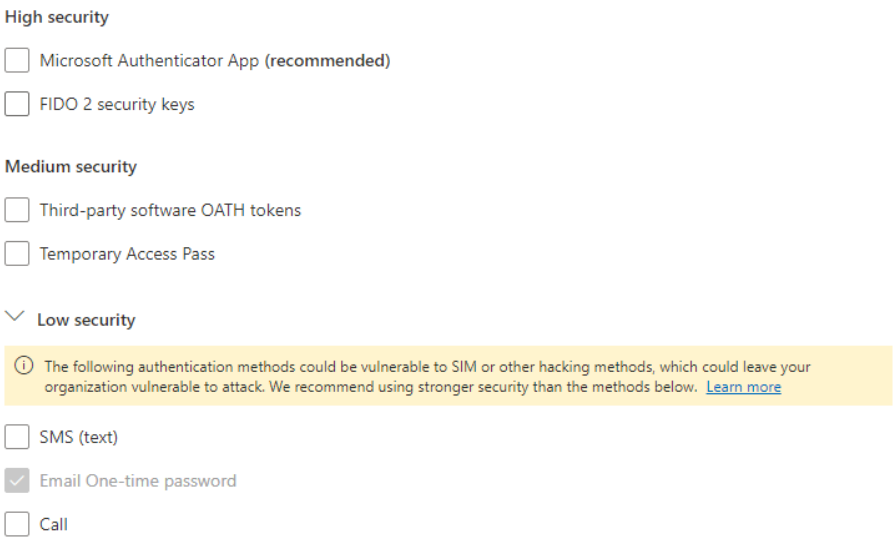
1.3.1 Passord

For enhver bedrift er gode passord vaner noe av det viktigste en kan implementere for å unngå trusselaktører i å komprimere bedriften deres. Førstegangs passord vil bli laget av administrator og deretter la brukeren lage eget passord med MFA etter første innlogging. Her er noen gode vaner som er anbefalt av Microsoft hvor vi tar menneskers latskap inn som en variabel; (**MSpassord**)

- Passord krav for brukere som ikke har admin rettigheter.
  - Minimum 8 tegn, mer enn dette kan demotivere ansatte i å lage avanserte passord.
  - Ikke tving ansatte til å bruke tegn som !"¤%/(, selvom jeg personlig mener at det burde. Legge til et ekstra tegn er ikke vanskelig å huske
  - Ikke ha automatisk passord reset da dette gjør passordene mindre oppfinsomme over tid.
  - Bannlys ofte brukte passord, rockyou.txt er en god start. (*Eliminate bad passwords using Microsoft Entra Password Protection* udatert)
  - Bruk en password manager! Dette gjør det lettere for ansatte å huske sine passord og gjør det lettere å ha forskjellige passord på flere tjenester.
  - La brukerne endre sine egne passord. Vi vil ikke at passord skal sendes over ukrypterte medier.

1.3.2 MFA

Multifaktor autentisering, eller MFA, er også et av de viktigste sikkerhetstiltakene man kan implementere. Det fungerer ved at ansatte først skriver inn passordet sitt og deretter autentisere seg ved en av disse mulighetene;



Figur 1: MFA options

Legg merke til at metodene for MFA er rangert etter hvor sikkere de er. Microsoft Auth App er noe jeg personlig bruker når det er en rask og sikker måte for å autentisere seg. I tillegg er det gratis og lite arbeid for bedriften å implementere.

For administratorer kan man bruke verktøy som bruker FIDO 2 security keys for nøkkelbasert autentisering som minsker risikoen for man-in-the-middle angrep. Et godt produkt er YubiKey 5 Series, men kjøp av dette kan ta tid å sette opp og vil **koste** bedriften betraktelig mer når de skal bestille produktet.

1.3.3 Principle of least privilege

Det er en rekke sikkerhetsfeil som kan oppstå skulle ansatte ha tilgang til ressurser som ikke er nødvendig. Spesielt er det farlig for organisasjonen dersom en trusselaktør har tilgang til en konto med eskalerte privileger. Derfor vil vi tildele kun de nødvendige ressursnivåene som er nødvendig for at ansatte skal kunne gjøre jobben sin.

Hver ansatt vil være tildelt en spesifikk gruppe som igjen har de spesifiserte tilgangene som trengs. Eksempler på dette er;

- **Begrenset tilgang til data.** OneDrive, kode, andre miljøer.
- **Tidsbegrenset tilgang til ressurser.** Ansatte vil kun ha tilgang i et gitt tidsrom.
- Personell- og finansiell informasjon.
- Administrative rettigheter i ulike miljøer.

1.3.4 Sikkerhetstiltak for apper i M365

For apper som SharePoint, OneDrive og Teams er det viktig å definere hvilken adgang ansatte i og utenfor organisasjonen har. Dette vil si å implementere **conditional access** (*What is Conditional Access?* Udatert).

Bruksområder Med Microsoft Entra Conditional Access kan bedriften implementere automatiske aksesskontrollbeslutninger for å få tilgang til sine skyapper basert på gitte betingelser. Dette vil være en sentral del av CyberDune systems sin rolle for å opprettholde sikkerheten for store deler av sitt M365-miljø.

I en bedrift med mange ansatte er det viktig å holde orden på hvem som har hvilke rettigheter, og her kommer gruppering inn i spill. Her en liste på flere metoder å gjøre dette på.

- **Grupper (og enkelt brukere**; Spesifikk tilgang til enkelt grupper.
- **IP lokasjon**; IP-adresser som bedriften har laget er det eneste som får tilgang.
- **Enhet**; Kun bedriftens enheter får tilgang.
- **Applikasjon**; Bruk av applikasjoner kun til de som har fått tilgang.

Vi kan nå velge betingelser for at en ansatt skal ha tilgang til en tjeneste. Dette kan være alt fra bruk av MFA for å bruke OneDrive eller endring av passord ved første innlogging av en applikasjon. Det er stort bruksområde for bruken av conditional access men det er viktig at man ikke kaster policier overalt. Sakte men sikkert testing og implementering er kritisk for å unngå fremtidge problemer.

Sterke- og svake sider

Positivt

- **Forbedret sikkerhet, treffer alle punkter innen Zero Trust**
- **Økt oversikt over rettigheter til ansatte**
- **Automatiserbart**

Negativt

- **Riktig konfigurasjon kan være komplekst og tidskrevende**
- **Lisenskostnad kreves**
- **Ved å geografisk begrense tilgang kreves det VPN**

1.3.5 Exchange Online Protection (EOP)

Selv om vi snakker om generell sikkerhet er det noen policier som fortjener sin plass utifra sikkerheten de bidrar til. Exchange Online er en standard kommunikasjonsmedium i M365 som brukes for å snakke både internt og eksternt, og uten et sikkerhetslag er det friflyt av informasjon mellom partene. Spam, phising og farlige lenker er et stort problem for alle bedrifter og her nevnes noen av egenskapene som bedriften kan implementere for å redusere sannsynligheten for å bli et offer.

- **Anti-malware**; legger på flere filtrere som flagger meldinger som inneholder malware i seg. Filtrene kan legges på grupper eller domene for å automatisere prosessen. *Anti-malware protection in EOP* udatert.
- **Anti-spam**; bruker ett sett med regler og kriterier for å determinere om en melding er relevant for deg. Gjennom powershell kan vi redigere det etter behov. *Configure anti-spam policies in EOP* udatert
- **Data loss prevention (DLP)**; beskytter sensitiv data ved å monitorere meldinger som blir sendt over kommunikasjonsmediet. Disse analyserer data man sender og vil blokke deg sendingen dersom det skal være noe sensitivt. *Learn about data loss prevention* udatert
- **Connection filtering**; identifiserer gode og dårlige email servere ved å se på IP-adressen og enten blokkere eller tillatte forbindelsen. *Configure connection filtering* udatert

1.3.6 Backup

En bedrift kan implementere så mange sikkerhetstiltak de vil for sin infrastruktur, men det vil alltid være en mulighet for at trussel aktør får tak i bedriftens data eller eskalerte rettigheter. Derfor må vi tenke på føre-var prinsippet innen risiko ved å opprette en backup for den viktigste M365 dataen. Microsoft 365 Backup vil lanseres i 2024, men fram til det er det tredje-parts løsninger for dette, som f.eks; Veeam. *Microsoft 365 Backup* udatert

Positivt

- Data beskyttelse ved løsepengevrius, menneskefeil eller naturkatastrofe.
- Enkel overføring ved potensiell migrering.
- Bedre kontroll over data.

Negativt

- Kostbart og tidskrevende.
- Må stole på tredjepartsleverandør
- Redundans. Microsoft har en viss grad for backup, men ikke fullstendig

1.4 Diskusjon og refleksjon

Det er mange tiltak en bedrift kan ta for å øke sikkerheten i sin bedrift. En liten bedrift vil kanskje gjøre konfigurasjonen selv, men uten erfaring er sterkt anbefalt å få et konsulentfirma inn i bilde for å forsikre at alt står opp mot best practise. Det kan være lett å tenke at; Det vil ikke skje med oss", men det er mange trusselaktører der ute som har scrips som scanner AD og M365 miljøer for svakheter, og vil angripe uten nåde.

Jeg er selv fornøyd med å ha implementert mer input validering og modul sjekker slik at man ikke kaster bort tid med å måtte slette og lage nye funksjoner (grupper/brukere/kanaler).

Hva kunne blitt gjort bedre?

- Mer bruk av CSV filer som inkluderer større datamengder. Jeg følte det ikke var nødvendig etter hva oppgaven spør etter, men vi vil alltid tenke skallering og automatisering.
- Bruk av **Microsoft secure score** for å gjøre det lettere å se hva bedriften har av svakheter eller mangler i sikkerheten sin.
- Mer implementering av sikkerhet innen Microsoft Teams og Sharepoint. Det er mange elementer som kan konfigurers, men nesten for mange til å ta med i obligen

Referanser

Anti-malware protection in EOP (udatert). URL: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-malware-protection-about?view=o365-worldwide.

Configure anti-spam policies in EOP (udatert). URL: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-spam-policies-configure?view=o365-worldwide.

Configure connection filtering (udatert). URL: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/connection-filter-policies-configure?view=o365-worldwide.

Eliminate bad passwords using Microsoft Entra Password Protection (udatert). URL: https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad.

Learn about data loss prevention (udatert). URL: https://learn.microsoft.com/en-us/purview/dlp-learn-about-dlp.

Microsoft 365 Backup (udatert). URL: https://techcommunity.microsoft.com/t5/microsoft-syntex-blog/welcome-to-microsoft-inspire-2023-introducing-microsoft-365/ba-p/3874887.

What is Conditional Access? (Udatert). URL: https://learn.microsoft.com/en-us/entra/identity/conditional-access/overview.