FAKULTET FOR INFORMASJONSTEKNOLOGI OG ELEKTROTEKNIKK

INFT2504 SKYTJENESTER SOM ARBEIDSFLATE

29.10.2023

Forfatter
Elias Rudsbråten

Innhold

1 OPPGAVE 1 - TEORETISK PERSPEKTIV (50 %)

1.1 Beskyttelse mot phishing angrep

Besvarelse:
Sikkerhet rundt Exchange Online er kritisk dersom man vil beskytte sin organisasjon for phishing-angrep. Oppgaven vil hovedsakelig snakke rundt tjenesten **Exchange Online Protection (EOP)** som man får i alle Microsoft/Office-365 abonnementer, og inneholder flere gode implementasjoner for å sikre Exchange Online sine postbokser. Jeg kommer til å spesifiserer **ON**, **OFF** eller **DEPENDENS** for policier dersom det er anbefalt å bruke eller at det kan komme anpå situasjonen, og dette vil være min tilnærming for oppgavespørsmålet; "Hvordan ville du implementert disse?"

Policies:

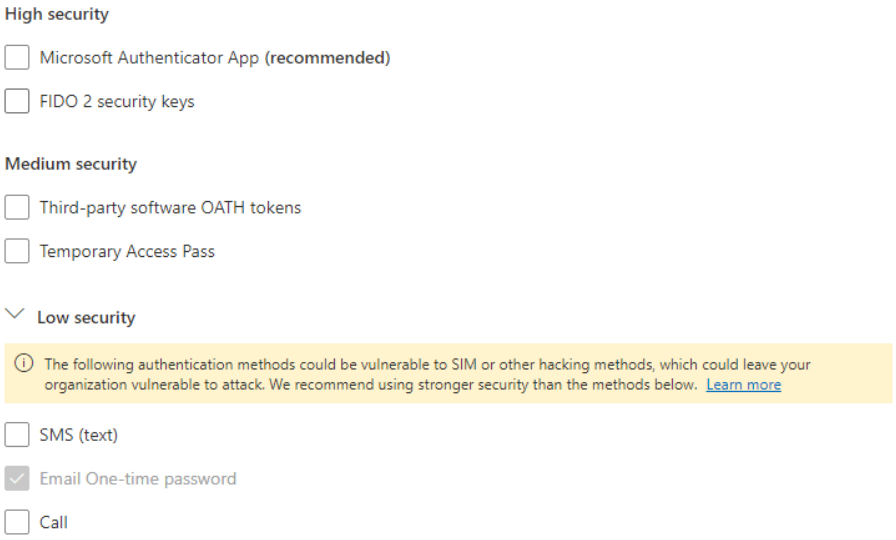
- **Anti-malware**; er en policy som vil sette mail i karantene dersom de inneholder skadevare noe som hindrer ansatte i organisasjonen fra å utsette sin maskinvare (*Anti-malware protection in EOP* udatert). Man kan lage en ny policy med kommandoen; New-MalwareFilterPolicy.
  - **EnableFileFilter/FileTypes;** ON: Blokkering av visse filtyper, spesielt kjørebare filer eller biblioteker da disse kan inneholde automatisk kjøring ved nedlasting.
  - **ZapEnabled;** ON: Zero-hour auto purge (ZAP) vil sette meldinger som det viser seg å ha innholdt skadevare **etter** de har ankommet i en Exchange Online mailbox. Slik unngår vi nye malware som går uoppdaget i å befinne seg i mailboxen når de senere blir oppdaget og flagget som skadevare.
- **Anti-spam filtrering**; bruker ett sett med regler og kriterier for å determinere om en melding inneholder truende innhold (*Configure anti-spam policies in EOP* udatert). Vi kan konfigurere både **incoming-** og **outbound** mail som blir sendt inn til eller fra organisasjonen. Mail som inneholder spam lignende innhold blir satt i karantene og eventuelt varsler brukere eller administrator dersom dette er konfigurert. Kommando; New-HostedContentFilterRule
  - **ExceptIfRecipientDomainIs;** DEPENDENT: Ved å spesifisere domene for organisasjonen kan vi utelukke meldinger som ikke er interne. Dette kan føre til at ansatte ikke får sendt eller motatt til/fra legitime epost kontoer så man må se på behovet og risikoen til situasjonen.
- **Connection filtering**; identifiserer gode og dårlige email servere ved å se på IP-adressen og enten blokkere eller tillatte forbindelsen (*Configure connection filtering* udatert). Vi kan spesifisere hvilke IP adresser som organisasjonen ikke skal motta fra, og her ville jeg brukt svartelister man kan finne på nettet. Kommando; Set-HostedConnectionFilterPolicy med -IPBlockList og IPAllowList
  - **ConfigurationXmlRaw;** DEPENDENT: Her kan vi hente IP-er fra en xml fil som vi enten vil tillate eller blokkere. Er det kun noen få IP-er det er snakk om er ikke dette nødvendig.
  - En negativ side ved connection filtering er hvordan man kan **spoofe** IP-addressene sine for å unngå å bli svartelistet, ved å lage nye IP pakker med en falsk kilde IP adresse. For å unngå dette ville jeg ha satt opp **sender protection framework (SPF)** (*Set up SPF to help prevent spoofing* udatert) som vil validere mail serveren som ble brukt under sending.

Sikkerhetstiltak:

- **Multifaktor autentisering (MFA)** er en effektivt sikkerhetsmekansime mot phishing angrep. Skulle trusselaktør får tilgang til ansatte sitt navn og passord må de fortsatt ha tilgang til det andre autentiseringsverktøyet man har satt for tjenesten. Dette er mulig for trusselaktøren å oppnå, men målet vårt er å legge flere lag for å sinke og komplisere angrepet.
  - Anbefalte MFA verktøy er; **Microsoft Authenticator app** for vanlige brukere og **FIDO 2 security key** for ansatte med høyere klarering. Det er viktig å nevne at FIDO keys koster penger og er derfor ikke noe man kan gi til alle ansatte.

1.2 Styring av e-postlevering i prosjektteam

Besvarelse:
Man vil velge innstillingen **"Only allow messages from people inside my organization"**. Ved å opprette en gruppe og kun legge til utvalgte ansatte som hører til distribusjonsgruppen, kan vi enklere bestemme hvem som skal kunne sende mail eller ikke.



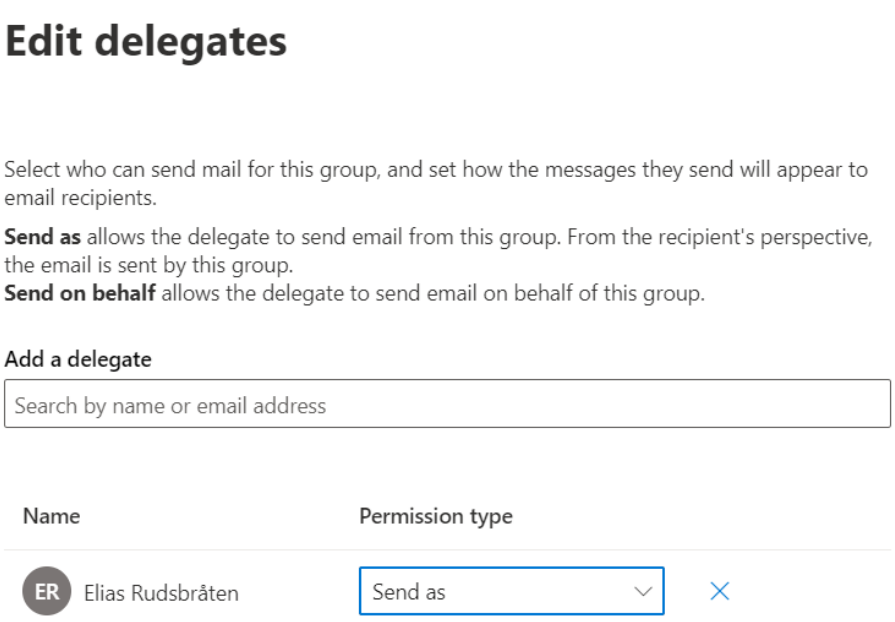
Figur 1: Distribusjonsgruppe GUI

1.3 Delegering og godkjenning av meldinger i ledelsen

1.3.1 Manage delegates

For at vi skal oppnå dette må vi legge til en delegat, altså en ansatt fra ledelsen som skal se over dokumentet før det sendes ut. I Exchange Online kan vi som admin velge en delegat og deretter velge mellom send aseller send on behalf". I dette tilfelle velger vi send asettersom ledelsen skal kun se over dokumentet men ikke være den som sender det. Vi kan se i bilde under hvordan vi kan gjøre dette i GUI.

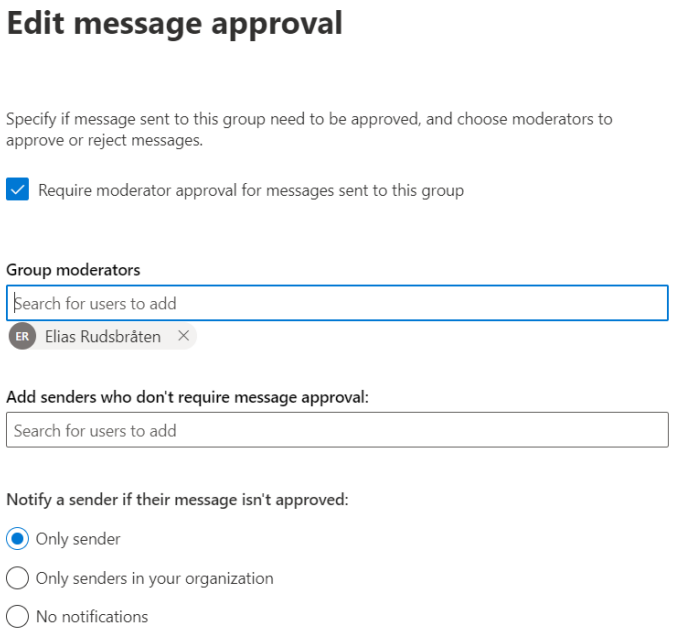
Dette kan også gjøres via powershell med kommandoen; Add-RecipientPermission -Identity brukerens-Mailbox -Trustee delegatensBrukernavn -AccessRights SendAs



Figur 2: Valg av delegat for gruppen

1.3.2 Message approval

Som vist i bilde under velger vi at meldinger som blir sendt til gruppen, altså klientene til organisasjonen, skal modereres før de blir sendt. Deretter ville jeg valgt hvem fra ledelsen som skal være moderator for alle meldinger sendt til gruppen, for eks; HR.



Figur 3: Valg av delegat for gruppen

Dette kan også gjøres i powershell **Set-DistributionGroup -Identity gruppeNavnModeratedBy ”moderator@domene.comSendModerationNotifications ”Always”**

I tillegg ville vi **eventuelt** lagt til en bypass for ansatte som har gjentatte samtaler med klienter og meldingene ikke er kritiske å moderere.

2 OPPGAVE 3 – SLUTTBRUKERENHETER (50 %)

2.0.1 Device Compliance

For ansatte som er på reiser kan det være en trussel for organisasjonen dersom deres enhet skulle være komprimert eller hacket, men ved å opprette en CA for enhetene kan vi redusere risikoen for dette. Det er flere senarior hvor en sikkerhetsbrudd kan oppstå, og oppgaven vil snakke om hvilken konfigurasjon som vil svekke sannsynlighet for uautorisert tilgang. Det er spesielt viktig at vi sjekker om enheten oppfyller kravene som organisasjonen har for mengde kryptering, antivirusbeskyttelse og oppdatert programvare.

- **Enheter innenfor en spesifikk fysisk lokasjon**
  - Ved å begrense lokasjonen hvor enheter kan logge seg innfra unngår vi land som er kjent for å engasjere i cyberkriminalitet, eks; Nord-Korea, China, Russland.
  - En negativ konsekvens med dette er dersom organisasjonen har klientell innenfor noen av disse landene, men dette kan vi endre ved å filtrere hvilke enheter policien skal gjelde for.
- **Enheter som kun har moderne autentiserings klienter**
  - Dersom enheten bruker apper/nettsider som fortsatt bruker utdaterte protokoller eller er bygget på dårlig kode vil vi blokkere disse.
- **Enheter som kun er koblet til sikre nettverk**
  - Flyplasser eller nettkaféer er kjent for å tilby offentlig wifi og disse er sjeldent opp til standard når det kommer til sikkerhet. Angrep som Man-in-the-middle angrep, falske nettverk og packet sniffing kan gjøre stor skade.

2.0.2 CA for apps

Applikasjoner har tendenser til å bryte rettighetene til brukerne sine eller ha overdøvende og komplisert terms of service. Dette kan være alt fra å lagre data fra personlige meldinger eller måten man bruker appen på, og med tanke på bedrifter kan dette bryte deres retningslinjer for sikkerhet. Derfor er det viktig å lage en conditional access policy slik at vi kan dynamisk blokkere og godkjenne apper.

- **Apps**
  - **All apps**; For å sikre enheten vil alle applikasjoner bli sett på som farlige, til og med microsoft godkjente apper, ettersom nye oppdateringener eller zero-day svakheter kan oppstå.
- **Data protection**
  - **Backup org data** ON; Selvom man tar intern backup skal man alltid ha flere. Vi følger 3-2-1 backup strategien *The 3-2-1 Backup Strategy* udatert
  - **Encrypt org data** ON; Kryptering av data er kritisk for flere typer cyberangrep, spesielt MITM angrep hvor data kan bli avskjært og lyttet til.
  - **Sync policy managed apps with native apps** OFF; Synkronisering av data mellom organisasjons- og offentlige applikasjoner kan føre til data på avveie når offentlige apper har tendens til å lagre brukerens data.
  - **Printing org data** Dependent; IF(ON), øker vi arbeidsfleksibilitet når ansatte skal printe fysiske rapporter, men dette øker også sjansen for intern lekking av sensitiv data.
  - **Org data notifications** OFF; Vi vil ikke at applikasjoner skal vise notifikasjoner da dette kan lekke sensitiv data skulle enheter ha blitt komprimert.
  - **Start Microsoft Tunnel** ON; Ved å ta nytte av VPN har brukere en sikker kobling til nettverk og andre enheter.

Det er flere konfigurasjoner man kan justere for å unngå applikasjoner som har diffuse retningslinjer, men dette er noen av de kritiske innen for data beskyttelse.

2.0.3 MFA for alt og alle

MFA er et av de sikkerhetstiltakene som burde dedikeres en egen conditional access til når absolutt alt og alle i organisasjonen skal ha dette. I tillegg til å være et krav for å være opp til standard med GDPR, mitigerer MFA sannsyneligheten for at trusselaktør skal kunne logge seg inn på interne brukere. Det er et gratis sikkerhetslag og enkelt å konfigurere, og derfor etablerer vi det enn hvor vi kan.

- **Users:** All users
- **Target Resource:** Include: All Cloud apps
- **Conditions:** All device platforms og locations
- **Grant access:** Require multi-factor authentication

Det er ulike typer MFA organisasjonen kan ta nytte av avhengig av budsjett og sikkerhet.

- **Microsoft Autentication App**; En billig og effektiv form for autentisering som gir god sikkerhet.
- **FIDO 2 security key**; En mer kostbar variant men med økt sikkerhet ved bruk av public- og private nøkkler. Krever PIN/fingeravtrykk for å akseseress.

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.

Set up SPF to help prevent spoofing (udatert). URL: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/email-authentication-spf-configure?view=o365-worldwide.

The 3-2-1 Backup Strategy (udatert). URL: https://www.backblaze.com/blog/the-3-2-1-backup-strategy/.