Fakultet for informasjonsteknologi og informatikk

INFT2504 Skytjenester som arbeidsflate (2024 HØST)

Oblig01

Høst, 15. september 2024

1. Innledning

NyTech AS, en mellom stor teknologibedrift med 50 ansatte, har besluttet å implementere Microsoft 365 som et verktøy for å forbedre samarbeid, effektivitet og sikkerhet på tvers av organisasjonen. Med en struktur som omfatter flere avdelinger, fra utvikling, salg og markedsføring til kundesupport, IT-drift og administrasjon, er det avgjørende å sikre at implementeringen av Microsoft 365 tilpasses bedriftens spesifikke behov.

Denne rapporten tar sikte på å utvikle en omfattende strategi for lisensiering, postbokskonfigurasjon, sikkerhetstiltak og fremtidige hensyn som vil styrke bedriftens arbeidsflyt og sikkerhetsrammeverk.

2. Lisensiering og Implementeringsstrategi

2.1. Lisensiering

Jeg anbefaler at NyTech AS bruker «Microsoft 365 Business Premium» for alle ansatte av tre hovedårsaker:

- Enhetlig løsning: Denne lisensen gir tilgang til Office-applikasjoner som Outlook, Word, Excel og Teams, samt løsninger for samhandling som SharePoint og OneDrive, noe som støtter effektivt samarbeid på tvers av avdelinger.
- Sikkerhet og administrasjon: Denne tilbyr avanserte sikkerhetsfunksjoner som multifaktorautentisering (MFA), enhetsadministrasjon og beskyttelse mot cybertrusler, som er avgjørende for å sikre at IT-driften kan administrere systemene sikkert.
- Skalerbarhet: gir fleksibilitet for fremtidig vekst. Bedriften kan enkelt skalere opp med flere lisenser eller tilpasse abonnementene etter behov, noe som er ideelt for en voksende teknologibedrift.

2.2. Organisering av grupper i Microsoft 365:

Grupper i Microsoft 365 bør settes opp basert på selskapets avdelingsstruktur for å reflektere organisasjonens ulike funksjoner. Dette vil bidra til bedre samarbeid og en mer strømlinjeformet kommunikasjon. Nedenfor er en anbefalt organisering:

Avdeling/Team	Beskrivelse
Ledelse	Gruppe for ledelsen til å dele konfidensielle dokumenter og håndtere intern kommunikasjon.
Utviklingsavdeling	Hovedgruppe for utvikling med undergrupper for team for å støtte ressurskoordinering og prosjektdeling.
Salg og Markedsføring	Hovedgruppe for salg og markedsføring med undergrupper for hver funksjon for å koordinere kampanjer og dele materiale.
Kundesupport	Gruppe for kundesupport for å spore forespørsler og dele kunnskap for bedre tjenestekvalitet.
IT-drift	Dedikert gruppe for IT-administrasjon for å håndtere interne systemer og støttebehov.
Administrasjon	Gruppe for administrasjon til å håndtere kommunikasjon og dele dokumenter relatert til økonomi og administrative oppgaver.

Tabell 1: Gruppeorganisasjon

I tillegg til avdelingsspesifikke grupper bør det opprettes tverrfaglige grupper for å fremme samarbeid på tvers av ulike avdelinger:

Tverrfaglig Samarbeid	Beskrivelse
Utvikling og Salg	Gruppe dedikert til samarbeid mellom produktutvikling og salg.
Kundesupport og Utvikling	Gruppe for kommunikasjon og tilbakemelding mellom support og utviklere for å forbedre produkter.
Salg og Kundesupport	Gruppe for å styrke samarbeid rundt kundeoppfølging og salgsstøtte.

Tabell 2: Tverrfaglige grupper

2.3. Administrasjon og sikkerhet

Gi IT-drift forskjellige nivåer av administrative roller basert på behov for tilgang, og sørg for at kun de som trenger full kontroll har Global Administrator-roller (IT-sjef som global administrator eller andre administratorroller for tilgang til adminverktøy). Dette gir IT-avdelingen tilstrekkelig kontroll over konfigurasjon og sikkerhetsinnstillinger, samtidig som risikoen for uautorisert tilgang reduseres. Bruk Azure Active Directory (AAD) til å implementere Privileged Identity Management (PIM), slik at spesifikke rettigheter bare aktiveres når det er nødvendig, og for å gi midlertidig forhøyet tilgang til kritiske systemer. Sørg også for at Multifaktorautentisering (MFA) er aktivert for alle med administrativ tilgang, for å ytterligere styrke sikkerheten og redusere risikoen for kompromittering av administrator-kontoer.

3. E-post- og Samarbeidskonfigurasjon

3.1. Postboksoppsett for NyTech AS

Postboksoppsett for NyTech AS foreslår jeg følgende konfigurasjon:

- Brukerpostbokser: Opprett individuelle brukerpostbokser for hver ansatt (med standard lagringskapasitet på 100 GB), slik at de kan motta og sende e-post via sitt eget domene (f.eks., fornavn.etternavn@nytech.com).
- Delte postbokser: For å håndtere felles kommunikasjon, opprett delte postbokser som "support@nytech.com" for kundesupport og "sales@nytech.com" for salgsavdelingen. Dette vil tillate flere ansatte å få tilgang til og svare på e-poster fra en felles innboks.
- Ressurspostbokser: Opprett ressurspostbokser for felles ressurser som møterom (f.eks., "MeetingRoom1@nytech.com") og utstyr (f.eks., "Projector@nytech.com"). Dette gir ansatte muligheten til å booke disse ressursene via Outlook-kalenderen.

- Arkivpostbokser: Aktiver arkivpostbokser for ansatte som har behov for å lagre store mengder e-post over lengre tid f.eks for ansatte i ledelse og kundesupport som trenger å beholde e-post for compliance-formål.

3.2. Scenarier for Ressurspostbokser

- Scenario 1: Opprett ressurspostbokser for møterom, slik at ansatte enkelt kan reservere møterom gjennom Outlook når de planlegger møter.
- Scenario 2: Ressurspostbokser for deling av utstyr som projektorer og bærbare datamaskiner ved å opprette en ressurskalender der utstyr kan reserveres for spesifikke tidsrom og kan også hjelpe med å holde ov ersikt over tilgjengelig utstyr.

Oppsett og administrasjon: Administratorer konfigurerer ressurspostbokser i Exchange Admin Center (EAC), definerer tillatelser og tilgjengelighet, og setter opp automatisk bekreftelse av reservasjoner. IT-avdelingen administrerer tilgjengeligheten, og kan enkelt oppdatere og vedlikeholde bookinger via PowerShell for automatiserte oppgaver.

3.3. Implementert Microsoft 365-grupper

Opprett Microsoft 365-grupper for hvert avdelingsteam slik jeg gjorde/beskrev i avsnitt 2.2. (Organisering av grupper i Microsoft 365). Dette gjør det mulig å samle e-post, kalendere, og delte dokumenter på ett sted. Forbedre arbeidsflyten mellom utviklings-, salgs- og kundesupportteamene ved å opprette tverrfaglige grupper for spesifikke prosjekter.

3.4. Navnekonvensjon for gruppene

Avdeling	Gruppe
Ledelse	NyTech-Management (ADMIN: O365-TEAM-Ledelse-ADMIN)
Utviklingsavdeling	DEP-Utvikling (Team: NyTech-Dev-Team1, NyTech-Dev-Team2)
Salg og Markedsføring	DEP-SalgMarkedsføring (Funksjon: DEP-Salg, DEP-Markedsføring)
Kundesupport	DEP-Kundesupport
IT-drift	SEC-IT-ADMIN
Administrasjon	DEP-Administrasjon

Tabell 3: Avdelinger Og Grupper

Avdelinger Samarbeid	Samarbeidsgruppe
Utvikling og Salg	O365-TEAM-ProdSalg
Kundesupport og Utvikling	O365-TEAM-SupportDev
Salg og Kundesupport	O365-TEAM-SalgSupport

Tabell 4: Avdelinger Og Grupper

4. Sikkerhetsstrategi

4.1. Risikoprofil og kritiske sikkerhetsbehov

Avdeling	Risikoprofil	Kritiske sikkerhetsbehov
Ledelse	Tilgang til sensitiv strategisk informasjon; mål for BEC og phishing-angrep.	Anti-phishing, imitation protection, MFA, Conditional Access.
Utviklingsavdeling	Håndterer kildekode og intellektuell eiendom; høy risiko for datainnbrudd og tap av informasjon.	DLP, Safe Attachments, anti-phishing rettet mot utviklere.
Salg og Markedsføring	Kommuniserer med eksterne parter; utsatt for phishing, malware og risiko for datalekkasjer.	Safe Links, ATP, strenge policyer for håndtering av kundedata.
Kundesupport	Tilgang til kundedatabaser; risiko for sosial manipulering og håndtering av eksterne filer.	Safe Attachments, Safe Links, opplæring i sosial manipulering og phishing.
IT-drift	Full tilgang til infrastruktur; risiko for full systemkompromittering ved brudd.	MFA, PIM, Conditional Access.
Administrasjon	Håndterer finansiell informasjon; mål for svindel og økonomisk phishing.	Anti-phishing, DLP, beskyttelse mot BEC-angrep.

Tabell 5: Risikoprofil og kritiske sikkerhetsbehov

Liste over forkortelser:

- BEC: Business Email Compromise.
- MFA: Multi-Factor Authentication.
- DLP: Data Loss Prevention.
- ATP: Advanced Threat Protection.
- PIM: Privileged Identity Management.

4.2. Forhåndsdefinerte sikkerhetspolicyer

- Strenge Preset Security Policies: Denne policyen gir et høyt nivå av beskyttelse mot phishing, skadelig programvare og spam. Den anbefales spesielt for høyrisiko-brukere som ledelsen og IT-drift.
- Standard Preset Security Policies: Denne policyen er godt egnet for de øvrige ansatte og gir grunnleggende beskyttelse mot phishing, spam og malware.

4.3. Konfigurering

- Anti-phishing: Konfigurer en streng anti-phishing-policy som beskytter alle brukere, med ekstra beskyttelse for ledelsen. Denne policyen bør inneholde avanserte regler for å oppdage phishing-forsøk, særlig rettet mot impersonasjon av bedriftsledere og eksterne kontakter.
- Safe Attachments: Aktiver Safe Attachments for alle brukere. Vedlegg bør skannes automatisk i en sikker «sandbox» før de når mottakeren, for å sikre at de ikke inneholder skadelig programvare.
- Safe Links: Aktiver Safe Links for å beskytte brukere mot farlige URL-er. Alle lenker i e-poster og Office-dokumenter bør skannes i sanntid, med varsler om eventuelle skadelige nettsteder.

4.4. Tilpassede sikkerhetspolicyer for NyTech AS

- DLP-policy: Sikre at sensitiv kildekode og kundeinformasjon ikke deles utenfor organisasjonen.
- Anti-phishing-policy for ledelsen: Beskytt ledelsen mot impersonasjon og BEC-angrep med strenge autentiseringskrav.
- Sikkerhetspolicy for CFO og økonomiansvarlig: Implementer MFA for finansielle aktiviteter og oppsett av varsler for mistenkelige pengeoverføringer.

4.5. Configuration Analyzer

Bruk Configuration Analyzer i Microsoft Defender for Office 365 for å evaluere og optimalisere sikkerhetskonfigurasjonene. Configuration Analyzer skanner miljøet for å identifisere potensielle sårbarheter og gir anbefalinger for forbedringer. Ved å implementere disse anbefalingene kan NyTech AS kontinuerlig forbedre sikkerhet innstillingene og redusere risikoen for angrep.

5. Fremtidige hensyn

- eDiscovery-funksjonen kan implementeres for å sikre at juridiske og regulatoriske krav, som for eksempel GDPR (General Data Protection Regulation), overholdes. For NyTech AS vil dette være avgjørende ved juridiske etterforskninger eller revisjoner. GDPR krever at organisasjoner beholder personopplysninger og gjør dem tilgjengelige ved forespørsler. Ved å bruke eDiscovery kan administratorer sette data på juridisk vent (litigation hold) for å forhindre sletting av informasjon som kan være relevant i fremtidige juridiske saker eller compliance-prosedyrer.
- Fremtidige trinn:
    - Implementer Microsoft Endpoint Manager for håndtering av enheter og sikkerhetskontroller for å styrke beskyttelsen mot uautorisert tilgang og sikre at enheter er i samsvar med bedriftens sikkerhetsstandarder.
    - Vurder bruk av Power BI for datadrevet beslutningstaking, og implementer Azure Information Protection for å sikre at sensitive dokumenter blir beskyttet mot uautorisert tilgang både innenfor og utenfor organisasjonen.

6. Konklusjon

Gjennom en nøye tilpasset implementeringsplan for Microsoft 365, kan NyTech AS dra nytte av økt produktivitet og forbedret samarbeid, samtidig som organisasjonens verdifulle data og systemer beskyttes mot moderne cybertrusler.

Ved å benytte forhåndsdefinerte sikkerhetspolicyer og implementere tilpassede sikkerhetstiltak, vil bedriften være godt rustet til å møte både nåværende og fremtidige utfordringer innen cybersikkerhet. Fremtidige trinn som innføring av eDiscovery og forbedret enhetshåndtering vil ytterligere styrke sikkerheten og effektiviteten til NyTech AS, og sikre fortsatt vekst og innovasjon.

Referanseliste

Fra fagets pensum:

- Uke 34: 01-ssa-introduksjon.pdf, 02-ssa-abonnement-lisenser.pdf
- Uke 35: 03-ssa-IdentityAccessManagement.pdf, 04-ssa-EnOrganisasjoniSkyen.pdf
- Uke 36: 05-ssa-exchange.pdf
- Uke 37: 05-ssa-exchange security.pdf