Oppgave 3

Beskrivelse og mål for oppgaven

Den første oppgaven skal gå innom årsaken/forskjellen bak inndelingen av de fire ulike kategoriene av mulige "assets" i Microsoft 365 med fokus på sikkerheten rundt dem. Oppgave 2 skal løse utfordringen med å sørge for bra tilgjengelighet av dokumenter og rapporter i M365. Til slutt, skal oppgave 3 skal det vurderes hvilke tre conditional access konfigurasjoner er viktigst for bedriften for å sikre sitt IT utstyr.

Besvarelse

Oppgave 1

Det er gode grunner for at de forskjellige assets har sikkerhet på sine egne nivåer, ettersom hver av disse har sine egne svakheter som kan bli utnyttet. For å løse dette problemet for sine brukere, har Microsoft utviklet en rekke med tiltak som omfattende beskytter alle nivåene som inkluderer brukere, data, enheter og apper. De forskjellige tiltakene er spesielt viktige ettersom de beskytter sine egne spesifikke deler dersom sikkerheten til noe annet de er avhengige av blir brutt. For eksempel, med tanke på situasjonen der en laptop blir stjålet, kan laptopen være beskyttet med passord eller til og med MFA. Likevel er det en mulighet for en trussel å koble fra disken og koble den til en annen enhet for å få tilgang til data som den inneholder. Men dersom beskyttelse er innført også på data med for eksempel kryptering, vil det fortsatt være en større utfordring å få tilgang til den.

Dette kan også strekke seg lenger enn kun å beskytte seg fra hendelser forårsaket av angripere. Deler av de forskjellige nivåene er også med på å holde styr på tilgangskontroll, slik at bare de med de riktige tillatelsene får tilgang til visse ressurser. Man ønsker ikke at konfidensielle dokumenter skal bli åpnet av hvem som helst i hvilken som helst app. Dårlig sikkerhet på apper kan sannsynlig være årsaken bak at sensitiv informasjon lekkes, og derfor er det ekstra viktig å ha sikkerhet på alle nivåer som inngår i beskyttelse av data. I tillegg til beskyttelse, kan det inngå overvåkning av de ulike kategoriene som senere kan bli brukt for beskyttelse eller forebygging av den.

Oppgave 2

En måte å forebygge tap av data hos bedriften er å ta i bruk Microsofts Data Loss Prevention. Den sørger for at sensitiv data ikke havner utenfor bedriften på flere ulike måter. DLP klarer å tolke konteksten bak ulike handlinger innen de ansattes arbeidsmiljø, og ved hjelp av det blokkere uønskede handlinger. I dette tilfellet burde CyberDyne Systemes for eksempel sette opp policies som blokkerer kopiering av sensitiv informasjon, både små deler av tekst og hele filer. I tillegg kan deling, tilgang og visning av informasjon begrenses. Bedriften kan sette opp DLP for å dekke alle slags Microsoft-tjenester som de bruker som for eksempel Exchange Online, SharePoint Online, Microsoft Teams og OneDrive.

Å unngå tap av data inkluderer også pålitelig oppbevaring og tilgjengelighet av kritisk informasjon. Denne delen kan dekkes ved hjelp av data governance, altså datastyring. Bedriften kan sette opp arkivering av data, og i tillegg sette opp retention labels, altså oppbevaringsetiketter. Retention labels passer på av datalagring og -sletting holder seg innen policies slik at kritisk informasjon beholdes slik som ønsket.

For å sikre at kun de som skal ha tilgang til dataen får det, kan bedriften benytte label policies.Dersom dette blir aktivert, krypterer etikettene (labels) filene for dem som har begrenset tilgang. Denne måten å administrere tilgang på sørger for at kun brukerne med tilsvarende rettigheter får tilgang til informasjonen som beskyttes av etiketten.

I tillegg som forsikring, kan bedriften også overvåke sine policies for å undersøke aktiviteten bak dem og å oppdage for eksempel brudd av policies, som senere kan brukes for forebygging av sikkerhet eller aktivt forsvar.

Oppgave 3

Policy Name	Krev godkjente apper og app-beskyttelse for Office 365 hos alle brukere.
Applied to	All users
Cloud Apps or Actions	Office 365
Conditions	Any device & Any location
Access Control	Krev godkjente apper og app-beskyttelse.

Den første CA konfigurasjonen som CyberDyne Systemes bør innføre er å kreve bruk av godkjente apper og app-beskyttelse. Dette skal gjelde uansett bruker, hvor som helst, med hvilken som helst enhet. Grunnen for at denne CA konfigurasjonen skal brukes er på grunn av at i oppgave 2 ønsket bedriften å sørge for at data ikke går tapt. Med denne konfigurasjonen sørges det for at ingen usikrede apper brukes i sammenheng med jobben for å unngå datatap. Denne konfigurasjonen sørger også for at kun bedriftens enheter tas i bruk med tanke på oppgaven.

Policy Name	Krev MFA for alle brukere
Applied to	All users
Cloud Apps or Actions	Office 365
Conditions	Any device & Any location
Access Control	Krev multifaktorautentisering.

Den andre CA konfigurasjonen som bedriften bør innføre er et krav på bruk av multifaktorautentisering av alle brukere. Her bør det tas i bruk MFA ved hjelp av autentiseringsappen til Microsoft i stedet for mobilnummer for å unngå SIM swapping. Ved tilfellet der passordene til noen ansatte blir oppdaget av trusler, eller enheten blir stjålet, hindrer MFA dem fra å få tilgang til brukere og tjenester uten bekreftelse fra MFA. Selv om dette kan virke ubeleilig for noen brukere å bruke hver gang, er det viktig for bedriften å beskytte seg selv fra alle slags svakheter, som i dette tilfellet er de ansatte.

Policy Name	Ingen vedvarende nettleserøkt for alle brukere
Applied to	All users
Cloud Apps or Actions	All cloud apps
Conditions	Any device & location, Exclude trusted locations
Access Control	Ingen vedvarende nettleserøkt. Krev reautentisering etter 1 time.

Den tredje CA konfigurasjonen som er viktig for bedriften å hindre vedvarende nettleserøkt for alle brukere. Altså dette sørger for at de ansatte ikke forblir innlogget på sine arbeidsområder. Dette sørger for at dersom en enhet blir stjålet fra en ansatt, er det ikke mulig å få tilgang til arbeidsområdet uten innlogging som da også vil kreve MFA. Likevel, for å ikke hindre arbeidsflyten til de som jobber on-premises, ekskluderes kjente steder fra denne policyen, slik at de ikke skal påvirkes. Ved å ekskludere kjente steder, skal det være en forutsetning at de stedene har god fysisk sikkerhet.

Diskusjon og refleksjon

Ved å bruke Data Loss Protection, kan bedriften sørge for at alle tjenester som de tar i bruk, blir sikret. Ved å ha omfattende beskyttelse, sørges det for at færre muligheter for tap av data dukker opp. Selv om label policies i seg selv bør beskytte informasjon fra uønskede parter, kan det likevel hende at for eksempel dokumenter blir satt opp med feil label, som letter tilgangen eller motsatt. Derfor hadde det også vært en mulighet å sette opp flere tilgjengelighetskontroller.

Oppgave 3 tar for seg kun Office 365 for to av konfigurasjonene, som kunne også dekket alle cloud apps for enda mer beskyttelse, spesielt for MFA. Med tanke på tabell 3, kunne det i tillegg vært en CA for å sjekke om enheter som brukes i de pålitelige stedene faktisk er klarerte enheter, slik at de uklarerte enhetene fortsatt ikke har vedvarende nettleserøkt. Men igjen, alt dette er avhengig av om selve stedene er godt nok sikret slik at trusler ikke får tilgang på grunn av vedvarende øktene til de ansatte.

Siden i oppgave 2 var det et krav for bedriften å sikre seg selv mot datatap, tok jeg det med til oppgave 3 og laget en conditional access for å gjøre akkurat det, og å knytte oppgavene sammen i tillegg.

Selve oppgaven gikk generelt greit, men siden første deloppgave kunne til tider være litt uklar, kan det være små deler som kan være uoppnådd. Deloppgave 2 og 3 følte jeg at gikk veldig bra, og at jeg fikk dekket det meste med tanke på sikkerheten rundt situasjonene beskrevet i oppgavene.

Kilder

ssa-ls10-Sikkerhet og databeskyttelse.pdf
ssa-ls11-Administrer sikkerhet.pdf
https://learn.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide
https://learn.microsoft.com/en-us/microsoft-365/compliance/encryption-sensitivity-labels?view=o365-worldwide