Oppgave 2

Problem og mål

Teoribiten av oppgaven vil gå gjennom en prosess der en bedrift starter å bruke Microsoft 365. Selve bedriften består av tre avdelinger, HR, IT og Developer. De vil ta i bruk Teams, SharePoint, og en felles gruppe for alle ansatte. I tillegg skal de kunne booke to møterom. Med tanke på dette, er målet med oppgaven å finne fram til sikkerhetstiltak som kreves for at M365 skal være trygt for bedriften å bruke. I den praktiske delen skal det lages et script som utfører alle oppgavene fra teoribiten. Dette inkluderer å lage brukere, og å sette opp de forskjellige tjenestene.

Besvarelse

For å beskytte Microsoft 365 miljøet til bedriften, er det en rekke med tiltak som kan innføres. Først og fremst, det mest åpenbare tiltaket er mest sannsynlig multifaktorautentisering. Dette er med å beskytte kontoer ved å bekrefte at den som logger inn faktisk er den som eier brukeren. I sammenheng med Microsoft 365, vil MFA mest sannsynlig foregå gjennom Microsoft sin Authenticator app der brukeren må enten godkjenne innloggingen med en knapp, eller skrive inn en engangskode som fornyes hvert 30. sekund. Altså i tilfellet der et passord har blitt kompromittert, vil truslene fortsatt ikke klare å komme seg videre uten MFA.

Selv om man fort kan kun fokusere på kun tekniske sårbarheter, er social engineering også et problem som kan dukke opp. I dette tilfellet er det de ansatte som er sårbarheten. For å unngå slike forsøk på angrep, kan bedriften lære opp ansatte innen beste praksis om eposthåndtering. Dette inkluderer å unngå spam, søppelpost, forsøk på phishing, spoofing og spredning av skadevare.

For å videre hjelpe bedriften å unngå angrepsforsøk gjennom epost som ble nevnt ovenfor, kan de benytte tjenesten Exchange Online Protection (EOP) som innfører flere typer filtere og teknologier som skal forhindre spam i Exchange Online sin eposttjeneste. Som beskrevet i leksjon 5, er disse Connection Filtering, Incoming Spam Filtering, Outbound Spam Control, Transport Rules, Email Authentication, og End-User settings. Alle disse er med på å forhindre at skadelige eposter ikke skal rekke postkassen i det hele tatt. Dette skjer ved for eksempel å sjekke avsenderens omdømme eller etter spor av egenskaper som gir tegn på spam. Ved å sikre at skadelig epost ikke rekker postkassen til en ansatt,

Når det kommer til tilgjengelighet, som for eksempel av grupper og rettigheter knyttet til grupper/avdelinger, må bedriften sørge for at det kun er de riktige personene som får tilgang til det de skal ha tilgang til. Siden HR sitt arbeid omhandler personer, vil mye av arbeidet deres bruke persondata. Dette er noe som de andre avdelingene ikke har noe grunn å ha tilgang til, ettersom arbeidet deres omhandler noe helt annet. Dette gjelder begge veier, siden HR ikke har anledning til å bruke kode fra Developer-avdelingen eller nettverksinformasjon fra IT-avdelingen. Ved å begrense adgang til informasjon som de ansatte ikke krever å ha tilgang til, vil også sannsynligheten for at data går på avveie og misbrukes minskes.

En måte å begrense tilgjengelighet er å bruke Teams-områdene som bedriften ville sette opp. Ansatte får kun tilgang til det Teamet som avdelingen deres hører til. Inne der vil de kunne ha sikrede samtaler og møter mellom andre medlemmer fra avdelingen, slik at konfidensielt informasjon holdes kun inne i avdelingen. Tilgjengelighet til filer kan også knyttes til Teams slik at filer ikke skal bli åpnet av eksterne personer. I tillegg til Teams, kan filer lagres på SharePoint som bedriften også ville innføre. Her vil også kun de med tilgang få kunne hente filene. Hvis avdelingene skulle hatt behov for å dele filer med eksterne parter, kan gjester enten legges til i Teams, eller en sikret link til filen deles ved hjelp av SharePoint.

Bedriften må også gå gjennom sine innstillinger i tjenestene de bruker, og endre dem for å tilfredsstille sikkerhetskravene deres. Det er spesielt viktig for bedriften å fokusere på innstillingene hos tjenestene der de deler opp de ulike avdelingene slik at relevant informasjon beholdes innen avdelingen. Et spesifikt eksempel på dette er SharePoint (og OneDrive), der delingsnivået som standard er satt på det mest åpne nivået. Det vil også finnes tilfeller der standardinnstillingene er bra nok for sikkerheten i bedriften, som gjør at arbeidet for å endre eller opprette instillinger slippes. Å beskytte administratorbrukere er viktig for bedriften ettersom de har flere rettigheter, og å endre på innstillinger og policies er en måte å beskytte dem på. M365 har også "alert policies" som gir bedriften muligheten å spore aktivitet innen bedriften. Disse varslene kan hjelpe bedriften med å spore uønskede hendelser og løse dem deretter. Et eksempel på dette er å bruke dette for å se om noen deler en fil eksternt, som egentlig skulle holdes innad i avdelingen. Bedriften kan selv sette opp sine egne alert policies for å spore akkurat de de har behov til å spore.

Diskusjon og refleksjon

Med tanke på MFA, er det svært viktig for bedriften at de ikke benytter telefonnummere for dette. Ved å bruke telefonnummer for MFA, er det mulig for trusler å utføre SIM swapping som betyr å stjele telefonnummeret til offeret via social engineering eller inside-hjelp hos operatøren. Dette kan da brukes for å motta kodene som MFA spør om for å logge inn i brukeren. På grunn av dette er som sagt Microsoft Authenticator den beste løsningen for MFA for bedriften.

Generelt sett er filtrering av epost positivt, men det er noen tilfeller det altfor strenge filtere på epost kan ende opp med å kaste bort legitime epost. I slike situasjoner er det en mulighet å lette på filtrene, eller å whiteliste avsendere som bedriften forventer ved hjelp av tjenesten Connection Filtering fra Exchange Online Protection. Dette er en avveining som bedriften må vurdere. Enten mottar de spam litt oftere, eller så går noen få legitime meldinger med mistenkelige egenskaper tapt.

Selv om det å bruke standardinstillinger og standard policies, kan være en grei løsning for noen deler av bedriften, kan denne løsningen misbrukes. Hvis en trussel kjenner til svakhetene i innstillingene hos bedriften, kan det være lett å utnytte dette for å utføre skade på bedriften. Det samme gjelder policies, som for eksempel i alert policies, der en trussel kan unngå oppmerksomhet ved å unngå å utløse varsler som kan spores senere.

Jeg tok utgangspunkt i Microsoft sin egen artikkel om topp 10 måter å sikre data på. Ved å bruke listen i artikkelen, valgte jeg de viktigste tiltakene og utdypte dem ved hjelp av Microsoft sine egne artikler, i tillegg til leksjonene fra dette emnet. Dette føltes ut som en grei måte å løse oppgaven på, og jeg føler jeg fikk med det viktigste. Det som jeg likevel kunne ha nevnt og utdypt mer om var felles kontaktpunkt for avdelingene, slik at de ansatte ikke sender feil informasjon eller data til feil person.

Kilder

ssa-ls05-Trusler Exhange Online.pdf \ ssa-ls07-teams.pdf \ https://learn.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/secure-your-business-data?view=o365-worldwide \ https://learn.microsoft.com/en-us/microsoft-365/business-premium/m365bp-avoid-phishing-and-attacks?view=o365-worldwide \ https://learn.microsoft.com/en-us/microsoft-365/business-premium/create-teams-for-collaboration?view=o365-worldwide \ https://learn.microsoft.com/en-us/microsoft-365/business-premium/set-up-meetings?view=o365-worldwide \ https://learn.microsoft.com/en-us/microsoft-365/business-premium/share-files-and-videos?view=o365-worldwide \ https://blog.mozilla.org/en/internet-culture/mozilla-explains/mozilla-explains-sim-swapping/

https://portal.azure.com/#home