SJEKKLISTE

Utnytter du sikkerhetspotensialet med Microsoft 365?

advania

Innhold

Innledning

Hvordan beskytter jeg viktig informasjon? Hvordan gir jeg trygg tilgang og unngår hackere? Hvordan sikrer jeg hjemmekontor? Hvordan stopper jeg phishing?

Dette er utfordringer for IT-ledere i dag. Økt sikkerhetsrisiko er avgjørende for norske bedrifter. Med en stadig mobil arbeidshverdag er investering i kultur, kompetanse og sikkerhetstjenester viktig.

Microsoft 365, en ledende skyplattform, gir innebygd sikkerhet for både brukerdata og bedriftsinformasjon, tilpasset 2023.

Med Microsoft 365 får du:
- Beskyttelse mot trusler
- Sikring av virksomhetsdata
- Beskyttelse av PC-er og mobile enheter for brukerne
- Enkel administrasjon av sikkerhet

Noen sikkerhetsfunksjoner i Microsoft 365 er klare til bruk, mens andre trenger konfigurering for å sikre at virksomhetens tjenester fungerer som de skal etter aktivering av sikkerhetsfunksjonene. For å maksimere sikkerhetsfordelene anbefaler Microsoft at kunder får hjelp fra profesjonelle partnere.

Sjekklisten vi har utarbeidet er designet for å redusere sikkerhetsrisiko i virksomheten. Den inneholder åtte punkter som er viktige for å utnytte sikkerhetspotensialet i Microsoft 365. Her får du også råd om hvordan du kan forbedre sikkerheten i din virksomhet.

Sjekklisten består av følgende punkter:

1. Kartlegg sikkerhetsbehovene
2. Velg riktig abonnement og konfigurasjon
3. Etablér en god sikkerhetskultur
4. Intern opplæring og trening
5. Aktiver flerfaktor-autentisering
6. Blokker gammel programvareprotokoll
7. Implementer moderne sikkerhetsrammeverk
8. Vurder verdiøkende sikkerhetstjenester

Husk at datasikkerhet alltid vil handle om å redusere risikoen, ikke eliminere den. Derfor må du sørge for å beskytte virksomhetens informasjon og systemer lagvis. For hvert lag du innfører reduseres risikoen for å bli utsatt for et dataangrep.

God fornøyelse!

Med vennlig hilsen,

Garzai Ehsas
Microsoft Lead, Advania

1. Kartlegg sikkerhetsbehovene

Investerer tid i å kartlegge virksomhetens sikkerhetsbehov.

Denne kartleggingen bør inneholde en grundig gjennomgang av virksomhetens verdier, identifisering av sårbarheter, analyse av gjeldende trusselbilde og vurdering av relevante sikkerhetstiltak.

Sikkerhet er en kontinuerlig prosess. Ved ansettelse av nye medarbeidere, oppdatering av IT-strategier eller endringer i virksomhetens IT-miljø, må sikkerhetsløsningene gjennomgås og opprettholdes. Det er også viktig å ha en tydelig ansvarsfordeling slik at alle er klar over sin rolle og utfører den på en god måte.

2. Velg riktig abonnement og konfigurasjon

Når du har kontroll på sikkerhetsbehovet, har du et godt utgangspunkt for å vurdere hvilket Microsoft 365-abonnement som passer best for virksomheten din. Sørg for at tjenestene som er inkludert i lisensene dine, er aktivert og riktig konfigurert.

Sikkerhetsfunksjoner i Microsoft 365 varierer; noen er enkle å implementere, mens andre krever spesifikk konfigurering for å sikre at virksomhetens tjenester forblir stabile. Advania jobber tett for å redusere trusselbildet for virksomheter ved å kombinere ulike kompetanser innen strategi, teknologi og operativ sikkerhet.

Rådgivning og verdiøkende tjenester fra Advania bidrar til å forbedre sikkerheten gjennom implementering av Microsoft 365 etter beste praksis og proaktiv forvaltning. Dette inkluderer konfigurering og optimalisering av sikkerhetsfunksjonaliteten, samt løpende drift og forvaltning av brukernes enheter for å redusere potensielle sårbarheter.

Konfigurering av sikkerhetsfunksjonalitet

Visste du at de fleste bedrifter benytter standard sikkerhetsinnstillinger i Microsoft 365? Dette innebærer at de betaler for sikkerhetsfunksjoner uten å utnytte det fulle potensialet som følger med lisensen, og dermed kan de være sårbare for ulike sikkerhetshendelser.

Microsoft 365 tilbyr et bredt spekter av sikkerhetspolicyer og nivåer som muliggjør beskyttelse mot trusler, sikring av virksomhetens informasjon og beskyttelse av brukernes PC-er og mobile enheter. Dette gjør det også enkelt å administrere sikkerheten. Slike tiltak bidrar til å forhindre phishing, beskytte mot falske lenker, begrense pålogging fra høyrisiko land og mye mer.

Viktig å merke seg er at denne funksjonaliteten krever tilpasning til hver enkelt virksomhet. Hos Advania har vi utviklet beste praksis for konfigurasjon og vedlikehold av disse løsningene. Vi hjelper deg med å velge riktig lisensiering og tilpasse Microsoft 365 effektivt i organisasjonen din. På denne måten maksimerer du nytten basert på virksomhetens spesifikke behov.

Les mer om hvordan du kan løfte virksomheten din til neste nivå med Microsoft 365 og Advania på laget.

3. Etablér en god sikkerhetskultur

Visste du at 90 % av dataangrep forårsakes av menneskelige feil?
Ifølge Nasjonal sikkerhetsmyndighet (NSM) kan 80–90 % av alle dataangrep unngås hvis virksomheten innfører noen få, enkle tiltak. Dette inkluderer tekniske tiltak, som å sørge for at sikkerhetsoppdateringer installeres så fort som mulig, men også tiltak som forbedrer den menneskelige atferden.

God IT-sikkerhet begynner med en solid forankret sikkerhetskultur i virksomheten. For å oppnå dette må du som leder gå foran som et godt eksempel. Som leder har du ansvaret for at alle dine ansatte tar sikkerhet på alvor og viser sunn skepsis når dokumenter og annen intern informasjon skal deles med eksterne parter. I tillegg må det etableres en kultur der det er naturlig å varsle dersom det oppstår mistanker om sikkerhetsbrudd eller uønskede avvik.

En nødvendig og god sikkerhetskultur kan ikke eksistere uten en informasjonsflyt som sikrer at alle ansatte, mellomledere og ledere er på samme nivå. Med andre ord må de ha et felles kunnskapsgrunnlag som de kan basere sine beslutninger og vurderinger på. Sikkerhetskulturen avhenger også av at det finnes gode rutiner og prosesser for hvordan de ansatte skal varsle og hvem de skal kontakte dersom de trenger mer informasjon eller opplæring."

Retningslinjer for deling av informasjon

I tillegg til å ha en solid sikkerhetskultur må du som leder sikre at det er etablert tydelige governance-modeller, retningslinjer og rammeverk for hvordan informasjon skal kommuniseres både internt og eksternt. Det er viktig at sensitive dokumenter håndteres på en måte som sikrer at eksterne brukere ikke får tilgang til dem, selv om dokumentet feilaktig sendes til en feil e-postadresse, og at de blir sensurert ved skjermdeling i Teams. Når alle i virksomheten er kjent med retningslinjene, øker sannsynligheten for at de vil etterleve dem og raskt varsle om eventuelle avvik.

Dette omfatter også hvilke tillatelser og muligheter hver enkelt ansatt har til å redigere, dele og administrere data. Ved å begrense hver enkelt brukers muligheter til å dele informasjon, øker du sikkerheten i virksomheten. Dette kan til og med begrenses ned til dokumentnivå.

4. Intern opplæring og trening

Dersom de ansatte har tilstrekkelig forståelse for hvilke tiltak som er kritiske, hvorfor dette er viktig og hvordan de kan varsle dersom noe ikke er som det skal, vil sikkerheten i virksomheten din øke betraktelig. Derfor er internopplæring et viktig tiltak for å redusere trusselbildet.

I tillegg er det en fordel om de ansatte har en viss forståelse for hvilke angrep de og virksomheten som helhet kan bli utsatt for.

Innføring av nye sikkerhetssystemer og -rutiner kan bringe med seg store og små endringer i sluttbrukernes arbeidshverdag. Frykten for støy som følge av nye rutiner og systemer kan lede til intern motstand mot endringene. Dersom du ønsker gode rutiner og systemer for sikkerhet i din virksomhet, må du lede virksomheten inn i endringen på en god måte.

Som leder er det derfor av vesentlig betydning at du stiller deg bak endringene, bruker systemene aktivt og snakker varmt om nye sikkerhetsrutiner. Dette bidrar til at de ansatte får den kunnskapen de trenger for å unngå fatale brudd og vet hva de skal gjøre om de blir utsatt for et angrep.

Dette kan på mange måter sammenlignes med brannøvelser. Det er ikke veldig sannsynlig at det begynner å brenne i deres lokaler, men det er en selvfølge at dere har rutiner og retningslinjer for hvordan de ansatte skal handle ved brann. Det er ingen grunn til at dere ikke også bør arrangere organiserte øvelser for å teste de ansattes digitale sikkerhetskompetanse.

Et eksempel på en slik test kan være å sende ut en e-post som utgir seg for å være svindel. Hent ut statistikk på hvordan de ansatte behandler e-posten: Hvor mange klikket på lenker og hvor mange oppga sensitiv informasjon? Bruk tallene og eksempelet i internundervisning.

Høy brukeradopsjon

I tillegg til gode sikkerhetsrutiner er det vesentlig at du som leder legger til rette for høy brukeradopsjon.

Selv om brukeren ikke må sette seg inn i nye systemer, vil han eller hun kanskje oppleve at det er visse handlinger som av sikkerhetsmessige grunner ikke lenger lar seg gjøre. Dette kan det være lurt å informere om, gjerne gjennom små videosnutter eller mikrolæring som beskriver hvilken ny funksjonalitet som ligger i Microsoft 365.

Dersom de ansatte ikke bruker de nye løsningene og den tilgjengelige funksjonaliteten, risikerer du at det oppstår en følelse av at ledelsen jobber imot de ansatte ved å tvinge dem til å bruke nye systemer uten god grunn. Høy brukeradopsjon handler med andre ord ikke bare om at endringen faktisk bidrar til at virksomhetens daglige drift blir tryggere, men også om at de ansatte skal fortsette å ha tillit til at ledelsen tar gode avgjørelser.

For å sikre høy brukeradopsjon må endringen få positiv oppmerksomhet ved at fordelene endringene vil føre med seg understrekes og fremheves. Dette må kommuniseres tydelig og med konkrete eksempler. Nedenfor finner du fem gode tips til hvordan du kan sikre høy brukeradopsjon og god innføring av nye verktøy og rutiner.

1. Sett tydelige mål
2. Kommuniser behovet for endringen
3. Tilby opplæring og skap trygge rammer
4. Arranger intensivkurs
5. Identifiser engasjerte ansatte og bruk disse som ambassadører og superbrukere

5. Aktiver flerfaktor-autentisering

I dag lever brukeridentiteten våre overalt på nettet. Det betyr at vi må sikre våre enheter og vår identitet på langt mer avanserte måter enn å beskytte hvert lokale nettverk med en brannmur. Mer enn 80% av identitetsrelatert hacking skyldes svak sikring av brukeridentitet.

Identitet og tilgangsstyring er blant de viktigste sikkerhetsfunksjonalitetene i Microsoft 365.

Den enkleste og mest effektive måten å sikre brukerens identitet på, er å innføre flerfaktor-autentisering for alle systemer. Dette er viktig for å sikre miljøet ditt og kan konfigureres på en måte som tar hensyn til både sikkerhet og brukerproduktivitet.

Kort fortalt handler flerfaktor-autentisering og tilgangsstyring eller autentisering basert på brukeridentitet om at du skal kunne forsikre deg om at brukeren alltid er den vedkommende utgir seg for å være. Dette gjør du ved å koble brukernavn og passord til noe brukeren har, for eksempel ved at påloggingen må godkjennes med en kode, SMS eller en enkel bekreftelse i en app. I tillegg er det mulig å legge på et ekstra lag med sikkerhetsfunksjonalitet ved å også inkludere brukerens lokasjon når påloggingen skal bekreftes.

> "Flerfaktor-autentisering høres ut som noe som burde være bransje-standard, men det er ikke tilfellet i dag. Faktisk er det overraskende få som har konfigurert dette etter Microsoft sine anbefalinger"
>
> - Garzai Ehsas, Microsoft Lead

Grunnen til at så mange virksomheter ikke har innført flerfaktor-autentisering som en standardløsning for sine systemer er hensynet til brukeropplevelse og kostnader. Moderne flerfaktor-autentisering-løsninger er svært smidige, og er en effektiv måte å redusere faren for å bli utsatt for identitetstyveri og sikkerhetsbrudd.

6. Blokker gammel programvareprotokoll

Utdaterte programvareprotokoller refererer til forespørsler fra eldre programvarer som ikke har moderne sikkerhetsmekanismer. Det kan for eksempel være et eldre økonomisystem, eldre Office-klienter som ikke lenger oppdateres med den nyeste programvaren eller utdaterte e-postsystemer på mobilen.

– Eldre programvareprotokoller støtter blant annet ikke flerfaktor-autentisering og er derfor en sentral kilde til sikkerhetshull hos mange norske virksomheter, forteller Ehsas.

Ifølge Microsoft kommer majoriteten av kompromitterende innloggingsforsøk fra slik programvareprotokoll som ikke støtter flerfaktor-autentisering.

> Den vanligste årsaken til sikkerhetsbrudd er at det er mulig å prøve uendelig mange brukernavn- og passordkombinasjoner via dette «hullet», sier Thomas Coll, senior Cloud konsulent i Advania.

Den beste måten å forhindre slike sikkerhetshull på er å blokkere forsøkene en gang for alle via sikkerhetssystemene i Microsoft Azure, noe Advania kan hjelpe deg med. For brukernes del gjelder det å sørge for å alltid ha oppdatert programvare og operativsystemer. Det å oppdatere programvare og operativsystemer kan ansees som et forebyggende tiltak mot sikkerhetsbrudd og dataangrep.

7. Moderne sikkerhetsrammeverk

Mangel på et moderne rammeverk for sikkerhet øker risikoen for at du blir utsatt for et sikkerhetsbrudd eller angrep. Et eksempel på et moderne sikkerhetsrammeverk er Zero Trust-prinsippet.

I vår digitale hverdag handler ikke sikkerhet lenger om brannmurer og antivirusprogrammer, men om å muliggjøre fleksibilitet og innovasjon – uten at det går på bekostning av sikkerheten. Med Microsoft 365 kan du etablere et rammeverk som muliggjør nettopp dette.

For å gi deg noen eksempler på hvordan et slikt rammeverk kan bidra til å redusere virksomhetens trusselnivå har vi trukket frem to funksjonaliteter i Microsoft 365:

- Defender for Office
- Defender for Endpoint

Microsoft Defender for Office er en skybasert tjeneste som filtrerer dine filer og på den måten bidrar til å forhindre at potensielt skadelig programvare og virus får tilgang til ditt nettverk, dine servere og enheter. Det vil si at filer i SharePoint, OneDrive og Teams, samt e-postvedlegg skannes for skadelig kode og låser ondsinnede filer for brukeren. Dette er noen av de angrepsflatene kriminelle som oftest benytter seg av. Derfor er det viktig å forsøke å hindre dem i å plassere skadelig innhold på dine servere.

Det er i tillegg mulig å konfigurere en funksjonalitet som forhindrer at en e-postadresse som ligner på en av VIP-brukerne dine blir levert internt. Disse e-postene havner heller i søppelpostmappen merket med en etikett med etterligningsinformasjon. Dette bidrar i stor grad til å redusere faren for å bli utsatt for phishing og direktørsvindel..

Microsoft Defender for Endpoint beskytter dine ansattes enheter. Fysiske brannmurer på virksomhetens nettverk gir ikke lenger tilstrekkelig sikkerhet når de ansatte stadig oftere jobber fra andre lokaliteter eller på farten.

Defender for Endpoint er også en skybasert tjeneste som gjør det mulig for din IT-avdeling å oppdage sårbarheter i realtid gjennom trusselmonitorering og –analyser. Tjenesten gjør at den innebygde anti-virus-løsningen man har i Windows 10/11, Defender, nå blir sentralt styrt fra Microsoft 365-skyen din. Dermed er det enkelt for avdelingen å handle raskt når en alarm går og skalere sikkerhetstiltakene slik at deres forretningskritiske informasjon til enhver tid er beskyttet.

Microsoft Defender

8. Vurder verdiøkende sikkerhetstjenester

Selv om det finnes en rekke god sikkerhets funksjonalitet i Microsoft 365, bør alle virksomheter vurdere tilleggstjenester for å få en best mulig ende-til-ende sikkerhet.

Backup og restore

Stadig flere virksomheter opplever å bli utsatt for sikkerhetsbrudd og sikkerhetskopiering av kritiske filer og informasjon er viktigere enn noen gang. Sikre deg med en god backupløsning, og sørg for at den blir rutinemessig vedlikeholdt og kontrollert. Dette reduserer konsekvensen av en eventuell sikkerhetshendelse betydelig, da det gir deg mulighet til å raskt gjenopprette virksomhetens data, også hvis de blir infisert.

Ved å investere i gode backup-løsninger sørger du ikke bare for at viktig informasjon ikke går tapt, du sørger også for at varigheten av en eventuell driftsstans reduseres betraktelig.

Det finnes mange eksempler på virksomheter som har vært oppe og kjørt som normalt igjen, kun få timer etter å ha blitt angrepet av kryptovirus, takket være gode backuprutiner og et pålitelig system.

Sikre deg tilgang til kompetanse og bistand

Det kan være kostbart å ha all kompetanse tilgjengelig i eget hus. Det finnes en rekke gode tjenester som senker terskelen for å ha et kontinuerlig og proaktivt fokus på å holde trusselbildet nede, og sikre deg tilgang til riktig kompetanse dersom en hendelse skulle inntreffe.

Et eksempel på en slik tjeneste er å inngå en avtale med et Security Operations Center, også kalt en SOC-tjeneste. Dette er en tjeneste som blant annet kan detektere unormal atferd knyttet til brukere, kontoer og prosesser, før en sikkerhetshendelse finner sted.

SOC-tjeneste

En SOC-tjeneste gir deg tilgang på et team av eksperter som vil håndtere og mitigere alle sikkerhetsrelaterte hendelser, samtidig som de holder deg og din virksomhet løpende orientert gjennom hendelsen. Dersom du har en IT-partner som ivaretar denne funksjonen, vil virksomhets infrastruktur og brukere være i trygge hender gjennom hele året. Du vil i tillegg kunne motta faste månedlige rapporter knyttet til alle sikkerhetsrelaterte hendelser samt få anbefalinger om relevante sikkerhetstiltak.

Med stadig mer sofistikerte angrepsmetoder er det mye som tyder på at en SOC-tjeneste er fremtidens måte å forhindre og håndtere angrep på. En slik tjeneste vil først og fremst kunne hindre at angrepet finner sted i det hele tatt, men også sikre at kompetent sikkerhetspersonell håndterer en eventuell situasjon.

Hva venter du på?

Ta kontroll på IT-sikkerheten i din virksomhet.

Kontakt oss

advania

The tech company
with people at heart

advania.no