Topp 10 sikkerhetstiltak i 2024

Denne topp 10 listen gjelder bedrifter som benytter Microsoft sine skyløsninger som Teams, OneDrive, Sharepoint og Office.

1. Sterke autentiseringsmetoder, minst to faktorer er 100% påkrevd i dag
2. Backup av dine skydata er ikke en del av tjenesten fra skyleverandøren, sørg for å ha regelmessig ekstern backup av dette
3. Utvidet antivirus med EDR, enten via utvidet Microsoft-lisens eller via 3.part.
4. Brannmur med lisens for sikring mot angrep på bedriftens utstyr
5. Sikker nettverkskonfigurasjon for sikring mot infiserte enheter i bedriften
6. Hold all programvare på alle maskiner oppdatert, ikke bare programvare fra Microsoft
7. Opplæring av ansatte til å motstå phishing
8. Benytt Microsoft Secure Score som et målbilde på din sky-sikkerhet
9. Implementer Signin-risk policies og User-risk policies for å hinder angripere å benytte kompromitterte kontoer
10. Implementere sikkerhetsregler og -prosedyrer

1. **Sterke autentiseringsmetoder**
   Sterke autentiseringsmetoder gir økt sikkerhet ved å legge til ekstra lag med beskyttelse utover bare brukernavn og passord. Her er noen fordeler med sterke autentiseringsmetoder:
   a. Sterke autentiseringsmetoder gir et ekstra sikkerhetslag, noe som gjør det vanskeligere for uautoriserte personer å få tilgang til kontoer selv om passordet skulle bli kompromittert.
   b. I tilfelle at brukerens passord blir kompromittert gjennom phishing, lekkasje eller andre angrep, gir sterke autentiseringsmetoder et ekstra hinder for angripere.
   c. Bedrifter som bruker sterke autentiseringsmetoder kan opprettholde sikrere forretningsprosesser og beskytte sensitive data og tjenester.
   d. Sterke autentiseringsmetoder er ofte nødvendige for å oppfylle sikkerhetsstandarder og forskrifter, spesielt i bransjer som håndterer sensitive data (for eksempel personopplysninger, finansiell informasjon eller helseinformasjon).
   e. MFA gir ekstra beskyttelse selv om brukeren bruker samme passord på flere steder, fordi angriperen likevel trenger den ekstra autentiseringsfaktoren.

   I sum gir sterke autentiseringsmetoder en robust og effektiv løsning for å forhindre uautorisert tilgang og beskytte sensitive data og ressurser. Det er derfor sterkt anbefalt å implementere slike metoder for å styrke sikkerheten i digitale identiteter og systemer.

2. **Backup av dine skydata**
   Backup av dine skydata er noe mange tar for gitt at er inkludert i skytjenesten de betaler lisenser for, som f.eks. Microsoft 365. Microsoft sier selv at de står for tjenestene mens dataene er ditt ansvar. Derfor bør alle som benytter seg av Microsoft sine skytjenester ordne en ekstern backup av disse dataene.
   a. Ekstern backup gir en sikkerhetskopi av dataene dine i tilfelle tap eller utilsiktet sletting. Dette vil være avgjørende for å gjenopprette viktig informasjon som er gått tapt på grunn av feil, angrep eller andre uforutsette hendelser.
   b. Hvis du blir utsatt for ransomware eller andre sikkerhetsbrudd, kan en ekstern backup gi en isolert kopi av dataene som ikke er tilgjengelig for angriperen. Dette gjør det lettere å gjenopprette data uten å betale løsepenger. Løsepenger hjelper i bare noen få tilfeller, og mange bedrifter har brukt flere årsverk på å selv generere dataene på nytt selv.
   c. Det å ha en ekstern backup av skydata er en god praksis for datasikkerhet og kan være nødvendig for å overholde bransje- og regulatoriske krav, spesielt når det gjelder lagring og sikring av data.
   d. Eksterne backupløsninger gir vanligvis en enkel gjenopprettingsprosess. Dette gjør det raskt og enkelt å hente dataene dine etter et tap, enten det er på grunn av feil, korrupte filer eller andre problemer.
   e. Ved å opprettholde en ekstern backup, er du ikke fullstendig avhengig av sikkerhetstiltakene som tilbys av skytjenesteleverandøren din. Dette gir en ekstra sikkerhetskopi som du har kontroll over.
   f. Mange eksterne backupløsninger tilbyr versjonskontroll, noe som betyr at du kan gjenopprette dataene dine til tidligere punkter i tid. Dette er nyttig hvis du oppdager tap eller feil en stund etter at de har skjedd.
   g. Med en rask gjenopprettingsprosess kan ekstern backup bidra til å minimere nedetid etter tap av data. Dette er spesielt viktig for forretningskritiske applikasjoner og tjenester.

3. **Utvidet antivirus med EDR**
   Antivirus med Endpoint Detection and Response (EDR) kombinerer tradisjonell antivirusbeskyttelse med avansert trusseloppdagelse og responsfunksjoner. Her er noen fordeler med å implementere antivirusløsninger som inkluderer EDR:
   a. EDR gir avansert trusseloppdagelse ved å analysere aktiviteter og oppførsel på endepunkter. Dette gjør det mulig å identifisere trusler før de kan forårsake skade.
   b. Mange EDR-løsninger inkluderer automatiserte responsfunksjoner som lar organisasjoner raskt isolere berørte systemer, blokkere skadelig aktivitet og minimere risikoen for spredning.
   c. EDR bidrar til raskere gjenoppretting etter et sikkerhetsbrudd ved å gi verktøy for å isolere, sanere og gjenopprette berørte endepunkter og systemer.
   d. Tradisjonelle antivirusløsninger kan ha begrensninger når det gjelder å oppdage avanserte trusler. EDR bruker avansert analyse for å identifisere og håndtere sofistikerte angrep som kan omgå tradisjonelle signaturbaserte metoder.
   e. EDR overvåker kontinuerlig endepunkters oppførsel for å identifisere unormale aktiviteter som kan indikere et potensielt angrep. Dette gjør det mulig å handle raskt før skaden skjer.
   f. EDR bruker heuristiske og atferdsbaserte analyser for å oppdage ukjente og potensielt skadelige trusler, inkludert zero-day-angrep som ikke har kjente signaturer.

g. Sammen med antivirus gir EDR en helhetlig tilnærming til endepunktsbeskyttelse, som dekker både forebygging og respons. Dette er spesielt viktig i dagens komplekse trusselbilde.

4. **Brannmur med lisens**
   Når vi snakker om en brannmur med lisens, refererer vi til en brannmurløsning som krever en gyldig lisens for å aktivere og bruke de mest avanserte funksjonene. I dag er dette noe som alle bedrifter bør ha, da tradisjonelle brannmurer er enklere å få kontroll på for angripere.
   a. Leverandører av lisensierte brannmurer arbeider kontinuerlig med å forbedre produktene sine. Ved å ha en aktiv lisens, kan du dra nytte av regelmessige programvareoppdateringer og nye funksjoner som bidrar til å styrke sikkerheten over tid.
   b. Med en lisensiert brannmur får du tilgang til kontinuerlige sikkerhetsoppdateringer og patches fra leverandøren. Dette sikrer at brannmuren er oppdatert med de nyeste sikkerhetsforbedringene for å beskytte mot kjente trusler.
   c. Lisensierte brannmurer gir ofte tilgang til et bredt spekter av funksjoner og verktøy som kan være avgjørende for å sikre nettverket ditt. Dette kan inkludere innbruddsbeskyttelse, VPN-støtte, innholdsfiltrering, og mer avanserte sikkerhetsfunksjoner.
   d. Lisensierte brannmurer kan integrere trusselintelligens og oppdateringer fra leverandørens sikkerhetsnettverk. Dette gir informasjon om de nyeste truslene og hjelper brannmuren med å identifisere og blokkere disse truslene i sanntid.
   e. Noen bransjer og samsvarskrav kan kreve bruk av lisensierte og sertifiserte sikkerhetsprodukter. Ved å bruke en brannmur med gyldig lisens, kan du lettere oppfylle slike krav.

5. **Sikker nettverkskonfigurasjon**
   Implementeringen av en sikker nettverkskonfigurasjon er en integrert del av en helhetlig sikkerhetsstrategi og bidrar til å styrke organisasjonens motstandsdyktighet mot stadig mer sofistikerte trusler og angrep.
   a. En sikker nettverkskonfigurasjon bidrar til å minimere angrepsflaten ved å begrense unødvendige tjenester, porter og protokoller. Dette reduserer mulighetene for angrep og utnyttelse.
   b. Ved å implementere sikre nettverkskonfigurasjoner, for eksempel VLAN, sikkerhetsgrupper og andre sikkerhetstiltak, blir nettverket mer motstandsdyktig mot ulike typer angrep, inkludert inntrengingsforsøk og malware-spredning.
   c. Sikre nettverkskonfigurasjoner kan inkludere tiltak for å beskytte mot distribuerte tjenestenektangrep (DDoS-angrep), som kan forsøke å overbelaste nettverket for å gjøre det utilgjengelig.
   d. Sikre nettverkskonfigurasjoner legger vekt på kryptering av kommunikasjon. Dette sikrer at dataene som sendes over nettverket, for eksempel brukernavn og passord, er beskyttet mot avlytting.
   e. Sikre nettverkskonfigurasjoner hjelper organisasjoner med å oppfylle samsvarskrav og reguleringer ved å implementere nødvendige sikkerhetskontroller og beskyttelsesmekanismer.

6. **Hold all programvare på alle maskiner oppdatert**
   Å holde programvaren oppdatert er en viktig praksis for å styrke datasikkerheten, forbedre systemets stabilitet og ytelse, og sikre at organisasjonen holder tritt med de stadig skiftende sikkerhetsutfordringene og teknologiske fremskrittene.
   a. Oppdateringer inkluderer ofte sikkerhetsrettelser som tetter kjente sårbarheter. Å holde programvaren oppdatert bidrar til å beskytte systemene mot potensielle trusler og angrep.
   b. Oppdaterte programvareversjoner kan inkludere signaturer og heuristikk som gir bedre beskyttelse mot nye former for malware og skadelig programvare.
   c. Oppdateringer inneholder ofte feilrettinger og ytelsesforbedringer. Dette bidrar til å opprettholde systemstabilitet og optimal ytelse.
   d. Oppdateringer kan også inkludere støtte for ny maskinvare. Dette er spesielt viktig for å sikre at eldre programvare er kompatibel med nye enheter og teknologier.
   e. Oppdateringer kan introdusere nye funksjoner og forbedringer, noe som gir brukerne økt funksjonalitet og bedre brukeropplevelse.
   f. Oppdatering av programvaren er ofte nødvendig for å overholde bransje- og regulatoriske sikkerhetsstandarder. Dette er spesielt relevant i bransjer som håndterer sensitive data.
   g. Uutnyttede sårbarheter i programvare utgjør en risiko. Oppdatert programvare reduserer denne risikoen ved å lukke potensielle sikkerhetshull.
   h. Når all programvare er oppdatert, bidrar det til å bygge en robust og helhetlig sikkerhetsinfrastruktur, reduserer angrepsflaten og gir bedre beskyttelse mot trusler.

7. **Opplæring av ansatte til å motstå phishing**
   Opplæring av ansatte for å motstå phishing-angrep er en avgjørende faktor, da ansatte ofte er en første forsvarslinje mot denne typen trusler.
   a. Opplæring gir ansatte kunnskap om hvordan phishing-angrep ser ut og hvordan de fungerer. Dette reduserer sårbarheten mot å falle for falske e-poster, meldinger eller nettsteder.
   b. Opplæring gir ansatte ferdigheter til å identifisere vanlige indikatorer på phishing, som uventede e-postadresser, feilstavede ord, mistenkelige lenker og forespørsler om sensitive opplysninger.
   c. Ansattes kunnskap om phishing bidrar til å styrke deres generelle cyberhygiene. Dette inkluderer å være forsiktig med ukjente e-poster, bekrefte identiteten til avsendere og unngå å klikke på tvilsomme lenker.
   d. Phishing er ofte inngangsporten for mange sikkerhetsbrudd. Opplæring reduserer risikoen for at ansatte blir offer for phishing, noe som igjen minimerer sjansene for vellykkede angrep.
   e. Opplærte ansatte er bedre i stand til å identifisere mistenkelige aktiviteter tidlig. Jo tidligere dette oppdages, jo raskere kan organisasjonen reagere for å begrense skaden ved et phishing-angrep.
   f. Opplæring bidrar til å skape en kultur med fokus på sikkerhet blant de ansatte. Dette fører til en mer proaktiv tilnærming til å identifisere og håndtere potensielle sikkerhetstrusler.
   g. Mange bransje- og regulatoriske standarder krever nå opplæring av ansatte som en del av organisasjonens sikkerhetspraksis. Opplæringen hjelper organisasjonen med å overholde slike krav.

Samlet sett gir opplæring av ansatte for å motstå phishing ikke bare umiddelbare fordeler ved å redusere risikoen for phishing-angrep, men bidrar også til å bygge en sterkere sikkerhetskultur innen organisasjonen.

8. **Benytt Microsoft Secure Score som et målbilde på din sky-sikkerhet**
   Microsoft Secure Score er et verktøy fra Microsoft som gir organisasjoner en måte å vurdere og forbedre sikkerhetsnivået i deres Microsoft 365-miljø.
   a. Microsoft Secure Score gir en tydelig sikkerhetsvurdering og et målbilde for organisasjonens sikkerhetsnivå i Microsoft 365. Dette gir et klart bilde av hvor organisasjonen står i forhold til beste praksis.
   b. Secure Score identifiserer spesifikke sikkerhetssvakheter og risikoer i organisasjonens konfigurasjon av Microsoft 365. Dette gjør det enklere å fokusere på områder som krever forbedring.
   c. Verktøyet gir prioriteringsanbefalinger basert på risiko og potensielle trusler. Dette hjelper organisasjonen med å fokusere på de mest kritiske sikkerhetstiltakene først.
   d. Secure Score sammenligner organisasjonens sikkerhetsnivå med beste praksis og bransjestandarder. Dette gir en referanse for hvor godt organisasjonen oppfyller sikkerhetsstandarder.
   e. Secure Score er dynamisk og oppdateres regelmessig med nye anbefalinger og beste praksis. Dette oppmuntrer til kontinuerlig forbedring av sikkerheten over tid.
   f. Organisasjoner kan måle progresjonen av sikkerhetsforbedringer ved å regelmessig overvåke endringer i Secure Score. Dette gir innsikt i effektiviteten av implementerte sikkerhetstiltak.
   g. For organisasjoner som må overholde spesifikke sikkerhetsstandarder og forskrifter, hjelper Secure Score med å identifisere og styrke samsvarsområder.
   h. Secure Score gir en plattform for å kommunisere sikkerhetsstatusen og forbedringene til ledelsen og interessenter, og det øker transparensen rundt sikkerhetsforhold.

   Implementeringen av Microsoft Secure Score som et målbilde for sky-sikkerhet gir organisasjoner praktiske retninger for å styrke sikkerheten i Microsoft 365-miljøet og øke den generelle motstandsdyktigheten mot cybertrusler.

9. **Implementer Signin-risk policies og User-risk policies**
   Implementering av Sign-in risk policies og User risk policies er viktige tiltak for å styrke sikkerheten i en organisasjons digitale miljø. Disse retningslinjene er en del av Identity and Access Management (IAM) og Conditional Access.
   a. Sign-in risk policies gir muligheten til å identifisere mistenkelige påloggingsforsøk eller atferd. Dette gjør det mulig å reagere tidlig på potensielle sikkerhetsbrudd.
   b. Basert på risikoen knyttet til et påloggingsforsøk, kan sign-in risk policies utløse behovet for sterkere autentiseringsmetoder. Dette styrker sikkerheten ved å kreve ekstra bekreftelse ved høy risiko.
   c. Ved høy risiko kan sign-in risk policies automatisere responsmekanismer, for eksempel midlertidig blokkering av kontoen eller varsler til sikkerhetsteamet.
   d. Policies for påloggingsrisiko gir mulighet for å oppdage unormale aktiviteter, for eksempel pålogging fra ukjente geografiske områder eller på unormale tidspunkter.

e. User risk policies evaluerer risikoen knyttet til den enkelte brukeren. Dette gir mulighet for dynamisk tilpasning av sikkerhetstiltak basert på brukerens risikonivå.
f. Policies for brukeratferdsrisiko bidrar til å beskytte mot kompromitterte kontoer ved å oppdage mistenkelig aktivitet som kan indikere uautorisert tilgang.
g. Ved høy risiko kan user risk policies automatisere responsmekanismer, som midlertidig blokkering av kontoen eller endring av brukerens tilgangsnivå.
h. Policies for brukeratferdsrisiko hjelper med å identifisere avanserte trusler som kan omgå tradisjonelle sikkerhetstiltak ved å fokusere på brukerens atferd og mønstre.
i. Policies for brukeratferdsrisiko kan hjelpe organisasjonen med å overholde sikkerhetsstandarder og reguleringer ved å implementere ekstra sikkerhet for risikoutsatte brukere.

Implementeringen av Sign-in risk policies og User risk policies er avgjørende for å oppnå en adaptiv og proaktiv tilnærming til sikkerhet, der risikobaserte beslutninger tas i sanntid for å beskytte organisasjonens digitale ressurser og data.

10. Implementere sikkerhetsregler og -prosedyrer

Utvikle og håndheve klare sikkerhetsregler og -prosedyrer, og sikre at alle i organisasjonen er klar over dem.

a. Dataklassifiserings- og beskyttelsespolicy er en måte å merke bedriftens dokumenter med en grad av konfidensialitet. Bedriften må først lage regler for hva som skal trigge de forskjellige gradene innen dataklassifiseringen. Deretter må regler for dette opprettes i skyløsningen. Til slutt må brukerne læres opp, og instrueres i hvordan dette skal brukes.
b. Regler for kommunikasjon med eksterne bør nedfelles. Dette bør gjelde i alle kommunikasjonsformer som benyttes i bedriften. Brukerne må lære disse reglene og følge disse i sin daglige kommunikasjon. Et eksempel kan være at ansatte skal være oppmerksomme på personvern og konfidensialitet når de kommuniserer eksternt, og at de må unngå deling av sensitiv informasjon uten riktig godkjenning.
c. Ansatte skal gjennomgå regelmessig opplæring om sikkerhetsbevissthet for å identifisere og unngå potensielle trusler gjennom ekstern kommunikasjon. Dette er med på å redusere risikoen for phishing-angrep.
d. Epost er fortsatt en av de kommunikasjonskanalene med flest phishing-forsøk. Sikker bruk av epost bør derfor være en prioritert oppgave i enhver bedrift. Dette inkluderer konfigurasjoner i epost-tjenesten, men også opplæring av ansatte, samt etablering av regler og prosedyrer for epost-kommunikasjon.

Sikkerhetstiltakene i denne listen må sees på som noen av de viktigste tiltakene for mange bedrifter, men ikke nødvendigvis alle. Avhengig av oppsett, bruk og konfigurasjoner kan det være andre tiltak som må vurderes. Uansett vil tiltakene i denne listen være viktige tiltak for de aller fleste som benytter seg av Microsoft sine skyløsninger.