Microsoft 365 Security Assessment Advanced

En gjennomgang av virksomhetens sikkerhetsrisikoer

Når foretok du sist en sikkerhetsgjennomgang? Kjenner du til de grunnleggende sikkerhetskravene? Benytter du Secure Score for å få kunnskap om sikkerhet? Sikkerhet blir en stadig viktigere faktor for alle virksomheter som allerede jobber hundre prosent digitalt eller er på vei dit. Samtidig øker kompleksiteten og risikoene når alt er oppkoblet. Derfor er det viktigere enn noen gang å ha en integrert tilnærming til sikkerhet.

Microsoft 365 Security Assessment Advanced hjelper deg med å få oversikt over virksomhetens risikoer og behov når det gjelder sikkerhetsarbeidet knyttet til Microsofts produktportefølje. Gjennomgangen vil hjelpe deg med å identifisere og planlegge for sikre identiteter og sikker lagring av data og informasjon, applikasjoner, klienter og øvrig IT-infrastruktur. Den gir et øyeblikksbilde av IT-miljøet knyttet til Microsoft 365 (tidligere Office 365) og nåværende risikoer, slik at du kan håndtere dem på en strukturert og sikker måte og jobbe mer proaktivt i fremtiden.

Hva er forskjellen mellom Essentials og Advanced?
I Microsoft 365 Security Assessment Essentials gjennomgår vi virksomhetens grunnleggende sikkerhet, mens Microsoft 365 Security Assessment Advanced innebærer en betydelig mer omfattende analyse.

Hva får du ut av Microsoft 365 Security Assessment Advanced?

- En tydelig rapport som beskriver virksomhetens risikoer og sikkerhetsbehov
- Et bilde av hvordan vi kan hjelpe deg med å styrke sikkerhetsarbeidet
- Anbefalinger og tid med sikkerhetsekspertene våre

Hvordan?

1 **Oppstartsmøte**
Vi lager en felles tidsplan, synkroniserer forventninger til prosjektet og identifiserer interessenter hos oss og hos dere. Vi starter dessuten gjennomgangen med en undersøkelse som vi fyller ut sammen.

2 **Gjennomgang**
Vi fortsetter med mer utførlige spørsmål og gjennomgår Security Score, Shadow IT, Office 365 ATP, Windows Security og Attack Simulator. Vi installerer dessuten tjenestene som kreves for datainnsamlingen som ligger til grunn for rapporten. Datainnsamlingen pågår i minst to uker. Vi vurderer virksomhetens gjeldende sikkerhetsstatus, og du lærer mer om hvordan du beskytter virksomhetens enheter og e-postløsning, multifaktorautentisering, autentiseringsmetoder, passordpolicyer, håndtering av eksterne brukere, innlogginger, rettigheter og sikker fildeling.

3 **Rapport og veikart**
Etter at den tekniske analysen er foretatt, sammenstiller vi de ulike delene av gjennomgangen. Deretter kommer vi med anbefalinger og forslag til tiltak (i prioritert rekkefølge) som vi ser behov for å iverksette for å tette hullene vi har funnet. Her får du også anledning til å sitte ned med ekspertene våre og få en grundig gjennomgang av funnene deres.