Microsoft 365 Security Assessment Advanced

En gennemgang af din virksomheds sikkerhedsrisici

Hvornår har du sidst gennemført en sikkerhedsgennemgang? Har du styr på de nye grundlæggende krav til sikkerheden? Bruger du Secure score til at få indsigt i sikkerheden? Sikkerhed bliver en stadigt vigtigere faktor for alle virksomheder, der allerede arbejder helt digitalt eller er på vej hen imod det. Samtidig øges kompleksiteten og risiciene, når alt er forbundet. Derfor er det vigtigere end nogensinde at have et integreret syn på sikkerhed.

Microsoft 365 Security Assessment Advanced hjælper jer med at få et overblik over de risici og behov, I som virksomhed har, når det handler om sikkerhedsarbejdet i forbindelse med Microsofts produktportefølje. Gennemgangen hjælper med at identificere og planlægge sikre identiteter, sikker lagring af data og informationer, applikationer, klienter og anden IT-infrastruktur. Den giver et øjebliksbillede af IT-miljøet i forbindelse med Microsoft 365 (tidligere Office 365) og de nuværende risici, så du på en struktureret og sikker måde kan håndtere dem og arbejde mere proaktivt i fremtiden.

Hvad er forskellen på Essentials og Advanced?
I Microsoft 365 Security Assessment Essentials gennemgår vi din virksomheds grundlæggende sikkerhed, mens vi i Microsoft 365 Security Assessment Advanced foretager en langt mere omfattende gennemgang.

Hvad får du ud af Microsoft 365 Security Assessment Advanced?

- En tydelig rapport, der beskriver din virksomheds risici og sikkerhedsbehov
- Et billede af, hvordan vi kan hjælpe dig med at styrke sikkerheden
- Anbefalinger og tid med vores sikkerhedseksperter

Hvordan foregår det?

1 Opstartsmøde
Vi lægger en fælles tidsplan, afstemmer forventningerne til projektet og identificerer interessenter hos os og hos jer. Vi påbegynder også gennemgangen ved hjælp af en undersøgelse, som vi udfylder i fællesskab.

2 Gennemgang
Vi fortsætter med en række mere dybdegående spørgsmål og gennenmgår Security Score, Shadow IT, Office 365 ATP, Windows Security og Attack simulator. Vi installerer også de tjenester, der er nødvendige for den dataindsamling, der ligger til grund for rapporten. Dataindsamlingen tager mindst to uger. Vi evaluerer virksomhedens aktuelle sikkerhedsstatus, og du får mere at vide om, hvordan du sikrer virksomhedens enheder og e-mailløsning, multifaktorgodkendelse, godkendelsesmetoder, adgangskodepolitikker, håndtering af eksterne brugere, logins, tilladelser og sikker fildeling.

3 Rapport og køreplan
Når dataindsamlingen er gennemført, sammenholder vi de forskellige dele af gennemgangen. Derefter udarbejder vi anbefalinger og forslag til tiltag (med prioriteringsrækkefølge), som vi mener skal gennemføres for at lukke de huller, vi har fundet. Her får du også tid til at sætte dig sammen med vores eksperter og få en grundig gennemgang af deres resultater.