Microsoft 365 Security Assessment Advanced

En genomgång av din verksamhets säkerhetsrisker

När genomförde du en säkerhetsgenomgång senast? Har du koll på de grundläggande säkerhetskraven? Använder du Secure score för att få säkerhetsinsikter? Säkerhet blir en allt viktigare faktor för alla verksamheter som redan jobbar helt digitalt eller är på väg dit. Samtidigt ökar komplexiteten och riskerna när allting är uppkopplat. Att ha en integrerad syn på säkerhet är därför viktigare än någonsin tidigare.

Microsoft 365 Security Assessment Advanced hjälper dig att överblicka de risker och behov din verksamhet har när det kommer till säkerhetsarbetet kopplat till Microsofts produktportfölj. Genomgången hjälper dig att identifiera och planera för säkra identiteter, säker lagring av data och information, applikationer, klienter och övrig IT-infrastruktur. Den ger dig även en ögonblicksbild av IT-miljön kopplat till Microsoft 365 (tidigare Office 365) och nuvarande risker för att du på ett strukturerat och säkert sätt skall kunna åtgärda dem och arbeta mer proaktivt i framtiden.

Vad är skillnaden mellan Essentials och Advanced?

I Microsoft 365 Security Assessment Essentials går vi igenom din verksamhets grundläggande säkerhet medan vi i Microsoft 365 Security Assessment Advanced gör en betydligt mer omfattande genomlysning.

Vad får du ut av Microsoft 365 Security Assessment Advanced?

- En tydlig rapport som beskriver din verksamhets risker och säkerhetsbehov
- En bild av hur vi kan hjälpa dig att stärka upp säkerhetsarbetet
- Rekommendationer och tid med våra säkerhetsexperter

Hur går det till?

1 Uppstartsmöte
Vi sätter en gemensam tidsplan, synkar förväntningar på projektet och identifierar stakeholders hos oss och hos er. Vi sätter även igång genomgången med hjälp av en undersökning som vi fyller i tillsammans.

2 Genomgång
Vi fortsätter med ett utförligare frågebatteri och går igenom Security Score, Shadow IT, Office 365 ATP, Windows Security och Attack simulator. Vi installerar även de tjänster som behövs för den datainsamling som ligger till grund för rapporten. Datainsamlingen pågår minst två veckor. Vi utvärderar din verksamhets aktuella säkerhetsstatus och du får lära dig mer om hur du säkrar upp verksamhetens enheter och e-postlösning, multifaktorautentisering, autentiseringsmetoder, lösenordspolicyer, hantering av externa användare, inloggningar, behörigheter och säker fildelning.

3 Rapport och roadmap
Efter att datainsamlingen är genomförd sammanställer vi de olika delarna av genomgången. Sedan tar vi fram rekommendationer och förslag på åtgärder (med prioriteringsordning) som vi ser skulle behöva genomföras för att täppa till de gap vi hittat. Här får du också tid att slå dig ner med våra experter för att grundligt gå igenom vad de hittat.