Microsoft 365 Security Assessment Advanced

Katsaus yrityksesi tietoturvariskeihin

Milloin teit viimeksi tietoturvakatsauksen? Tunnetko yleiset tietoturvavaatimukset? Käytätkö Secure Score -pisteytystä tietoturvatietojen saamiseksi? Tietoturvasta huolehtiminen yhä tärkeämpää kaikille yrityksille, jotka työskentelevät jo täysin digitaalisesti tai ovat siirtymässä digitaaliseen työskentelytapaan. Mutta kun kaikki on yhteydessä verkkoon, myös monimutkaisuus ja riskit kasvavat. Siksi on tärkeämpää kuin koskaan, että yrityksillä on kokonaisvaltainen näkemys tietoturva-asioista.

Microsoft 365 Security Assessment Advanced auttaa sinua saamaan yleiskuvan yrityksesi riskeistä ja tarpeista koskien Microsoftin tuotevalikoimaan liittyvää tietoturvatyötä. Katsaus auttaa sinua tunnistamaan luotettavat identiteetit, tietojen turvalliset tallennustavat sekä sovellusten, päätteiden ja muun IT-infrastruktuurin turvalliset hallintatavat. Se antaa myös tilannekuvan Microsoft 365:een (aiemmin Office 365) liittyvästä IT-ympäristöstä ja nykyisistä riskeistä, jotta voit korjata ne strukturoidusti ja turvallisesti sekä työskennellä jatkossa aiempaa ennakoivammin.

Mitä eroa on Essentialsin ja Advancedin välillä?
Microsoft 365 Security Assessment Essentialsissa käymme läpi yrityksesi yleisen tietoturvan, kun taas Microsoft 365 Security Assessment Advancedissa teemme huomattavasti kattavamman läpikäynnin.

Mitä etuja Microsoft 365 Security Assessment Advanced tarjoaa?

- Selkeä raportti, jossa kuvataan yrityksesi riskit ja tietoturvatarpeet
- Kuva siitä, miten voimme auttaa sinua vahvistamaan tietoturvatyötä
- Suosituksia ja apua turvallisuusasiantuntij oiltamme

Miten tämä toimii?

1 **Alkutapaaminen**
Asetamme yhteisen aikataulun, synkronoimme projektia kohtaan asetetut odotukset ja tunnistamme sidosryhmät kummallakin puolella. Vastaamme myös yhdessä kyselyyn, joka toimii katsauksen aloituspisteenä.

2 **Katsaus**
Jatkamme yksityiskohtaisemmalla kysymyssarjalla ja käymme läpi Security Scoren, Shadow IT:n, Office 365 ATP:n, Windows Securityn ja Attack Simulatorin. Asennamme myös raportin perustana olevien tietojen keräämisen edellyttämät palvelut. Tietojen kerääminen kestää vähintään kaksi viikkoa. Arvioimme yrityksesi nykyisen tietoturvatilanteen. Saat lisätietoja yrityksen laitteiden ja sähköpostiratkaisun suojaamisesta, monivaiheisesta todennuksesta, todennusmenetelmistä, salasanakäytännöistä, ulkoisten käyttäjien hallinnasta, kirjautumisista, käyttöoikeuksista ja turvallisesta tiedostojen jakamisesta.

3 **Raportti ja tiekartta**
Tietojen keräämisen jälkeen kokoamme yhteen katsauksen eri osat. Sen jälkeen laadimme suosituksia ja ehdotuksia toimenpiteistä (tärkeysjärjestyksessä), jotka meidän mielestämme olisi toteutettava havaittujen puutteiden täyttämiseksi. Voit myös käydä löydetyt asiat perusteellisesti läpi asiantuntijoidemme kanssa.