Microsoft 365 Security Assessment

Wil je zeker weten dat jouw organisatie is opgewassen tegen potentiële aanvallen en cyberbedreigingen? Maak dan gebruik van de Microsoft 365 Security Assessment.

Met de Microsoft 365 Security Assessment brengen we mogelijke risicofactoren en kwetsbaarheden in jouw Microsoft-omgeving in kaart. Op basis van een snelle assessment geeft ons team van specialisten praktische aanbevelingen om de beveiliging te verbeteren.

Assessment

Microsoft 365 Security Assessment

Duur: 3 dagen (remote /onsite)

Omschrijving

Bezorgd over gegevensbescherming en cyberdreigingen? Met de Microsoft 365 Security Assessment identificeren we risico's en kwetsbaarheden in jouw Microsoft omgeving en bieden we praktische beveiliging aanbevelingen met een snelle assessment.

Onze onsite Security Check evalueert de huidige beveiligingsmaatregelen en leidt tot een Plan van Aanpak voor concrete verbeteringen.

Doelstellingen

- Inzicht krijgen in het belang van een veilige Microsoft omgeving.
- Inzicht krijgen in relevante aandachtspunten.
- Ontdekken van beveiligingsopties in jouw Microsoft omgeving.
- Inzicht krijgen in het beveiligingsniveau van jouw Microsoft omgeving.
- De volgende stappen bepalen om jouw Microsoft omgeving verder te beveiligen.

Uitkomsten

- Een plan van aanpak op basis van de workshop.
- Een exemplaar van het presentatiemateriaal als inspiratie en naslag.

Methode

Onderzoek
Een korte inventarisatie en assessment wordt uitgevoerd op jouw Microsoft omgeving.

Beoordeling en analyse
Een Ekco specialist deelt de bevindingen, bespreekt mogelijkheden en doet aanbevelingen om de security te optimaliseren.

Ontwikkel een plan
Ontvang een Plan van Aanpak; een geprioriteerde lijst met aanbevelingen op basis van de workshop.

Scope

- De assessment omvat geen aanpassingen aan jouw IT-omgeving. De focus ligt op het in kaart brengen van jouw situatie en het opstellen van een plan. Eventuele verdere werkzaamheden worden afzonderlijk besproken.
- De workshop behandelt de volgende onderwerpen:
  - Zero Trust
  - Conditional Access
  - Identiteit
  - Apparaten
  - Data
  - Applicaties
  - Netwerk & Infrastructuur
  - Beleid en bewustzijn
  - Microsoft Defender
  - SIEM en SOC

Assessment

Microsoft 365 Security Assessment

Overzicht

Doelgroep

- Security, privacy en IT georiënteerde rollen binnen de organisatie.

Vereiste voorkennis

- Ervaring met beheer van Microsoft.
- Inzicht in de eigen Microsoft omgeving.

Benodigde tijd

- 6 uur op de eerste dag,
- 2 uur op de derde dag voor de close-out meeting.

Overige benodigdheden

- Toegang tot de Microsoft omgeving.
- Een account in de Microsoft 365 omgeving, met de Global Reader en Security Reader rol.

Assessment en kennisoverdracht		
Scoping	Kennismaking Scoping	• Kennismaking • Scoping call om de vereisten en structuur van de opdracht door te nemen.
Dag 1	Data verzamelen Workshop	• Korte inventarisatie en Quick Assessment We nemen de tijd om jouw huidige situatie in kaart te brengen. We analyseren jouw IT-omgeving, identificeren knelpunten en verbeterpunten. • Interactieve workshop De Quick Assessment omvat een interactieve workshop waarin we de bevindingen uitleggen, best practices voor organisatiebeveiliging delen en specialisten de resultaten bespreken.
Dag 2	Analyse Rapportage	• Na de inventarisatie en workshop stellen we een Plan van Aanpak op met stappen en benodigdheden.
Dag 3	Presentatie	• We bespreken het Plan van Aanpak en lichten de activiteiten en volgorde toe.

Meer informatie? Neem contact met ons op

info_nl@ek.co

www.ekco.nl

088 – 070 0600