

Basis op Orde

De security baseline voor Microsoft 365

Een Microsoft 365 omgeving bevat veel informatie. Deze informatie is eenvoudig benaderbaar, verwerkbaar en uitwisselbaar. Daarom is het van groot belang dat de juiste maatregelen worden genomen om de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie te waarborgen en te voldoen aan interne en externe regelgeving.

Beveiliging van Microsoft 365

Microsoft 365 biedt verschillende apps en services om samen te werken en informatie te delen als Microsoft Teams, SharePoint, OneDrive en Yammer. Deze zijn altijd en overal (mobiel) toegankelijk voor medewerkers en mensen van buiten de organisatie. Een zorgvuldige beveiliging van dit werkproces brengt verschillende uitdagingen met zich mee:

- Hoe regelen we de toegang tot informatie en met wie werken we samen?
- Hoe beheren en beveiligen we onze identiteiten?
- Wat is onze (zeer) gevoelige informatie en hoe gaan we hiermee om?

Het Basis op Orde traject is erop gericht om samen met u de juiste maatregelen in kaart te brengen en hiermee een Microsoft 365 security baseline te realiseren. Om veilig te werken met Microsoft 365 moet het voor u mogelijk zijn om uw informatie en medewerkers te beschermen, afwijkingen en incidenten te detecteren en deze ook te kunnen onderzoeken. Het zogenaamde **Protect, Detect, Investigate** and **Respond model**.

In ons Basis op Orde traject werken we samen met uw medewerkers om de juiste maatregelen in kaart te brengen. Deze maatregelen resulteren in een Microsoft 365 security baseline. Hiernaast identificeren we maatregelen en processen voor de langere termijn. Onze focus ligt hierbij op de bescherming van identiteit en informatie, het werken met mobiele devices en het tegengaan van interne en externe bedreigingen.

Na dit traject bent u er zeker van dat de basis op orde is van uw Microsoft 365 beveiliging en heeft u een roadmap voor de komende periode. Deze maatregelen kunnen zonder additionele licenties worden doorgevoerd en verhogen het niveau van beveiliging direct.

Basis op Orde traject

Het Basis op Orde traject kent een gemiddelde doorlooptijd van drie weken en is opgebouwd uit de volgende onderdelen:



Tijdens een **inspiratiesessie** nemen we mee op reis door de wereld van bedreigingen én kansen.



Tijdens de workshop **Secure Score en Bedreigingen** wordt de Microsoft 365 Secure Score en Azure AD Identity Protection gebruikt om inzage te krijgen in de huidige volwassenheid van uw beveiliging.



De workshops **Identiteit, Informatie, Apparaatbeheer** en **Azure** gaan in op deze specifieke onderdelen.



Het traject wordt afgesloten met een op maat gemaakte **roadmap** met aanbevelingen voor de korte, middellange en lange termijn.

Doelgroep

- Chief Information Security Officer (CISO)
- Chief Information Officer (CIO)
- Security Officer
- IT Manager
- IT Security
- IT Compliance

Meer weten of direct aan de slag?

Wilt u meer weten over wat het Basis op Orde traject uw organisatie kan opleveren of een offerte op maat? Neem dan contact op met uw Motion10 Accountmanager of [Albert Hoitingh](#), Modern Work & Security Lead bij Motion10.