Dataplatform Security Check

Cloud Security Care

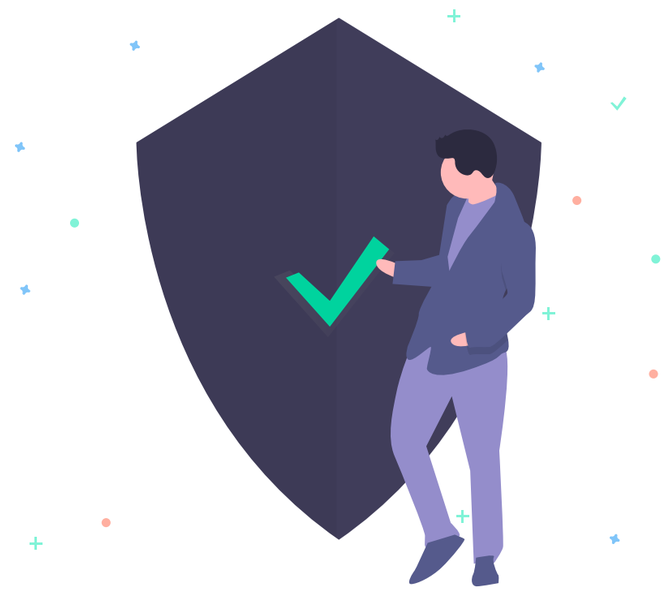
Steeds meer organisaties stappen over naar de Microsoft Azure cloud om hun moderne dataplatform te realiseren. Met uitstekende redenen: het gebruik is eenvoudig, schaalbaar en kostenefficiënt. Toch speelt er bij de overstap naar Azure nog een ander thema van essentieel belang: security.

Dataplatform Security Check

Motion10 stelt zonder meer dat Microsoft een veilige infrastructuur biedt voor uw cloud-omgeving, inclusief uw dataplatform. Het correct configureren van het platform en bijbehorende services is echter uw eigen verantwoordelijkheid. Hetzelfde geldt voor het nemen van specifieke veiligheidsmaatregelen en het houden van toegangscontrole voor gebruikers en applicaties. Helaas zijn veel organisaties zich hier onvoldoende van bewust, waardoor te weinig aandacht wordt besteed aan het beveiligen van hun dataplatform als geheel. Daardoor lopen zij onnodig risico's, zoals ongewenste toegang tot het platform, datalekken en het niet voldoen aan AVG-wetgeving.

De meest voorkomende security uitdagingen die wij in de praktijk tegenkomen zijn:

- *Het verlenen van toegang van alle Azure services tot SQL DB*
- *Het verlenen van toegang van externe consultants en eigen medewerkers tot de volledige resource group.*
- *Het leggen van Data Factory verbinding met een database met harcoded gebruikersnamen en wachtwoorden*
- *Het niet naleven van AVG-regels*
- *Het niet intrekken van rechten na het vertrek van een medewerker of consultant*
- *Het niet frequent of niet opnieuw automatisch genereren van Azure Storage Acces Key*
- *Het verlenen van te veel rechten en het niet of nauwelijks toekennen van beperkte of tijdelijke rechten (least privilege)*



Motion10 heeft op basis van diverse studies, Microsoft-richtlijnen en eigen praktijkervaring een lijst opgesteld met meer dan 100 checks en best practises voor een veilig dataplatform: de Dataplatform Security Check. De Dataplatform Security Check wordt constant up-to-date gehouden en uitgebreid en is opgebouwd uit een securityvolwassenheidsmodel voor tien essentiële deelgebieden binnen een modern dataplatform:

1. *Data Bricks*
2. *Key vault*
3. *SQL DB*
4. *Netwerk*
5. *Firewall*
6. *Algemeen*
7. *Blog Storage*
8. *Resource groups*
9. *Data Factory*
10. *Power BI*

Op basis van een gericht assessment op de deelgebieden die voor u van toepassing zijn, beoordelen wij waar uw organisatie staat op het gebied van de security van uw cloud dataplatform. Na afloop van de Dataplatform Security Check beschikt u over een concreet stappenplan met verbeterinitiatieven voor het bereiken van een veilig modern dataplatform in Azure.

Van intake tot inzichten in slechts twee weken

Workshop

- Workshop met IT, beheer en development
- Afstemmen en inregelen toegang dataplatform

Assessment

- Doorlopen checklist op relevante deelgebieden
- Scoring security (overall en deelgebieden) en uitwerken advies

Advies

- Eindpresentatie met bevindingen op 10 deelgebieden
- Roadmap verbeterinitiatieven met ureninschatting

Meer weten of direct aan de slag?

Wilt u meer weten over wat de Dataplatform Security Check uw organisatie kan opleveren? Neem dan contact op met Jorgo de Muinck, Solution Lead Data & Analytics, op 06 27 32 29 92 of jorgo.demuinck@motion10.com of met uw Accountmanager'.