Ministerie van Justitie en Veiligheid

CIO Rijk, CIO-beraad, CTO-raad, deelnemers SLMMicrosoft, Google Cloud en AWS Rijk, geïnteresseerden

Hoofddirectie Bedrijfsvoering
Directie Informatievoorziening en Inkoop
Strategische Inkoop

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Contactpersoon
SLM Microsoft, Google Cloud en AWS

SLMMicrosoft@minjenv.nl

Datum
10 januari 2025

Onze referentie
181224

Bijlage(n)
geen

memo

BIO Compliance Initiative Template voor Microsoft Azure.

Aanleiding memo

Strategisch Leveranciersmanagement Microsoft, Google Cloud en AWS (SLM) heeft onderzoek laten doen naar het *BIO Compliance Initiative Template* van Microsoft. De uitkomsten zijn opgenomen in een rapport waar instaat hoe gebruikersorganisaties het BIO Compliance Initiative Template kunnen gebruiken als ondersteuning voor het inrichten van Microsoft Azure, volgens de vereisten van de BIO (Baseline Informatiebeveiliging Overheid). De resultaten van het onderzoek geven een uitgebreid inzicht in de werking, inrichting en wijze waarop het template organisaties kan ondersteunen bij BIO-compliance.

Vanwege de veelzijdigheid van de onderzoeksresultaten en om deze toegankelijk te maken voor hen die minder bekend zijn met de BIO en de technische werking van Azure, zijn de resultaten en conclusies in dit memo beknopt samengevat.

Allereerst wordt ingegaan op de vraag wat het BIO Compliance Initiative Template behelst. Daarna volgt een samenvatting van de resultaten en volgen enkele aanbevelingen van SLM.

Onderzoek BIO Compliance Initiative Template

Microsoft heeft voor gebruikers van Microsoft Azure een template ontwikkeld, genaamd het BIO Compliance Initiative Template. Dit template is een hulpmiddel dat organisaties kunnen implementeren en gebruiken als ‘policy’ binnen een Microsoft Azure-omgeving. Volgens Microsoft maakt dit template het mogelijk om de inrichting en instellingen van systeeminstellingen (workloads) binnen de Azure-omgeving te monitoren op conformiteit met de BIO vereisten.

Om te beoordelen hoe het template ondersteuning biedt aan gebruikersorganisaties bij het voldoen aan de BIO hebben wij een

Hoofddirectie
Bedrijfsvoering
Directie Informatievoorziening en Inkoop
Strategische Inkoop

Datum
10 januari 2025

Onze referentie
5214524

onderzoek naar het template laten uitvoeren met hierbij de volgende hoofdvraag: *"In hoeverre en op welke wijze (met welke maatregelen aan de gebruikerszijde) is bij het toepassen van het BIO Compliance Initiative Template, Microsoft Azure door een gebruikersorganisatie BIO-compliant te gebruiken?"*

Scope van het BIO Compliance Initiative Template

In de basis monitort het template of systeeminstellingen binnen Azure zijn ingesteld conform de Microsoft Best Practices (Microsoft Cloud Security Benchmark), waarbij de indeling van het template is gebaseerd op de 'BIO Thema-uitwerking Clouddiensten'. Microsoft heeft op basis van deze Thema-uitwerking per thema inzichtelijk gemaakt welke systeeminstellingen gemonitord worden. Op deze wijze kan de gebruiker per thema beoordelen of binnen haar Azure-omgeving wordt voldaan aan de Microsoft Best Practices en derhalve de thema-uitwerking. Door de huidige inrichting is het voor de gebruiker echter niet direct inzichtelijk welke monitoring van het template toeziet op bijbehorende BIO-normen aangezien deze mapping ontbreekt.

Om te beoordelen welke monitoring door het template betrekking heeft op de BIO-normen (wat niet identiek is aan de Thema-uitwerkingen), is als onderdeel van het onderzoek een mapping gemaakt tussen gemonitorde systeeminstelling en de BIO. Uit het onderzoek blijkt dat er in totaal 261 systeeminstellingen binnen Azure worden gemonitord door het Template (basisversie 2.3.3 van het template), variërend van monitoring op toereikende encryptiestandaarden tot aan een controle op het afdwingen van MFA voor administrators. Per BIO-norm is allereerst beoordeeld in hoeverre deze betrekking heeft op een technische cloudinrichting en derhalve gemonitord kan worden door het template. Resultaat hiervan is dat van de bestaande 250 BIO-normen (Controls en Overheidsmaatregelen) voor 65 normen beoordeeld is dat een technisch element aanwezig is met betrekking tot IaaS en PaaS oplossingen en derhalve monitoring op de systeeminstellingen kan plaastvinden. Uit de mapping is geconcludeerd dat 32 van deze 65 BIO-normen worden geraakt door het BIO Compliance Initiative Template.[1]

Het template dekt uitsluitend de technische normen die zijn opgenomen in de BIO. Het is belangrijk te benadrukken dat procesmatige normen, zoals beleid en procedures, door de organisatie zelf moeten worden ingericht en onderhouden om volledig BIO-compliant te zijn. Dit ligt buiten de scope van het template, wat gezien de aard ervan logisch is.

[1] Op p. 15-16 van de rapportage is dit nader uitgewerkt en schematisch weergegeven.

Hoofddirectie
Bedrijfsvoering
Directie Informatievoorziening en Inkoop
Strategische Inkoop

Datum
10 januari 2025

Onze referentie
5214524

Daarnaast gaat het template verder dan de BIO-normen door ook systeeminstellingen te monitoren die niet specifiek aan een BIO-norm zijn gekoppeld. Het template is immers gebaseerd op de Best Practices van Microsoft (Microsoft Cloud Security Benchmark) en is dus omvangrijker dan enkel de BIO.

Werking en randvoorwaarden van het BIO Compliance Initiative Template

Tot slot zijn er validatiewerkzaamheden verricht om de werking van monitoring door het template te beoordelen. Hiervoor zijn drie systeeminstellingen geselecteerd. Voor deze instellingen is vastgesteld dat het template de status correct weergeeft volgens de geconfigureerde systeeminstellingen binnen de Azure-omgeving en dat bij wijzigingen in de systeeminstellingen de status van het template overeenkomstig wordt aangepast.

Daarnaast zijn de randvoorwaarden voor effectief gebruik van het template beoordeeld. Dit zijn als volgt:

- Zorg voor logging van meldingen en templatewijzigingen om BIO-compliance te waarborgen en ongeautoriseerde aanpassingen te detecteren.
- Stel periodieke controles of automatische alarmen in voor tijdige opvolging van template-meldingen.
- Laat wijzigingen aan het template via een formeel change proces verlopen.
- Beoordeel of het template op managementniveau of subscriptieniveau ingezet moet worden.
- Waarborg functiescheiding tussen IT- en template-beheerders om ongeautoriseerde wijzigingen te voorkomen.

Advies SLM n.a.v. het onderzoek

De resultaten van het onderzoek laten zien dat het BIO Compliance Initiative Template een goed hulpmiddel kan zijn voor gebruikers voor het BIO Compliant inrichten van een Azure-omgeving. Het template monitort uitgebreid of configuraties van systeeminstellingen binnen de Azure-omgeving zijn ingesteld volgens de Microsoft Best Practices (Microsoft Cloud Security Benchmark) en dat deze systeeminstellingen zijn te relateren aan verschillende BIO-normen. Dit kan gebruikers helpen bij het controleren of hun Azure-omgeving voldoet aan de BIO.

Wel adviseren wij organisaties scherp te zijn op het volgende:

1. Het template monitort systeeminstellingen, maar dwingt deze niet af.

Hoofddirectie
Bedrijfsvoering
Directie Informatievoorziening en Inkoop
Strategische Inkoop

Datum
10 januari 2025

Onze referentie
5214524

2. Gebruikersorganisaties dienen zich er bewust van te zijn dat de monitoring is gebaseerd op Microsoft Best Practices (Microsoft Cloud Security Benchmark). Deze practices kunnen echter afwijken van het beleid van de organisatie en daarmee de BIO-norm. Veel BIO-normen zien er namelijk op toe dat informatiebeveiliging wordt ingericht op basis van het beleid van de gebruikersorganisatie.
3. De huidige inrichting van het template is gebaseerd op de BIO Thema-uitwerking Clouddiensten en niet direct op de BIO-normen. Het onderzoek toont aan dat 32 BIO-normen (Controls en Overheidsmaatregelen) worden geraakt door het template en draagt derhalve bij aan het voldoen aan deze normen.
4. Gebruikersorganisaties moeten zelf rekening houden met een aantal randvoorwaarden voor het effectief inzetten van het template, zoals logging van meldingen, periodieke controles, formele change processen, en functiescheiding tussen IT- en templatebeheerders.
5. Het template kan in de toekomst door Microsoft nog worden aangepast, wat gevolgen kan hebben voor de inrichting en monitoring.

Met vriendelijke groet,

Team Strategisch Leveranciersmanagement Microsoft, Google Cloud en Amazon Web Services Rijk