Tweede Kamer
DER STATEN-GENERAAL

Notitie Restrisico's TK-workspace

datum 1 december 2023

Dienst automatisering
M +31 6 5.1.2e
E 5.1.2e @tweedekamer.nl

1 Inleiding

Tijdens de ontwikkeling van de moderne werkomgeving heeft er op verschillende momenten op verschillende niveaus (strategisch, tactisch) overleg plaats gevonden waarin punten op het gebied van informatiebeveiliging zijn besproken en vastgesteld. Deze notitie geeft inzicht in de verschillende besluiten die zijn genomen en de inrichtingskeuzes die zijn gemaakt met als doel om het restrisico te definiëren en te accepteren voor wat betreft de uitrol van Moderne werkomgeving voor de politieke organisatie.

1.1 Opsomming inrichtingskeuzes

In het governance overleg DA van 16 mei is de memo compliancy Moderne werkomgeving[1] besproken en vastgesteld. Deze memo geeft inzicht in de wijze van inrichting en afwijkingen t.o.v. een 2-tal advies documenten op gebied van moderne werkplek gebaseerd op Microsoft Cloud technologie. Beide advies documenten zijn bekend binnen de Rijksoverheid en worden veelvuldig gebruikt.

- White-Paper-Richtlijnen-Privacy-En-Informatiebeveiliging-Bij-Strategische-Adoptie-Microsoft-Cloud-V_.pdf
- SLM Rijk Handleiding privacyvriendelijke instellingen Microsoft 365 - voor beheerders (slmmicrosoftrijk.nl)

De memo beschrijft een 5.1.2h + 5.1.2i [redacted]

Daarnaast is door SLMrijk een rapport van Ernst & Young[3] gepubliceerd welke het resultaat weergeeft van een onderzoek naar BIO-compliance van Microsoft365. Deze is niet in de eerder genoemde memo meegenomen omdat het rapport onlangs is gepubliceerd.

[1] Memo Compliancy.docx (tweedekamer.nl)

[2] Memo BYOK versus MME
[3] Rapport BIO compliance Ernst & Young

Vanwege de gering gelakte tekst zijn de uitzonderingsgronden in paragraaf 1.2 niet volledig leesbaar. De informatie is geweigerd op grond van de artikelen: 5.12h en 5.1.2i Woo

1.2 BBN toets

In de maand mei heeft er een BBN-toets plaats gevonden onder begeleiding van bureau Ciso. De uitkomst van de toets is het niveau BBN[redacted] m.b.t. informatiesysteem Moderne werkomgeving met aanvullende aandacht voor beschikbaarheid. Op basis van deze toets is er een riskletter[4] opgesteld. De riskletter is samen met de reactie[5] van het projectteam besproken en vastgesteld in het governance overleg DA. In de reactie staan de verschillende acties benoemd die zijn opgenomen in TK-workspace inrichting.

1.3 Pentest

Bij ontwikkeling van de moderne werkomgeving is er gebruik gemaakt van een [redacted]

De resultaten van de [redacted].

1.4 AVG & Privacy

Conform het Rijks Cloudbeleid[7] is met de introductie van de Moderne werkomgeving ruim aandacht geweest voor de wet en regelgeving op het gebied van de AVG en privacy. De adviezen die zijn benoemd in de door SLM Rijk uitgevoerd DPIA's[8] op Microsoft 365 platform zijn meegenomen in de ontwikkeling van de werkomgeving. Daarnaast is er een AVG verwerkingsovereenkomst opgesteld voor de moderne werkomgeving en deze wordt vastgelegd in het AVG register.

[4] Riskletter BBN-toets
[5] Reactie Riskletter
[6] Advies notitie TK-workspace
[7] Rijks cloudbeleid
[8] DPIA

1.5 Informatiebeheer

In samenwerking met programma verbeteren informatie huishouding Tweede Kamer (VITK) is een basis beleid[9] op het gebied van informatiebeheer opgesteld. Op basis van dit beleid wordt de Moderne werkomgeving en dan met name Microsoft Teams ingericht de komende periode. In het strategisch overleg VITK – Moderne werkomgeving 30-11 is dit beleid vastgesteld.

2 Restrisico's

Op basis van eerder genoemde besluiten en adviezen volgt hieronder een opsomming van risico's die zijn benoemd, deze risico's worden als restrisico gedefinieerd. In een eerder overleg zijn deze risico's reeds geaccepteerd door de diverse overleg.

5.1.2h + 5.1.2i

5.1.2h + 5.1.2i

5.1.2h + 5.1.2i

5.1.2h + 5.1.2i

Advies richtlijnen microsoft Cloud

5.1.2h + 5.1.2i

5.1.2h + 5.1.2i

5.1.2h + 5.1.2i

[9] Beleid lifecycle MSTeams
[10] Memo wachtwoorden sync

5.1.2h + 5.1.2i

5.1.2h + 5.1.2i

3 Besluit

Het programma TK-workspace vraagt aan het governance overleg om op basis van de inventarisatie van de rest risico's, deze risico's te accepteren en geeft daarmee toestemming voor implementatie onder voorwaarde van een positief advies rapport pilot politiek.

Het gaat hier nadrukkelijk om het begin van de TK-workspace werkplek (verzie 1.0). Deze werkplek wordt op het gebied van functionaliteit, techniek en security verder doorontwikkeld naar een volgende versie met daarin de nodige verbeteringen op gebied van gebruikersgemak en informatiebeveiliging.

[11] IB maatregel en resultaat pilot2

Vanwege de gering gelakte tekst, kan het zijn dat enkele uitzonderingsgronden niet leesbaar zijn.
De op in hoofdstuk vier geweigerde informatie is geweigerd op grond van de artikelen: 5.12h en 5.1.2i Woo

4 Bijlage

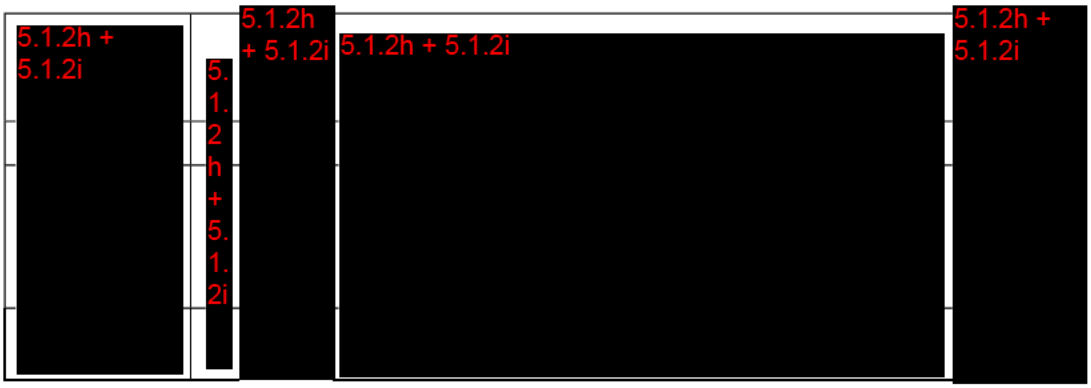
Hieronder een overzicht van de verschillende adviezen die zijn benoemd in de whitepaper t.b.v. implementatie M365 binnen Rijksoverheid.

4.1.1 Beveiligen en beheren van gegevens

De organisatie beveiligt en beheert gegevens, bijvoorbeeld door middel van versleuteling en dataclassificatie. De volgende [redacted] additionele beveiligingsmaatregelen die vanuit Microsoft 365 beschikbaar zijn, helpen de organisatie op weg met het beheren van gegevens die zich in de Cloud omgeving bevinden en tevens met het beveiligen van gegevens die intern en extern worden uitgewisseld.

Naam	Blz	OK - NOK	Toelichting	6-12 OK - NOK
5.1.2h + 5.1.2i	5.	5.1.2h + 5.1.2	5.1.2h + 5.1.2i	5.1.2h + 5.1.2i
			5.1.2h + 5.1.2i	
	5			


5.1.2h + 5.1.2i
5. 1. 2h + 5. 1. 2i
5.1.2h + 5.1.2i
5.1.2h + 5.1.2i
5.1.2h + 5.1.2i



4.1.2 Inrichten logische toegangsbeveiliging

Vanuit het domein Inrichten logische toegangsbeveiliging heeft de organisatie de verantwoordelijkheid om de Cloud omgeving zodanig in te richten, dat gebruikers de juiste toegangsrechten tot alleen de benodigde applicaties hebben. De volgende 5.1.2h additionele beveiligingsmaatregelen die vanuit Microsoft 365 beschikbaar zijn, helpen de organisatie op weg met het inrichten van sterke toegangsbeveiliging, het identificeren van risico's rondom identiteiten en het verbeteren van aanmeldings- en wachtwoordprocedures.

Naam	Blz	OK - NOK	Toelichting	6-12 OK - NOK
5.1.2h + 5.1.2i	5.1.2h + 5.1.2i	5.1.2h + 5.1.2i	5.1.2h + 5.1.2i	5.1.2h + 5.1.2i

5.1.2h + 5.1.2i	5.1.2h + 5.1.2i	5.1.2h + 5.1.2i	5.1.2h + 5.1.2i	5.1.2h + 5.1.2i

4.1.3 Logging en monitoring

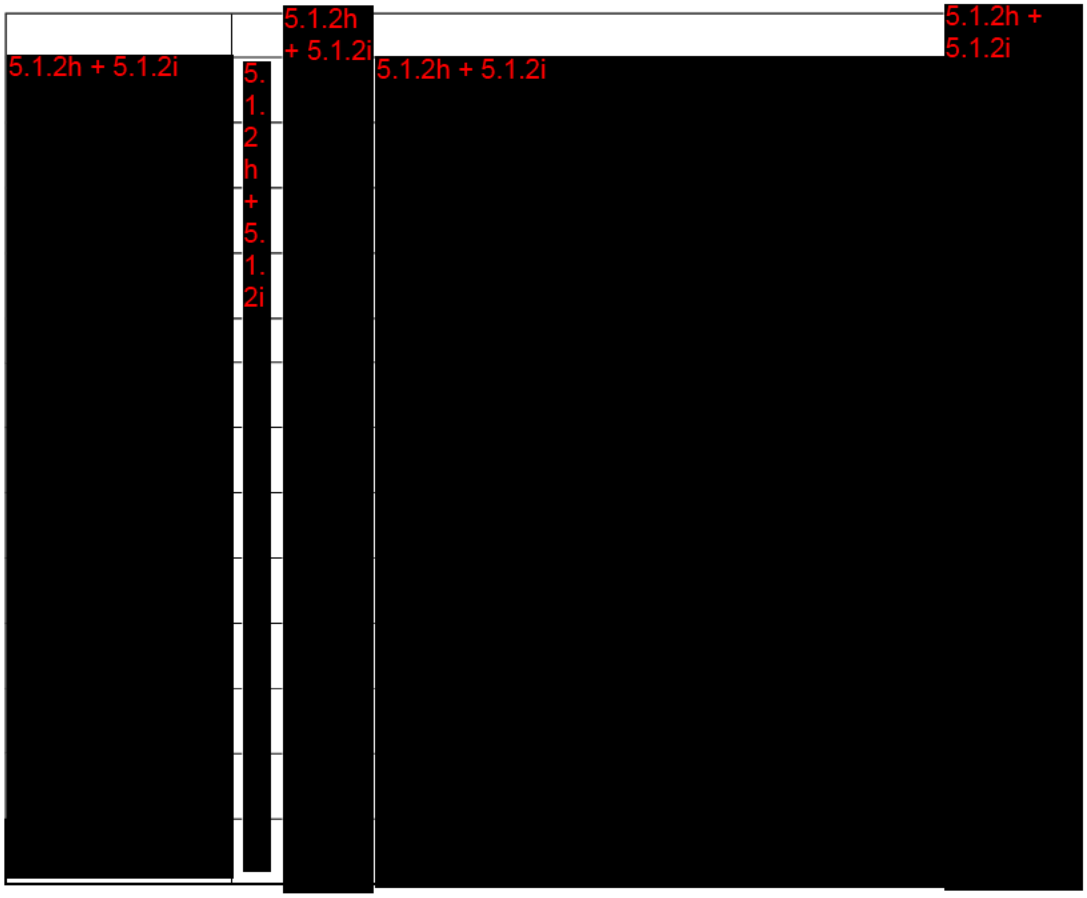
De organisatie heeft inzicht in gebruikers- en beveiligingsactiviteiten binnen de organisatie en beoordeelt deze regelmatig om (verbeter)acties te ondernemen. De volgende 5.1.2h + 5.1.2i additionele beveiligingsmaatregelen die vanuit Microsoft 365 beschikbaar zijn, helpen de organisatie met het tijdig doorvoeren van verbeteracties op basis van waardevolle inzichten.

Naam	Blz	OK - NOK	Toelichting	6-12 OK - NOK
5.1.2h + 5.1.2i	5.1.2h + 5.1.2i	5.1.2h + 5.1.2i	5.1.2h + 5.1.2i	5.1.2h + 5.1.2i

4.1.4 Beveiliging tegen dreigingen

De organisatie inventariseert informatiebeveiligingsgebeurtenissen en onderneemt tijdig actie op beveiligingsincidenten. De volgend 5.1.2h + 5.1.2i additionele beveiligingsmaatregelen die vanuit Microsoft 365 beschikbaar zijn, helpen de organisatie met het verlagen van de kans op en de impact van beveiligingsincidenten. Hiermee borgt een organisatie onder andere de continuïteit van processen, de bescherming van (gevoelige) gegevens van burgers en worden hoge kostenposten als gevolg van aanvallen die systemen kunnen platleggen, voorkomen.

Naam	Blz	OK - NOK	Toelichting	6-12 OK - NOK
5.1.2h + 5.1.2i	5.1.2h + 5.1.2i	5.1.2h + 5.1.2	5.1.2h + 5.1.2i	5.1.2h + 5.1.2i


5.1.2h + 5.1.2i
5.1.2h + 5.1.2i
5.1.2h + 5.1.2i
5.1.2h + 5.1.2i
5.1.2h + 5.1.2i