Risico analyse M365 Cloud toepassingen

Sector Informatiebeveiliging i.o., Risicomanagement

Definitief

Versie 1.0

Versie datum 22 november 2022

Rubricering Politie intern

« waakzaam en dienstbaar »

Documentinformatie

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing	Gemarkeerde wijzigingen

Distributie

Versie	Verzend datum	Naam	Afdeling / Functie

Interne review commentaar

Versie	Wanneer	Wie	Functie

Gebruikte documentatie

Documentnaam en versie	Ontvangen van opdrachtgever op

Document locatie

Versie	Locatie

Afstemming met opdrachtgever

Versie	Wanneer	Wie	Functie

Deelnemers (participanten) Risicoanalyse (onderverdelen naar sessies / workshops?)

Wie	Functie / Afdeling

Inhoudsopgave

Managementsamenvatting

Momenteel maakt de politie nog zeer beperkt gebruik van clouddiensten. Met de in gebruik name van M365 zal dit wijzigen. Initieel zullen niet alle applicaties en diensten die vallen onder M365 direct worden afgenomen. In deze risicoanalyse is alleen gekeken naar de informatiebeveiligingsrisico's en niet specifiek naar de privacy risico's of de rechtmatigheid van een verwerking in de cloud.

Ieder gebruik van clouddienstverlening brengt inherent risico's met zich mee.
Diverse onderzoeken en notities van onder andere inlichtingendiensten benoemen zowel de voor- als nadelen van het gebruik van cloudtechnologie.

Als gekeken wordt naar de voordelen dan zijn die vooral te vinden op het gebied van functionaliteit en kosten. Hierbij dient echter niet vergeten te worden dat, Microsoft aanzienlijk meer middelen ter beschikking heeft om de beschikbaarheid, integriteit en vertrouwelijkheid van de gegevens en de omgeving te borgen dan de politie heeft. Het hele businessmodel van Microsoft is mede gebaseerd op het behoud van vertrouwen in de omgeving die zij aanbiedt.
Het nadeel is echter wel dat vooral statelijke actoren zeer geïnteresseerd zullen zijn in het verkrijgen van toegang tot de cloudomgeving, aangezien zij daarmee ook direct toegang zouden kunnen verkrijgen tot grote hoeveelheden informatie.

In overweging nemende:

- De huidige status van de politieomgeving
- De functionele behoefte van de business
- De technologische ontwikkelingen
- De (cloud)strategie van de politie
- De benoemde risico's in deze rapportage
- De beperkte beheercapaciteit van de politie
- De middelen die Microsoft ter beschikking heeft om omgevingen te beschermen ten opzichte van de mogelijkheden die de politie heeft op dat vlak

En ervan uitgaande dat:

- Privacy technisch zowel voor AVG als Wpg voldaan kan worden aan de wettelijke vereisten
- Verwerkersovereenkomsten juist en volledig zijn gesloten
- Contractuele afspraken juist zijn vastgelegd en periodiek worden getoetst en geëvalueerd

Wordt mits de mitigerende maatregelen worden genomen en de restrisico's worden geaccepteerd positief geadviseerd over een ingebruikname van M365 diensten in de cloud, tot een rubriceringsniveau "politie vertrouwelijk"

Daar waar statelijke actoren mogelijk interesse zouden hebben in de gegevens van de politie of het verstoren van de dienstverlening van de politie zou overwogen moeten worden om niet direct uitsluitend gebruik te maken van clouddiensten. Indien het verwerkingen betreft van data betreffende specifieke georganiseerde criminele organisaties zou een afweging gemaakt moeten worden of de verwerking in de cloud verstandig is.

Hierbij wordt wel opgemerkt dat het verstandig is om voor kritieke dienstverlening uitwijkscenario's beschreven te hebben in het geval van een mogelijke verstoring van de dienstverlening in de cloud.

1. Inleiding

1.1. Aanleiding

Microsoft is net als vele andere dienstverleners, is ook Microsoft haar businessmodel aan het aanpassen. Dit betekent dat steeds meer diensten van Microsoft alleen worden aangeboden in de cloud. Momenteel maakt de politie nog zeer beperkt gebruik van clouddiensten. De behoefte van de politie is dat zij gebruik wenst te maken van meerdere functionaliteiten die worden geboden in de cloud. Een sprekend voorbeeld hiervan is het gebruik van MS teams. Ten tijde van corona is het gebruik van deze dienst beperkt versneld beschikbaar gesteld. Om gebruik te maken van de volledige functionaliteit moeten risico's worden bepaald en waar mogelijk worden gemitigeerd of indien dat niet mogelijk is worden geaccepteerd. Deze analyse gaat verder dan alleen het gebruik van MS teams maar behelst de volledige functionaliteit van M365.

1.2. Doel van deze risicoanalyse en onderzoeksvraag

In zijn algemeenheid is het resultaat van een risicoanalyse bedoeld voor het verbeteren van de beheersing van de informatiebeveiliging op de aspecten beschikbaarheid, integriteit en vertrouwelijkheid (en controleerbaarheid).

Het specifieke doel van deze risicoanalyse is het verschaffen van inzicht in de informatiebeveiligingsrisico's van de M365diensten van Microsoft in de publieke cloud. (Niet publiek toegankelijk).

De centrale onderzoeksvraag voor deze risicoanalyse is "*welke informatiebeveiligingsrisico's worden onderkend in de M365 diensten zoals die geboden worden door Microsoft en welke maatregelen kan de politie nemen om de geïdentificeerde risico's te reduceren. Dit met als doel om het seniormanagement te laten beoordelen of de restrisico's door hen gedragen kunnen worden en daarmee een volgende stap mogelijk te maken in het gebruik van cloud technologieën binnen de politie*"

1.3. Maatstaf voor het analyseren van risico's

Een risico is een gebeurtenis die op kan treden en die een bedreiging vormt voor het behalen van een doelstelling van de politieorganisatie in brede zin. Een risicoanalyse maakt de risico's inzichtelijk die een bedreiging vormen voor één of meerdere doelstellingen. Voor het inzichtelijk maken van de mogelijke risico's is de SMART doelstelling noodzakelijk die als maatstaf wordt gebruikt voor het bepalen en wegen van de risico's. In zijn algemeenheid kunnen informatiebeveiligingsrisico's een nadelig effect hebben op de volledigheid, tijdigheid en juistheid van informatie die op haar beurt het behalen van een doelstelling kan bemoeilijken.

Voor de IV-organisatie van de politie is een IV-visie[1] geformuleerd welke aansluit op de strategische agenda van de politie. Dit heeft geleid tot een viertal doelstellingen voor de komende jaren:

1. Een betrouwbaar fundament en de basissystemen zijn op orde
2. Digitale transformatie en iedereen digitaal fit
3. Datagedreven politiewerk
4. In de top van innovatieve korpsen Europa

Naast de bovengenoemde doelstellingen bevat de IV-strategie een aantal richtinggevende principes. In deze analyse is rekening gehouden met deze principes.

[1] IV Strategie 2022-2025 v1.0.pdf

Daarnaast is voor het identificeren van informatiebeveiligingsrisico's en maatregelen expliciet rekening gehouden met de ambitie "een betrouwbaar fundament en de basissystemen zijn op orde", die tevens als bouwsteen fungeert in deze analyse.

De volgende doelstelling(en) is/zijn voor deze risicoanalyse als maatstaf gebruikt voor het inzichtelijk maken, bepalen en wegen van de risico's (zie voor de uitwerking van de risico's hoofdstuk 4 (*Risicoanalyse en maatregelen*):

Beschikbaarheid:

- De M365 applicaties moeten hoog beschikbaar zijn.

Integriteit:

- De informatie die is opgeslagen in M365 is te allen tijde een volledige en juiste afspiegeling van de werkelijkheid. (Rechten worden tijdig toegekend of ingetrokken)
- De omgeving van M365 kan niet worden gemanipuleerd zodat onterecht toegang wordt verleend tot resources van de politie.

Vertrouwelijkheid:

- De gegevens van de politie worden beschermd tegen inzage van ongeautoriseerde personen.

Om bij te dragen aan het bewerkstelligen van de doelstelling "een betrouwbaar fundament en de basissystemen zijn op orde", zullen de gebeurtenissen in kaart worden gebracht die een dreiging vormen voor het behalen van de genoemde doelstelling. Aanvullend worden maatregelen geformuleerd om de risico's te mitigeren.

1.4. Betrokken partijen

Opdrachtgever
De opdrachtgever voor deze risicoanalyse is, 5.1.2.e Dienst-hoofd IV

Opdrachtnemer
Deze risicoanalyse is uitgevoerd door 5.1.2.e , sector Informatiebeveiliging in overleg met 5.1.2.e Masterarchitect Infrastructuur

Risicoeigenaar
De risicoeigenaar is 5.1.2.e Directeur PDC

Deelnemers
De deelnemers die zijn betrokken bij deze risicoanalyse zijn vastgelegd in de documenthistorie.

1.5. Beschrijving van het onderzoeksobject en scope

Het onderzoeksobject is Microsoft 365, het betreft hier het "Office 365 pakket" zoals aangeboden door Microsoft in de publieke Cloud. Binnen deze Cloud omgeving maakt de politie gebruik van een eigen afgeschermde omgeving die alleen toegankelijk is voor de politie.

Binnen deze risicoanalyse wordt er vanuit gegaan dat gegevens worden verwerkt tot en met de rubricering Politie Vertrouwelijk[2].

Voor wat betreft de rechtmatigheid van de verwerking van persoonsgegevens wordt er in deze analyse vanuit gegaan wat de rechtmatigheid van de verschillende verwerkingen wordt getoetst en geborgd bij het uitvoeren van de GegevensbeschermingEffectBeoordeling.

1.6. Aanvalsoppervlak

De M365 applicaties verwerken persoonsgegevens, zoals namen en e-mailadressen.
De verwachting is dat statelijke actoren en criminele organisaties niet specifiek de cloudomgeving van Microsoft zullen aanvallen om de dienstverlening van de politie te verstoren of gegevens van de politie te bemachtigen. Gezien de grote hoeveelheid aan gegevens die momenteel wordt verwerkt in de cloud voor diverse klanten is het zeer aannemelijk dat de hiervoor genoemde actoren belangstelling hebben in de cloud omgeving van Microsoft..

Door informatie in de cloud te verwerken, wordt het aanvalsoppervlak vergroot. Kwaadwillende die voorheen geen toegang tot data verkregen omdat de data on premise werd verwerkt, kunnen nu via het internet pogingen doen om politiedata te ontvreemden ofwel onbeschikbaar te maken. Dagelijks zijn dreigingsactoren constant op zoek naar slecht geconfigureerde cloud servers. Het rapport van Rapid7[3] maakt duidelijk dat kwaadwillende (actoren zoals scriptkiddies en statelijke actoren) actief op zoek gaan naar misconfiguraties van cloudservices en dat het niet moeilijk is om deze misconfiguraties te vinden en te misbruiken.

Kortom, hoewel dus een gerichte aanval op de politie in de cloud niet voor de hand ligt is niet uit te sluiten dat statelijke actoren als bijvangst mogelijk ook de gegevens van de politie zouden kunnen inzien of de dienstverlening zouden kunnen verstoren. Doordat de verwerking plaatsvindt in de cloud, wordt het aanvalsoppervlak vergroot.

1.7. Gehanteerde aannames en uitgangspunten

Voor deze risicoanalyse zijn de volgende aannames en uitgangspunten gehanteerd:

- Algemene Verordening Gegevensbescherming (AVG, art. 32)[8]
- Baseline Informatiebeveiliging Overheid (BIO)[9]
- Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI 2013)[10]
- de Archiefwet of
    - de Wet Basisregistratie Personen (Wet BRP)
    - de Wet politiegegevens (Wpg)
    - Wet justitiële en strafvorderlijke gegevens (Wjsg).
    - Wet openbaarheid van bestuur (Wob)
    - Wet open overheid (Woo)
- De dienstverlening wordt gehost/afgenomen in een publieke cloud (Microsoft) binnen de EER

Voor iedere specifieke verwerking worden indien nog de noodzakelijke documenten op gesteld om te komen tot een gewogen CIO oordeel en rechtmatige verwerking.

---

[2] *Note: Het rubriceringsniveau politie vertrouwelijk is momenteel nog niet in gebruik binnen de politie. Om aansluiting te vinden en te behouden met de rest van de overheid is momenteel een beleidsstuk in voorbereiding om deze rubricering toe te voegen.*

[3] https://www.rapid7.com/globalassets/_pdfs/research/2021-cloud-misconfiguration-report.pdf?contentTrack=true

1.8. Leeswijzer

Na deze inleiding waar het onderzoeksobject nader is gespecificeerd volgt de gedetailleerde risicoanalyse. In dat hoofdstuk worden de mogelijke risico's uiteengezet waarbij een schatting wordt gemaakt van de kans en impact van een bepaalde dreiging. Per risico wordt bepaald welke reactie wenselijk is met daarbij eventueel de geadviseerde beheersmaatregelen. Tot slot wordt in het eerstvolgende hoofdstuk de conclusie en het advies besproken.

2. Risicoanalyse en (beheers)maatregelen

2.1. Risicoanalyse en maatregelen in detail

Zoals in het beleid informatiebeveiliging is vastgelegd heeft informatiebeveiliging tot taak ‘de continuïteit van de dienstverlening aan de maatschappij zo goed als mogelijk te borgen door de beheersing van de risico’s rondom de informatievoorziening’. Een risico betreft het effect van een onzekerheid op de realisatie van (organisatie)doelstellingen. Een risico wordt omschreven door het benoemen van een oorzaak, gebeurtenis en het gevolg. Hierbij is een effect een afwijking van de verwachting - positief en/of negatief. In dit onderzoek wordt echter alleen gekeken naar de negatieve effecten op het behalen van de doelstellingen. Dit betekent nadrukkelijk niet dat deze analyse een volledig beeld geeft van alle mogelijke risico’s. De risico’s zijn in overleg met of in opdracht van de proceseigenaar vastgesteld.

Tijdens de analyse is gekeken naar welk effect een specifieke dreiging heeft op de **B**eschikbaarheid, **I**ntegriteit en **V**ertrouwelijkheid (**BIV**) van het onderzoeksobject. De risico’s worden in de matrix voorzien van een letter die staat voor één van de drie BIV-aspecten en een volgnummer. Voor het inschatten van kans en impact is gebruikt gemaakt van een 5-punts Likertschaal. De kans en impact leiden vervolgens tot een inschatting van het risico. Hierbij is de volgende definitie gehanteerd: Risico=Kans* Impact. In de bijlage is een tabel te vinden voor het bepalen van de impact.

5.1.1.b, 5.1.2.c, 5.1.2.i

5.1.1.b, 5.1.2.c, 5.1.2.i

Niet onder reikwijdte

Niet onder reikwijdte

Niet onder reikwijdte

Niet onder reikwijdte


Niet onder reikwijdte

Niet onder reikwijdte

Niet onder reikwijdte

3. Conclusie en advies

3.1. Conclusie

Momenteel maakt de politie nog zeer beperkt gebruik van clouddiensten. Met de in gebruik name van M365 zal dit wijzigen. Initieel zullen niet alle applicaties en diensten die vallen onder M365 direct worden afgenomen. In deze risicoanalyse is alleen gekeken naar de informatiebeveiligingsrisico's en niet specifiek naar de privacy risico's of de rechtmatigheid van een verwerking in de cloud.

Ieder gebruik van clouddienstverlening brengt inherent risico's met zich mee.
Diverse onderzoeken en notities van onder andere inlichtingendiensten benoemen zowel de voor- als nadelen van het gebruik van cloudtechnologie.

Als gekeken wordt naar de voordelen dan zijn die met name te vinden op het gebied van functionaliteit en kosten. Hierbij dient echter niet vergeten te worden dat, Microsoft aanzienlijk meer middelen ter beschikking heeft om de beschikbaarheid, integriteit en vertrouwelijkheid van de gegevens en de omgeving te borgen dan de politie heeft. Het hele businessmodel van Microsoft is mede gebaseerd op het behoud van vertrouwen in de omgeving die zij aanbiedt.
Het nadeel is echter wel dat met name statelijke actoren zeer geïnteresseerd zullen zijn in het verkrijgen van toegang tot de cloudomgeving, aangezien zij daarmee ook direct toegang zouden kunnen verkrijgen tot grote hoeveelheden informatie.

3.2. Advies

In overweging nemende:

- De huidige status van de politieomgeving
- De functionele behoefte van de business
- De technologische ontwikkelingen
- De (cloud)strategie van de politie
- Bovenstaande risico's en mogelijke mitigerende maatregelen
- De beperkte beheercapaciteit van de politie
- De middelen die Microsoft ter beschikking heeft om omgevingen te beschermen ten opzichte van de mogelijkheden die de politie heeft op dat vlak

En ervan uitgaande dat:

- Privacy technisch zowel voor AVG als Wpg voldaan kan worden aan de wettelijke vereisten
- Verwerkersovereenkomsten juist en volledig zijn gesloten
- Contractuele afspraken juist zijn vastgelegd en periodiek worden getoetst en geëvalueerd

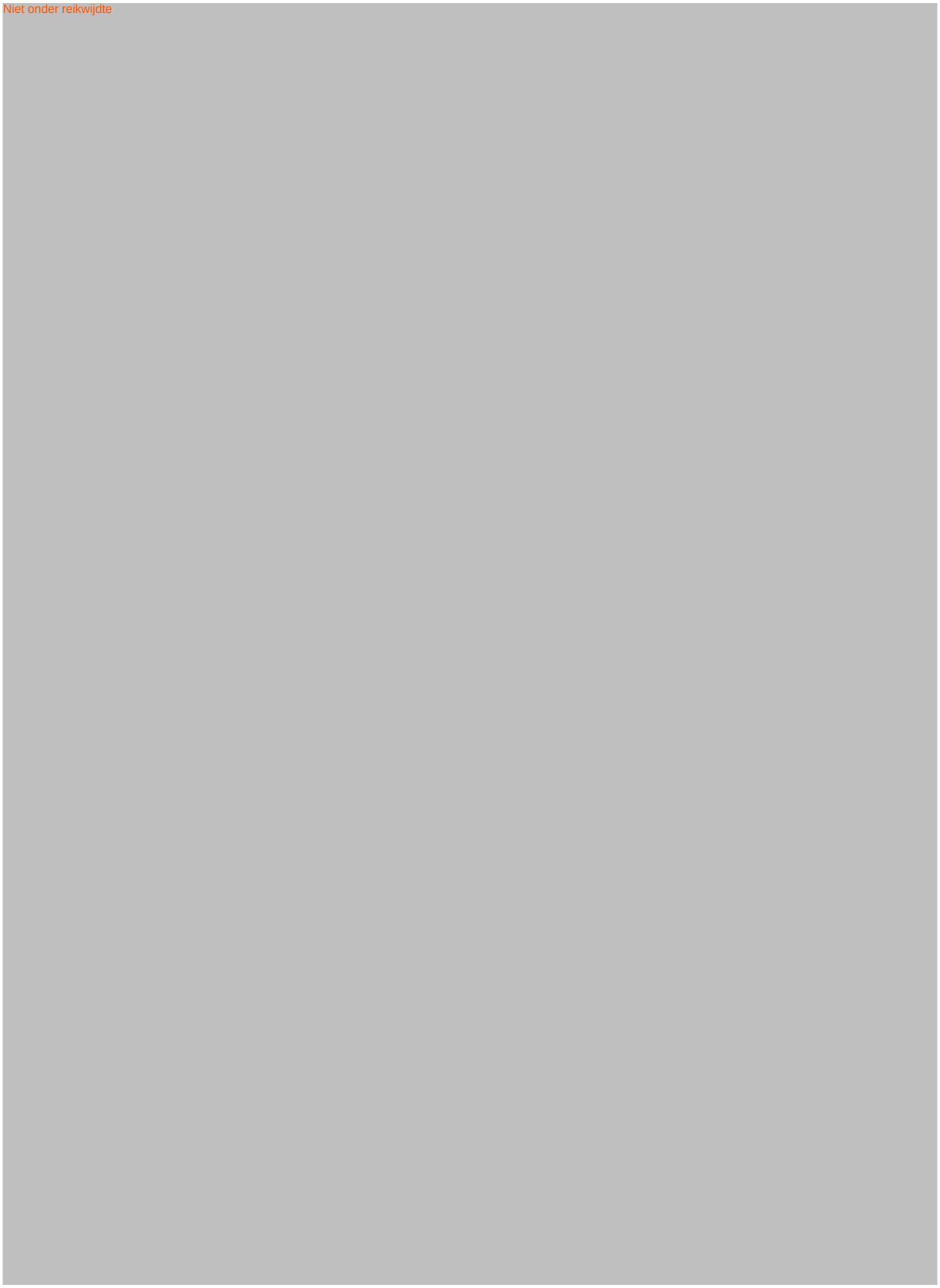
Wordt mits de mitigerende maatregelen worden genomen en de restrisico's worden geaccepteerd positief geadviseerd over een ingebruikname van M365 diensten in de cloud, tot een rubriceringsniveau "politie vertrouwelijk"

Daar waar statelijke actoren mogelijk interesse zouden hebben in de gegevens van de politie of het verstoren van de dienstverlening van de politie zou overwogen moeten worden om niet direct uitsluitend gebruik te maken van clouddiensten.
Indien het verwerkingen betreft van data betreffende specifieke georganiseerde criminele organisaties zou een afweging gemaakt moeten worden of de verwerking in de cloud verstandig is.

Hierbij wordt wel opgemerkt dat het verstandig is om voor kritieke dienstverlening uitwijkscenario's beschreven te hebben in het geval van een mogelijke verstoring van de dienstverlening in de cloud.


Niet onder reikwijdte

Niet onder reikwijdte



Niet onder reikwijdte

4.4. Tekenblad risico acceptatie

De risicoanalyse dient te worden ondertekend door de risico eigenaar. Met het ondertekenen worden de benoemde netto risico's geaccepteerd. Indien de aanbevolen maatregelen niet worden getroffen, worden daarbij logischerwijs de benoemde bruto risico's geaccepteerd.

Met het ondertekenen van dit document verklaart de risico eigenaar de risicoanalyse gelezen en begrepen te hebben bevonden en akkoord te gaan met het accepteren van de netto risico's of, indien de aanbevolen maatregelen niet worden getroffen, de bruto risico's.

Niet onder reikwijdte