TLP:GREEN

GENERIEK IMPLEMENTATIEPLAN

Monitoring & Detectie – SOC Operational Readiness – OR-6 t/m OR-9

Best Practice versie 1.1

Complexiteit document
Eenvoudig

Samenwerken maakt

DIGITAAL VEILIGER

VSSR

Inhoudsopgave

Voorwoord

De Rijksoverheid verwerkt grote hoeveelheden gevoelige informatie en is daarmee een interessant en gewild doelwit. Cybercriminelen en statelijke actoren zoeken naar kwetsbaarheden om zich zo toegang te verschaffen tot de supplychain, netwerken, systemen en (gevoelige) informatie.

De wereld van cyberdreigingen verandert snel en vraagt om gezamenlijke inspanning om weerbaar te zijn. Dit vraagt om samen te werken aan breder toegepaste én verbeterde SOC-dienstverlening. Het programma Versterken SOC Stelsel Rijk (VSSR) is opgezet om hieraan bij te dragen.

Een belangrijk onderdeel van SOC-diensten zijn de bewaking- en detectiediensten. Deze zijn erop gericht om een veelheid aan loggegevens en andere (meta-)datastromen afkomstig van de IT-infrastructuur, randapparatuur, bedrijfsapplicaties en andere dataverwerkingen in een organisatie te analyseren, aggregeren en correleren. Bewaking en detectiesystemen kunnen op basis hiervan verdachte gedragingen detecteren en alarm slaan.

Om een SOC effectief en doelmatig in te zetten is het noodzakelijk dat er een aantal onderwerpen binnen een organisatie zijn ingericht. VSSR levert diverse producten die rijksorganisaties ondersteunen bij het inrichten van een SOC en de daarvoor benodigde randvoorwaarden.

Achtergrond

VSSR levert verschillende kennisproducten die aansluiten bij de SOC Readiness Quickscan. Dit document maakt onderdeel uit van een tiental miniproducten die rijksorganisaties helpt om een aantal operationele randvoorwaarden in te richten.

Doelgroep

Versterken SOC Stelsel Rijk (VSSR) biedt met dit document handvatten voor IT-manager, IT-beheerder, Systeemeigenaren, IT-Assetmanager, Uitbestedingsmanager, Security Officer.

1 Documentgegevens

1.1 Documenthistorie

Versie	Datum	Omschrijving
V1.0	19-03-2025	Initiële versie
V1.1	6-7-2026	Referenties geactualiseerd

1.2 Referenties

Document	Link
OR-6 Platform Hardening	Zie "OR-6, Platform Hardening" onder SOC Operational Readiness (Configuratie & Logging) - Producten
OR-7 Malware Protection	Zie "OR-7, Malware Protection" onder SOC Operational Readiness (Configuratie & Logging) - Producten
OR-8 Application Control	Zie "OR-8, Application Control" onder SOC Operational Readiness (Configuratie & Logging) - Producten
OR-9 Application Hardening	Zie "OR-9, Application Hardening" onder SOC Operational Readiness (Configuratie & Logging) - Producten
VSSR-kennisdocumenten	VSSR (ncsc.nl)

1.3 Definities

Term	Omschrijving
Single point of failure	Een enkel punt in een systeem waarvan falen kan leiden tot het uitvallen van het hele systeem of bedrijfsproces.

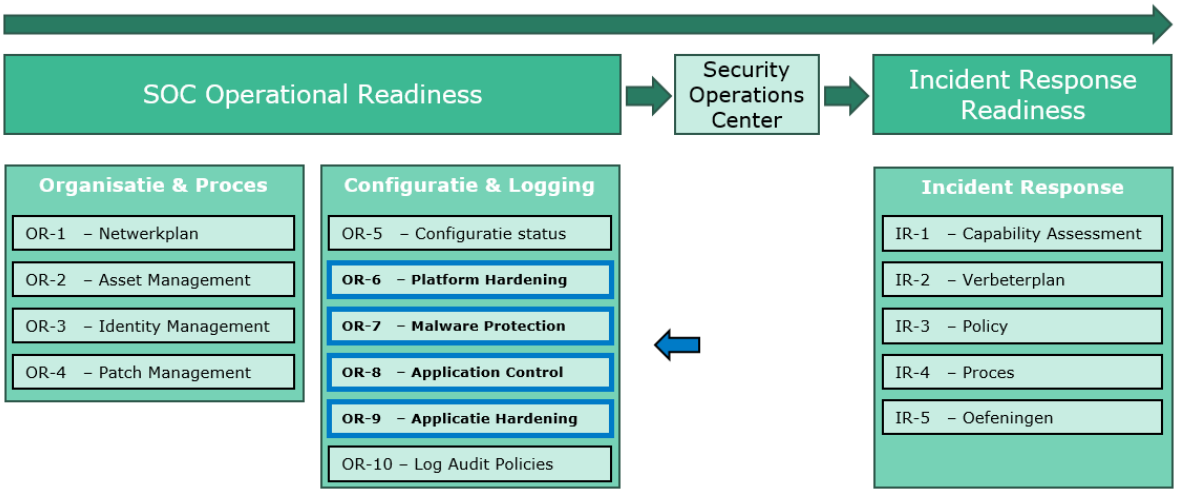
Ter verduidelijking van de terminologie en begrippen die in dit document worden gebruikt is er een verzameling van definities te vinden op Woordenboek - Cyberveilig Nederland.

2 Context miniproducten

Dit document maakt onderdeel uit van de SOC Readiness Assistance **miniproducten**. De SOC Readiness Assistance miniproducten ondersteunen uw organisatie bij de voorbereidingen die nodig zijn voor het optimaal benutten van een SOC(-dienst). Deze producten hebben een samenhangende opbouw maar kunnen ook los van elkaar worden gebruikt. De producten zijn in drie groepen te verdelen:

1) **Organisatie & Proces:** Helpt bij het inrichten van processen met als doel het SOC van de juiste informatie te voorzien om goed te kunnen monitoren.
2) **Configuratie & Logging:** Helpt bij het inrichten van basisbeveiliging met als doel om beter beschermd te zijn en de juiste logdata bij een SOC aan te kunnen leveren.
3) **Incident Response:** Met behulp van monitoring & Detectie zal een SOC security melding genereren. De Incident Response producten helpen bij het inrichten van de opvolging van deze meldingen binnen uw organisatie.

Onderstaande weergave toont dit document als onderdeel van **Configuratie & Logging** in het VSSR-Minipoducten raamwerk.



Figuur 1 - Dit document als onderdeel van het VSSR-Miniproducten raamwerk

De twee productgroepen behorende bij *SOC Operational Readiness* bestaan telkens uit een vergelijkbare set document die in figuur 1 per groep zijn weergegeven. Niet elk product bestaat uit exact de zelfde componenten maar veelal wordt de zelfde structuur gebruikt waarbij dit document het generieke implementatieplan voor OR-5 t/m 9, binnen **Configuratie & Logging**, behandelt.

3 Inleiding

Het implementatieplan biedt een gestructureerd kader om de configuratiehandleidingen voor Platform/Applicatie Hardening (OR-6, OR-9),Malware bescherming (OR-7) en Application Control (OR-8) voor een op Windows gebaseerde End-User-Computing-omgeving toe te passen.

Hardening als proces omvat het verwijderen of uitschakelen van onnodige functionaliteit en andere niet noodzakelijke elementen. De configuratiehandleiding “Basis Platform Hardening” (OR-6) geeft inzicht in de configuratie-instellingen die belangrijk zijn in het kader van beveiliging. De configuratiehandleiding “Applicatie Hardening” (OR-9) biedt een set basisconfiguraties voor het hardenen van standaardapplicaties zoals Word, Outlook en Edge.

De configuratiehandleiding "Malwarebescherming" (OR-7) beschrijft het basis antivirusbeleid, en de toepassing van ASR-regels (Attack Surface Reduction) om aanvalsvectoren te beperken. De configuratie handleiding “Application Control” (OR-8) uitleg geeft over de werking van Windows Defender Application Control (WDAC) en hoe de WDAC-wizard gebruikt kan worden om eenvoudig beleid in te stellen en te configureren.

De configuratiehandleidingen en dit implementatieplan dienen in combinatie te worden gebruikt. De configuratiehandleiding beschrijft de vereiste instellingen, terwijl het implementatieplan de procedures voor een gecontroleerde uitrol van deze instellingen uitlegt.

4 Implementatie stappenplan

In dit hoofdstuk wordt besproken hoe organisaties uitrol van configuraties op een gecontroleerde en systematische manier kunnen realiseren, met nadruk op het monitoren van de impact tijdens de pilotfase, het verzamelen van feedback en het documenteren van het proces.

Figuur 2 Stappenplan fasering

De flowchart (Figuur 2) biedt een visueel overzicht van het stappenplan voor de implementatie van configuraties. Het proces bestaat uit:

1. Voorbereiden, waarbij een inventarisatie van de huidige situatie wordt uitgevoerd en communicatie met de belanghebbenden plaatsvindt. Dit helpt om de scope van de uitrol te bepalen en verwachtingen te managen.
2. Testen, waarbij een testomgeving wordt opgezet om de impact van de instellingen te meten en te documenteren. Documentatie in deze fase is essentieel voor het traceren van de uitgevoerde wijzigingen, zodat deze in de toekomst eenvoudig kunnen worden bijgewerkt of aangepast. Dit stelt de beheerder in staat om mogelijke problemen vroegtijdig te identificeren zonder de productieomgeving te beïnvloeden.
3. Pilot, hierin wordt de uitrol gestart met een kleine, gecontroleerde gebruikersgroep. Deze groep wordt gekozen om de impact te monitoren op negatieve effecten in systemen of processen.
4. Uitrol, in deze fase wordt de uitrol verder opgeschaald naar de complete groep, waarbij bewaking en documentatie worden voortgezet om te zorgen dat alles naar behoren functioneert.
5. Evalueren, in laatste fase wordt feedback van de gebruikers verzameld en de documentatie bijgewerkt om uitgevoerde wijzigingen goed traceerbaar te maken, wat de aanpassing van de policies in de toekomst vereenvoudigt.

5 Implementatie proces

De volgende paragrafen behandelen de verschillende stappen zoals beschreven in figuur 1 Stappenplan fasering.

5.1 Voorbereiden

De voorbereiding is een belangrijke fase in het implementatieproces, waarin de noodzakelijke stappen worden genomen om wijzigingen op een gecontroleerde manier door te voeren. Dit helpt om ervoor te zorgen dat de implementatie soepel verloopt en dat er geen onverwachte problemen ontstaan.

5.1.1 Inventarisatie

Voordat wijzigingen worden doorgevoerd, is het belangrijk om een inventarisatie te maken van de benodigde vereisten voor de veranderingen. Dit omvat het identificeren van de apparaten, besturingssystemen en applicaties die door de wijzigingen getroffen worden. Ook moeten beheerders nagaan of er specifieke rechten of toegang nodig zijn om de configuraties in benodigde applicaties toe te passen en te beheren.

Taak	Actie
Identificeer apparaten	Maak een lijst van apparaten die de wijzigingen moeten ontvangen.
Bepaal de benodigde besturingssystemen	Controleer welke besturingssystemen en versies de wijzigingen vereisen[1].
Controleer licenties	In M365 is het belangrijk dat de juiste licenties beschikbaar zijn voor configuraties doorgevoerd kunnen worden.
Toegang en rechten controleren	Zorg ervoor dat de juiste beheerdersrechten tot benodigde applicaties beschikbaar zijn.

5.1.2 Compliance check

Bij het doorvoeren van configuratiewijzigingen moet rekening worden gehouden met de geldende interne beveiligingsrichtlijnen van de organisatie. De compliance check helpt ervoor te zorgen dat de wijzigingen voldoen aan geldende richtlijnen en intern beleid. Daarnaast wordt gekeken of de configuratiewijzigingen voldoen aan de beveiligingseisen van de CIS-Benchmark.

Taak	Actie
Controleer richtlijnen en intern beleid	Beoordeel de relevante (interne) richtlijnen die van invloed kan zijn op de wijzigingen.
Bespreek de relevante regelgeving	Bepaal gezamenlijk welk compliance-raamwerk van toepassing is binnen de organisatie/afdeling
Vergelijk de configuratiewijzigingen met de CIS-Benchmark	Vergelijk de wijzigingen met de CIS-Benchmark voor extra beveiligingsaanbevelingen

[1] https://learn.microsoft.com/nl-nl/mem/intune/fundamentals/manage-os-versions

5.1.3 Scope bepalen

Het bepalen van de scope houdt in dat moet worden vastgesteld welke gebruikers, apparaten en groepen door de wijziging getroffen worden. Het is belangrijk om duidelijk te definiëren wie de wijzigingen gaan ontvangen, bijvoorbeeld specifieke afdelingen of gebruikersgroepen, en welke systemen of applicaties onder de wijziging vallen.

Taak	Actie
Definieer de scope	Bepaal welke afdelingen, teams of gebruikersgroepen de wijziging moet ontvangen.
Bepaal systemen en applicaties	Stel vast welke systemen en applicaties onder de wijzigingen vallen.
Communicatieplan opstellen (indien gewenst)	Plan hoe de wijziging aan de betrokkenen wordt gecommuniceerd.
Evalueren van onbedoelde impact	Controleer of er systemen zijn die per ongeluk kunnen worden beïnvloed door de wijziging.

5.1.4 Acceptatie criteria vastleggen

Tijdens de voorbereidingsfase moeten ook acceptatie criteria worden vastgelegd. Het gaat hier om twee soorten criteria, namelijk: business acceptatie criteria en acceptatie criteria van het beheerteam. Deze stap is belangrijk om ervoor te zorgen dat de verantwoordelijkheden voor de nieuwe configuraties duidelijk zijn voor het beheerteam en de organisatie.

Taak	Actie
Leg de business acceptatie criteria vast	Definieer de vereisten en verwachtingen van de organisatie voor acceptatie van nieuwe configuraties
Leg de acceptatie criteria van het dagelijks beheerteam vast	Stel de operationele en technische voorwaarden vast voor een succesvolle implementatie

5.2 Testen

De testfase is een belangrijke stap om te controleren of de wijzigingen zoals beoogd functioneren, zonder negatieve gevolgen voor de systemen of gebruikers. Door deze fase zorgvuldig uit te voeren, kunnen beheerders er zeker van zijn dat de wijzigingen veilig en effectief kunnen worden uitgerold.

5.2.1 Test-lab

Het opzetten van een testomgeving is nodig om een gecontroleerde omgeving te hebben waarin de configuratiewijzigingen getest kunnen worden. De testomgeving moet zo dicht mogelijk bij de productieomgeving liggen om representatieve resultaten te verkrijgen. Binnen de testomgeving kunnen configuraties worden uitgeprobeerd om vast te stellen hoe de wijzigingen zich gedragen voordat ze daadwerkelijk worden geïmplementeerd. Indien de configuratie wijziging niet succesvol is, moet er een nieuwe evaluatie van de risico’s plaatsvinden. De niet geïmplementeerde wijzigingen kunnen mogelijk resulteren in blijvende cyberbeveiligingsrisico’s, die in de evaluatie opnieuw moeten worden beoordeeld. Hierbij dient gekeken te worden of deze instellingen in de toekomst alsnog geïmplementeerd kunnen worden en of er compenserende maatregelen mogelijk zijn, bijvoorbeeld door deze extra met use cases door het SOC te laten monitoren.

Taak	Actie
Testomgeving opzetten	Stel een testomgeving in die lijkt op de productieomgeving.
Configuratie testen	Pas dezelfde hardeningsinstellingen toe zoals later in de productieomgeving.

5.2.2 Prestatietest (kritieke systemen)

Deze stap is alleen noodzakelijk wanneer de configuratiewijzingen doorgevoerd worden op systemen met speciale toepassing, zoals devices die cruciale bedrijfsprocessen ondersteunen. Door prestaties te meten en te vergelijken met een vooraf vastgestelde verwachting, kunnen beheerders bepalen of de wijzigingen positief, neutraal of negatief effect hebben op de systeemprestaties en business processen.

Taak	Actie
Bepaal de baseline voor de systeemprestaties	Bepaald wat de prestatiestandaarden zijn die nu voor de systemen geïmplementeerd zijn.
Test systeemprestaties	Voer prestatietests uit om de prestaties van systemen na de wijziging te controleren.
Vergelijk met baseline	Vergelijk de prestatiegegevens met de gegevens vóór de wijziging.

5.2.3 Impact meten

Het meten van de impact van de wijzigingen is nodig om te begrijpen hoe deze veranderingen de business processen beïnvloeden. Dit omvat zowel technische prestaties als gebruikservaringen, en helpt om een compleet beeld te krijgen van de gevolgen van de configuratiewijzigingen.

Taak	Actie
Identificeer de impact	Meet de invloed van de wijziging
Controleer op ongewenste effecten	Kijk of de wijziging onverwachte gevolgen heeft op business processen

5.2.4 Documenteren

Documentatie speelt een belangrijke rol in het vastleggen van de resultaten en bevindingen van de testfase. Een gedetailleerd verslag van de testresultaten, bevindingen en eventuele problemen helpt bij toekomstige implementaties en zorgt voor transparantie naar alle betrokkenen.

Taak	Actie
Documenteer testresultaten	Leg de resultaten van de tests vast in een verslag waar de verwachte en werkelijke resultaten
Beschrijf bevindingen	Noteer gevonden problemen en bijzonderheden die tijdens de tests en de analyse zijn ontdekt.
Update ontwerpdocumentatie	Ontwerpdocumentatie dient naar aanleiding van de testen aangepast te worden aan de nieuwe situatie (configuratie zoals die daadwerkelijk in productie gebruikt wordt)

5.3 Pilot

In dit hoofdstuk wordt de uitrol van de configuratiewijzigingen behandeld. De uitrol vindt plaats in verschillende fasen om te zorgen voor een gecontroleerde implementatie.

5.3.1 Pilot – kleine gecontroleerde groep

De pilotfase houdt in dat de configuratiewijzigingen eerst op een beperkte schaal worden uitgerold. Dit helpt om te zien hoe de wijzigingen zich gedragen in een realistische, maar nog steeds gecontroleerde omgeving. Door eventuele problemen in deze fase te identificeren en op te lossen, kan de uitrol naar een grotere groep worden uitgevoerd. Deelnemers in de pilotgroep nemen actief deel te nemen door problemen te identificeren en nieuwe configuraties actief te gebruiken tijdens hun dagelijkse werkzaamheden.

Adviezen voor de grootte van de pilotgroep:

- Organisaties met 0-100 gebruikers: 10-20% van de gebruikers (minimaal 5 gebruikers).
- Organisaties met 100-500 gebruikers: 5-10% van de gebruikers (minimaal 20 gebruikers).
- Organisaties met meer dan 500 gebruikers: 2-5% van de gebruikers (minimaal 50 gebruikers).

Adviezen voor de samenstelling van de pilotgroep:

- Kies ten minste voor gewone en voor bijzondere gebruikers die een andere set met functionaliteiten hebben op hun werkstations (b.v. ontwikkelaars en beheerders) en gebruikers die een apparaat hebben waarmee een kritisch business proces ondersteunt wordt.
- Kies van elk kritisch bedrijfsproces minimaal 1 device / 1 medewerker (*Let op: hierbij wordt uitgegaan van de afwezigheid van single points of failure.*)

Taak	Actie
Selecteer pilotgroep	Kies een representatieve groep gebruikers
Uitrollen wijzigingen	Implementeer de configuratiewijzigingen binnen deze pilotgroep.

5.3.2 Bewaking

Gedurende de gehele pilotfase is bewaking van belang. Dit zorgt ervoor dat eventuele problemen snel kunnen worden geïdentificeerd en opgepakt. Bewaking helpt ook om te bevestigen dat de wijzigingen de gewenste effecten hebben en niet leiden tot ongewenste effecten.

Taak	Actie
Bepaal de bewakingsdoelstellingen	Bepaal de duur voor de bewaking zodat duidelijk is wanneer deze fase kan eindigen.
Raadpleeg escalatieplan (indien nodig)	Het escalatieplan kan worden ingezet wanneer er onverwachte storingen optreden.
Real-time bewaking (Indien gewenst)	Gebruik bewakingstools om de systemen in real-time te volgen.
Analyseren van logbestanden	Bekijk logbestanden om eventuele fouten of problemen te detecteren.
Gebruikersfeedback verzamelen	Houd contact met gebruikers om hun ervaringen te peilen.

5.3.3 Evaluatie

Na de uitrol naar de pilotgroep volgt een korte evaluatiefase. In deze fase wordt beoordeeld of de configuratiewijzigingen het gewenste effect hebben, of er onverwachte gevolgen zijn en of verdere aanpassingen nodig zijn. Dit is de laatste stap voordat de wijzigingen breder worden uitgerold. De gebruikers in de pilotgroep spelen een belangrijke rol in deze fase, omdat zij het beste kunnen beoordelen wat de impact is op de dagelijkse werkzaamheden en kritieke bedrijfsprocessen. Op

basis van hun feedback wordt bepaald of de wijzigingen kunnen worden doorgevoerd in de productieomgeving. Als de pilotgroep geen akkoord geeft, bekijkt het beheerteam het ontwerp opnieuw en past het waar nodig aan, zodat de configuratiewijzigingen op een zorgvuldige manier kunnen worden geïmplementeerd zonder bedrijfsprocessen te verstoren.

Taak	Actie
Resultaten evalueren	Beoordeel de prestaties en feedback na de uitrol.
Documenteren bevindingen	Leg alle bevindingen vast voor toekomstige referentie.
Beslissen over volledige uitrol	Maak op basis van de evaluatie een beslissing over de verdere uitrol.
Communiceren met belanghebbenden	Informeer alle betrokkenen over de uitkomsten en volgende stappen.

5.4 Uitrol

Uitrol betreft de definitieve uitrol van de configuratiewijzigingen naar alle gebruikers die binnen de eerder gedefinieerde scope vallen. Deze fase bouwt voort op de ervaringen en resultaten van de pilotfase en is bedoeld om de wijzigingen in productie te brengen.

5.4.1 Uitrol productieomgeving

Tijdens deze fase worden de configuratiewijzigingen uitgerold naar alle gebruikers en systemen die binnen de scope van de wijzigingen vallen. Afhankelijk van de omvang van de organisatie kan de uitrol in de productieomgeving gefaseerd worden uitgevoerd. Bij een kleinere omgeving (100-200 medewerkers) kan de uitrol in één keer plaatsvinden. Het is echter aan te raden onderscheid te maken tussen standaardgebruikers en gebruikers die betrokken zijn bij kritische bedrijfsprocessen. Gebruikers binnen deze kritische processen kunnen apart worden behandeld en stapsgewijs de nieuwe configuraties ontvangen.

Taak	Actie
Communiceren met betrokkenen	Informeer gebruikers en betrokkenen over de aanstaande wijziging.
Uitrol plannen	Stel een gedetailleerde planning op voor de uitrol. Gebruikers die betrokken zijn bij kritische bedrijfsprocessen worden apart genomen, waarbij elke paar dagen een medewerker de nieuwe configuratie ontvangt.
Uitrollen change	Implementeer de configuratiewijzigingen zoals gepland.
Ondersteuning	Zorg voor ondersteuning voor gebruikers tijdens de uitrol.

5.4.2 Bewaking & Documentatie

Nadat de configuratiewijzigingen zijn uitgerold, is het belangrijk om een fase van bewaking en documentatie te volgen. De documentatie omvat alle relevante informatie voor toekomstige referentie en eventuele audits.

Taak	Actie
Gebruikersfeedback verzamelen	Verzamel feedback van gebruikers
Resultaten documenteren	Documenteer alle bevindingen en leerpunten voor toekomstige referentie.

5.5 Evalueren

De evaluatiefase heeft als doel te bepalen of de configuratiewijzigingen succesvol zijn geïmplementeerd. In deze fase wordt ook nazorg geleverd, en de evaluatie dient om lessen te trekken voor toekomstige wijzigingen.

5.5.1 Nazorg

Nazorg is gericht op het ondersteunen van gebruikers en het oplossen van eventuele problemen na de uitrol.

Taak	Actie
Gebruikersondersteuning	Bied extra ondersteuning aan gebruikers bij problemen en vragen.
Kennisoverdracht	Zorg ervoor dat de helpdesk en supportteams goed geïnformeerd zijn over de wijzigingen en mogelijke problemen.

5.5.2 Beheer en Optimalisatie

Optimalisatie richt zich op het verbeteren van de configuraties op basis van de feedback en de verzamelde gegevens om de efficiëntie en effectiviteit te maximaliseren. Deze stap in de implementatieplan dient regelmatig uitgevoerd te worden, bijvoorbeeld minimaal eenmaal per jaar. Het is belangrijk om de bestaande policies en instellingen te herzien om te bepalen of ze nog goed functioneren en up-to-date zijn. Daarnaast kan hierbij ook gekeken worden naar bijvoorbeeld inactieve accounts.

Taak	Actie
Implementeren van verbeteringen	Pas de configuraties indien mogelijk aan op basis van de analyse om problemen te op te lossen.
Evaluatie van bestaande configuraties	Minimaal jaarlijkse opschoning van policies, settings, privileged access en andere registraties in M365.
Bijwerken documentatie	Werk de documentatie bij met de aangebrachte wijzigingen en/of verbeteringen.

5.6 Policy aanbevelingen

Het correct inrichten van policies in Microsoft Intune Admin Center vraagt om zorgvuldige planning en uitvoering. Door duidelijke titels, consistente naamgevingsconventies, duidelijke en volledige omschrijvingen en gedetailleerde documentatie te hanteren, wordt een gestructureerde en beheersbare beveiliging van het platform mogelijk. Het testen van policies voordat ze worden uitgerold en het regelmatig evalueren ervan zorgt ervoor dat de configuraties voldoen aan de beveiligingsdoelen van de organisatie. Hier volgen enkele aanbevelingen en best practices:

- Policy name
  - Gebruik een duidelijke en beschrijvende naam voor elke policy: "[Platform] - [Policy Type] - [Beschrijving]".
  - Vermijd het gebruik van afkortingen die niet algemeen bekend zijn.
  - Gebruik consistente naamgevingsconventies voor policies om beheer eenvoudiger te maken.
- Omschrijving
  - Voeg een duidelijke en beknopte omschrijving toe aan elke policy om het doel en inhoud ervan te verduidelijken.
  - Beschrijf in de omschrijving wat de policy doet, voor welke gebruikers of apparaten deze van toepassing is en eventuele specifieke groep.

- Platformkeuze:
    - Kies het juiste platform voor de policy. Voor policies gericht op Windows-apparaten, selecteer "Windows 10 en hoger".
    - Controleer regelmatig of de gekozen platforminstellingen nog steeds actueel zijn en voldoen aan het securitybeleid van de organisatie.
- Beperking van veranderingen per policy:
    - Splits configuraties op in meerdere policies wanneer mogelijk. Dit helpt bij het gemakkelijker identificeren en oplossen van problemen.
- Documentatie en Versiebeheer:
    - Documenteer elke policy en houd wijzigingen bij om te weten wat er is gewijzigd, wanneer en door wie.
    - Gebruik een centrale opslagplaats voor documentatie en versiebeheer. Noteer belangrijke details zoals beleidsdoel, toegepaste groepen en eventuele afwijkingen van de standaardconfiguraties.
- Beheer en Evaluatie:
    - Stel een evaluatiecyclus in, bijvoorbeeld elke vijf maanden, om policies te herzien en aan te passen waar nodig.

Uitgave

Versterken SOC Stelsel Rijk (VSSR)

Postbus 117, 2501 CC Den Haag

Turfmarkt 147, 2511 DP Den Haag

070 751 5555

Meer informatie

https://www.ncsc.nl/vssr

info@ncsc.nl

vssr.info@minjenv.nl (Rijksoverheid)

Maart 2025