TLP:GREEN

OR-9 CONFIGURATIEHANDLEIDING

Monitoring & Detectie – SOC Operational Readiness – **Applicatie Hardening**

Best Practice versie 1.2

Complexiteit document

Eenvoudig

Samenwerken maakt

DIGITAAL VEILIGER

VSSR

Inhoudsopgave

Voorwoord 3
Achtergrond 3
Doelgroep 3

1. Documentgegevens 4
2. Context miniproducten 5
3. Inleiding 6
3.1 Doel 6
3.2 Wat is applicatie hardening? 6
3.3 Randvoorwaarden 6
3.4 Raamwerken 7
3.5 Leeswijzer 7
4. Applicatie hardening 8
4.1 Hardening settings 8
4.2 Aanmaken van Policies in Apps 8
4.3 Microsoft Word & Powerpoint 8
4.4 Microsoft Outlook 10
4.5 Microsoft Excel 11
4.6 Microsoft Edge 13
4.7 Adobe 15

Bijlage I – Configuratiestatus checklist 16

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 monitoring- 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. Monitoring 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. Dit document maakt onderdeel uit van een set van miniproducten die rijksorganisaties helpt om een aantal SOC operationele randvoorwaarden in te richten.

Doelgroep

Versterken SOC Stelsel Rijk (VSSR) biedt met dit document handvatten voor Windows IT-beheerders, Systeemeigenaren, IT-Assetmanagers, Uitbestedingsmanagers, Security vertegenwoordigers en functionarissen betrokken bij informatiebeveiliging.

1. Documentgegevens

1.1 Documenthistorie

Versie	Datum	Omschrijving
V1.0	21-03-2025	Initiële versie
V1.1	03-11-2025	Toevoeging “Bijlage I – Configuratiestatus checklist”
V1.2	08-07-2026	Referenties geactualiseerd

1.2 Referenties

Document	Link
Checklist basisbeveiliging (OR-5)	Zie "Checklist basisbeveiliging ..(OR-5)" onder SOC Operational Readiness (Configuratie & Logging)
Generiek implementatieplan voor OR-6 t/m OR-9	Zie "Generiek implementatieplan” onder Platform/Applicatie Hardening & Malware bescherming (OR-6 t/m OR-9). Onderdeel van SOC Operational Readiness (Configuratie & Logging)
CIS Benchmark	https://www.cisecurity.org/cis-benchmarks
Microsoft Security baseline	https://learn.microsoft.com/en-us/windows/security/operating-system-security/device-management/windows-security-configuration-framework/windows-security-baselines
VSSR-kennisdocumenten	VSSR (ncsc.nl)

1.3 Definities

Term	Omschrijving
Entra ID	Microsoft cloudgebaseerde identiteits- en toegangsbeheeroplossing
Macros	Geautomatiseerde scripts of opdrachten die bepaalde taken kunnen automatiseren

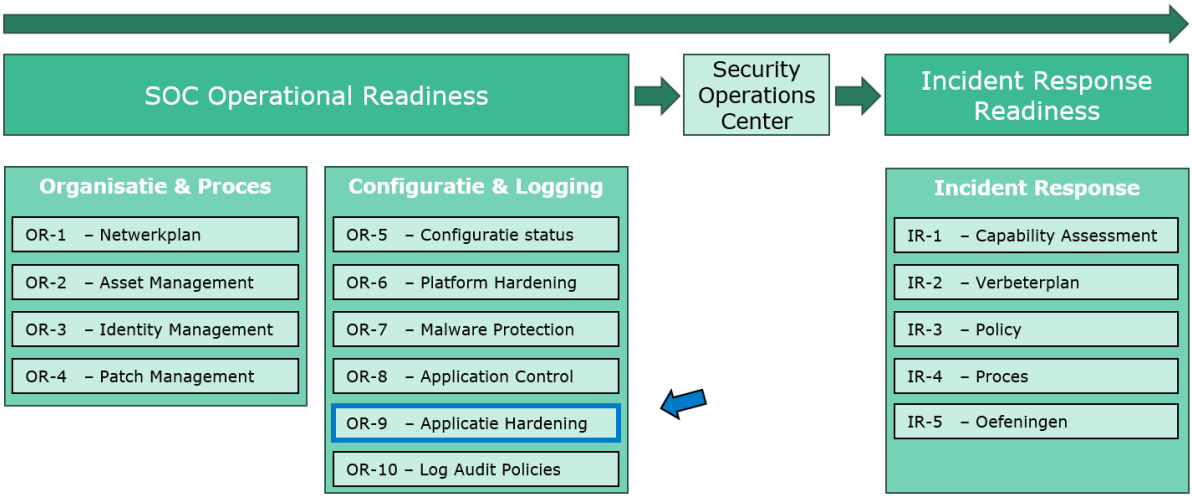
Ter verduidelijking van de overige terminologie en begrippen die in dit document worden gebruikt is er een verzameling van definities te vinden op Woordenboek - Cyberveilig Nederland.

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 de configuratiehandleiding is voor Applicatie Hardening (OR-9), binnen **Configuratie & Logging**, behandelt.

3. Inleiding

In dit hoofdstuk wordt stilgestaan bij het doel van dit document, namelijk basis applicatie hardening. Daarnaast worden de randvoorwaarden besproken die nodig zijn om deze configuratiehandleiding te kunnen gebruiken en de geraadpleegde raamwerken.

3.1 Doel

Het doel van deze configuratiehandleiding is om organisaties een startpunt te bieden voor de basis hardening van veelgebruikte generieke gebruikersapplicaties, zoals webbrowsers en officepakketten. Hardening omvat het aanpassen van configuraties om veiligheidsrisico's minimaliseren. Deze handleiding biedt een eerste stap in het verbeteren van de beveiliging binnen organisaties. Een belangrijk onderdeel hiervan is de Microsoft 365 Apps for Enterprise Security Baseline. De baseline is afgestemd op de beveiligingsaanbevelingen voor het Microsoft 365 Apps for Enterprise groepsbeleid en biedt richtlijnen voor het configureren en aanpassen van door Microsoft aanbevolen securityinstellingen. De configuraties in deze handleiding zijn bedoeld om de meest basale zwakke plekken aan te pakken, maar bieden geen volledige bescherming. Voor een uitgebreide beveiliging zijn aanvullende maatregelen nodig, afgestemd op de specifieke risico's en behoeften van de organisatie. Met deze handleiding kunnen organisaties een begin maken met het opzetten van een IT-omgeving die beter voorbereid is op veelvoorkomende dreigingen. Deze handleiding beschrijft de aanbevolen configuratiewijzigingen, maar deze omvatten niet direct de uitrol. De deployment dient als een aparte stap te worden uitgevoerd. Voor een uitgebreide toelichting op het uitrolproces wordt verwezen naar de implementatiehandleiding.

3.2 Wat is applicatie hardening?

Deze handleiding richt zich op de basis hardening instellingen voor veelgebruikte toepassingen binnen organisaties, zoals Microsoft Word, PowerPoint, Outlook, Excel en Adobe. De hardening wordt uitgevoerd binnen Microsoft Intune. Hiervoor is gebruik gemaakt van de Microsoft 365 Apps for Enterprise Security Baseline.

3.3 Randvoorwaarden

Om de configuratiehandelingen in deze handleiding te kunnen uitvoeren, dient aan een aantal essentiële randvoorwaarden te worden voldaan. Deze voorwaarden zijn belangrijk om ervoor te zorgen dat de hardeningprocessen correct worden geïmplementeerd. De minimale vereisten zijn als volgt:

- **Toegang tot een Windows Enterprise omgeving:** Een licentie voor Windows 11 Enterprise is vereist om de beschreven hardeningmaatregelen toe te passen.
- **Minimaal Microsoft E3 Licentie:** Deze licentie biedt de noodzakelijke beveiligings- en beheertools die essentieel zijn voor platform hardening.
- **Aanwezigheid van Microsoft Intune:** Microsoft Intune is vereist voor het beheer van apparaten en voor het afdwingen van beveiligingsbeleid op alle apparaten binnen de organisatie.
- **Basiskennis van Microsoft Intune:** Dit omvat het begrijpen van hoe je apparaten kunt onboarden, policies kunt opstellen en implementeren, en hoe je rapportages en monitoring kunt uitvoeren binnen Intune (bijvoorbeeld MD-102).
- **Apparaat management via Intune:** Dit is noodzakelijk voor het centraal beheren van beveiligingsinstellingen en voor de uitvoering van hardeningmaatregelen voor Intune managed devices.

- **Onboarding van alle apparaten in Entra ID:** Apparaten moeten minimaal geregisteerd zijn in Entra ID, bijvoorkeur Entra ID joined.
    - Bij gebruik van lokale Active Directory, moet Entra Connect of Cloud Sync ingeschakeld zijn.

3.4 Raamwerken

Deze handleiding maakt gebruik van twee frameworks om de hardening van de Windows Enterprise-apps te ondersteunen. De CIS-Benchmarks, ontwikkeld door het Center for Internet Security (CIS), bieden gedetailleerde, stapsgewijze instructies voor het veilig configureren van IT-systemen. Daarnaast wordt de Security Baseline for Microsoft 365 Apps gebruikt. Deze helpt IT-beheerders bij het bij het samenstellen van een uitgebalanceerde configuratie die rekening houdt met zowel beveiliging als productiviteit. Deze baseline is afgestemd op de beveiligingsaanbevelingen voor het Microsoft 365 Apps for Enterprise groepsbeleid en biedt richtlijnen voor het configureren en aanpassen van door Microsoft aanbevolen beleidsinstellingen.

3.5 Leeswijzer

Deze handleiding richt zich op het aanmaken van policies in Microsoft Intune om een begin aan applicatie hardening mogelijk te maken. In hoofdstuk 3.2 wordt een beknopte uitleg gegeven over het proces van het vinden van de configuraties. In de overige hoofdstukken worden de verschillende configuraties toegelicht.

Bij de instellingen is telkens aangegeven wat het niveau van hardening is (Level 1 t/m 5). Dit niveau geeft de mate van compleetheid waarin de basis hardening is geïmplementeerd en vormt een startpunt voor verdere beveiliging.

Daarnaast is aangeven op welk scherm de instelling gewijzigd kan worden. Naast de aanbevolen instelling is ook een onderbouwing aangegeven van de instelling.

4. Applicatie hardening

In dit hoofdstuk wordt stap voor stap uitgelegd hoe basis applicatie hardening kan worden geconfigureerd binnen de organisatie.

4.1 Hardening settings

In dit hoofdstuk worden aanbevelingen gedaan voor configuratiewijzigingen die kunnen bijdragen aan de eerste stap in het versterken van de beveiliging van standaardapplicaties, zoals Word, PowerPoint, Excel, Microsoft Edge en Adobe. De aanbevolen configuraties bieden een basis voor het hardenen van applicaties binnen de organisatie. De configuraties kunnen worden aangepast door het aanmaken van policies in de sectie "Apps" onder "Policies for Office" in Microsoft Intune.

4.2 Aanmaken van Policies in Apps

Het aanmaken van policies in *Apps* > *Policies for Office apps* is een belangrijk onderdeel van het beveiligen van je Office-omgeving. Het volgende hoofdstuk bestaat uit hardenings aanbevelingen die middels een policy in te regelen zijn. Onderstaande stappen kunnen bij elke wijziging gevolgd worden:

1. Policy per Applicatie Aanmaken:
    - Begin met het aanmaken van een afzonderlijke policy voor elke Office-applicatie.
    - Geef de policy een duidelijke naam die de betreffende applicatie reflecteert, bijvoorbeeld "Security Policy voor Word".
    - Specificeer in de beschrijving van de policy waar deze over gaat. Dit kan bijvoorbeeld zijn: "Beveiligingsinstellingen voor Word om macro's uit te schakelen" of "Encryptie-instellingen voor Outlook e-mails".
2. Scope Instellen:
    - Indien nodig, kun je de scope aanpassen aan specifieke gebruikersgroepen of afdelingen binnen de organisatie.
3. Configuratie-instellingen Weergeven en Security Baseline Kiezen:
    - Na het aanmaken van de policy verschijnt een scherm waar alle configuratie-instellingen voor Office-apps worden weergegeven.
    - Per applicatie kan een filter aangemaakt worden om de relevante instellingen te zien.
    - Kies voor de *security baseline* om ervoor te zorgen dat de configuratie-instellingen voldoen aan de Microsoft aanbevolen beveiligingsstandaarden. Dit maakt het eenvoudiger om te focussen op de specifieke beveiligingsinstellingen die nodig zijn voor elke applicatie.

4.3 Microsoft Word & Powerpoint

Het instellen van beveiligingsmaatregelen voor Microsoft Word en PowerPoint helpt om risico's zoals malware, phishing en exploits via kwaadaardige documenten te minimaliseren. **Test de instellingen altijd vooraf in een gecontroleerde omgeving (audit mode) voordat ze breed worden uitgerold, om mogelijke impact op bedrijfsprocessen te beoordelen.**

Block Macros from Running in Office Files from the Internet	
Configuratie-niveau	L1
Intune	Apps > Policies for Office apps
Aanbevolen configuratie	• Maak een policy • Kies de juiste scope • Zoek naar de configuratie in de titel • Selecteer: Microsoft recommended baseline

Block Macros from Running in Office Files from the Internet	
Toelichting	Deze instelling blokkeert het uitvoeren van macro's in Office-bestanden afkomstig van het internet, zelfs als "Enable all macros" is geselecteerd in het Trust Center.
Handleiding	Macros from the internet are blocked by default in Office - Microsoft 365 Apps | Microsoft Learn

VBA Macro Notification Settings	
Configuratie-niveau	L4
Intune	Apps > Policies for Office apps
Aanbevolen configuratie	• Maak een policy • Kies de juiste scope • Zoek naar de configuratie in de titel • Selecteer: Microsoft recommended baseline
Toelichting	De instelling bepaalt hoe de toepassing gebruikers waarschuwt wanneer Visual Basic for Applications (VBA) macro's aanwezig zijn in documenten. De instelling schakelt meldingen in bij het gebruik van VBA-macro's om gebruikers te waarschuwen.
Handleiding	Macros from the internet are blocked by default in Office - Microsoft 365 Apps | Microsoft Learn

Scan Encrypted Macros in Word Open XML Documents	
Configuratie-niveau	L5
Intune	Apps > Policies for Office apps
Aanbevolen configuratie	• Maak een policy • Kies de juiste scope • Zoek naar de configuratie in de titel • Selecteer: Microsoft recommended baseline
Toelichting	Deze instelling bepaalt of versleutelde macro's in Open XML-documenten gescand moeten worden door antivirussoftware voordat ze worden geopend.
Handleiding	Macros from the internet are blocked by default in Office - Microsoft 365 Apps | Microsoft Learn

Require that application add-ins are signed by Trusted Publisher	
Configuratie-niveau	L4
Intune	Apps > Policies for Office apps
Aanbevolen configuratie	• Maak een policy • Kies de juiste scope • Zoek naar de configuratie in de titel • Selecteer: Microsoft recommended baseline
Toelichting	Deze instelling bepaalt of add-ins voor een toepassing digitaal moeten worden ondertekend door een vertrouwde uitgever. Wanneer deze instelling is ingeschakeld, controleert de toepassing de digitale handtekening van elke add-in. Als een add-in niet is ondertekend, wordt deze uitgeschakeld en ontvangt de gebruiker een melding.
Handleiding	List of settings for the Microsoft 365 Apps for Enterprise security baseline in Intune - Microsoft Intune | Microsoft Learn

Disable Trust Bar Notification for Unsigned Application Add-ins and Block them	
Configuratie-niveau	L5
Intune	Apps > Policies for Office apps
Aanbevolen configuratie	• Maak een policy • Kies de juiste scope • Zoek naar de configuratie in de titel • Selecteer: Microsoft recommended baseline
Toelichting	Deze instelling bepaalt of een Office-toepassing gebruikers waarschuwt wanneer unsigned add-ins worden geladen, of deze add-ins stilzwijgend uitschakelt zonder melding. Als deze instelling is ingeschakeld, worden unsigned add-ins automatisch uitgeschakeld zonder de gebruiker te waarschuwen.
Handleiding	List of settings for the Microsoft 365 Apps for Enterprise security baseline in Intune - Microsoft Intune | Microsoft Learn

Set default file block behavior	
Configuratie-niveau	L1
Intune	Apps > Policies for Office apps
Aanbevolen configuratie	• Maak een policy • Kies de juiste scope • Zoek naar de configuratie in de titel • Selecteer: Microsoft recommended baseline
Toelichting	Deze instelling bepaalt of gebruikers Word-bestanden kunnen openen, bekijken of bewerken, afhankelijk van het blokkeren van bepaalde bestandstypen. Als deze instelling is ingeschakeld, kun je specificeren of geblokkeerde bestanden niet geopend kunnen worden, alleen in de beveiligde weergave (Protected View) geopend kunnen worden zonder bewerkingsmogelijkheden, of in de beveiligde weergave geopend kunnen worden met bewerkingsmogelijkheden.
Handleiding	List of settings for the Microsoft 365 Apps for Enterprise security baseline in Intune - Microsoft Intune | Microsoft Learn

4.4 Microsoft Outlook

Het configureren van beveiligingsinstellingen voor Microsoft Outlook helpt om risico's zoals phishing, schadelijke bijlagen en misbruik van e-mailfunctionaliteiten te verminderen. **Test de instellingen altijd vooraf in een gecontroleerde omgeving voordat ze breed worden uitgerold, om de impact op functionaliteit en gebruikerservaring te beoordelen.**

Outlook Security Mode	
Configuratie-niveau	L4
Intune	Apps > Policies for Office apps
Aanbevolen configuratie	• Maak een policy • Kies de juiste scope • Zoek naar de configuratie in de titel • Selecteer: Microsoft recommended baseline
Toelichting	Deze instelling bepaalt welke set beveiligingsinstellingen in Outlook wordt afgedwongen. Als deze instelling is ingeschakeld, kun je kiezen voor een beveiligingsconfiguratie die via Group Policy wordt beheerd. Dit zorgt voor een consistent beveiligingsniveau en maakt het mogelijk om specifieke beleidsinstellingen op Outlook toe te passen.
Handleiding	List of settings for the Microsoft 365 Apps for Enterprise security baseline in Intune - Microsoft Intune | Microsoft Learn

Prevent Users from Customizing Attachment Security Settings	
Configuratie-niveau	L3
Intune	Apps > Policies for Office apps
Aanbevolen configuratie	• Maak een policy • Kies de juiste scope • Zoek naar de configuratie in de titel • Selecteer: Microsoft recommended baseline
Toelichting	Deze instelling voorkomt dat gebruikers de blokkering van bijlagen in Outlook aanpassen. Als je deze instelling inschakelt, kunnen gebruikers de door Outlook geblokkeerde bijlagen niet wijzigen, wat zorgt voor een striktere beveiliging tegen potentieel gevaarlijke bestanden.
Handleiding	List of settings for the Microsoft 365 Apps for Enterprise security baseline in Intune - Microsoft Intune | Microsoft Learn

Do not Allow Outlook object model Scripts to Run for Public Folders	
Configuratie-niveau	L5
Intune	Apps > Policies for Office apps
Aanbevolen configuratie	• Maak een policy • Kies de juiste scope • Zoek naar de configuratie in de titel • Selecteer: Microsoft recommended baseline
Toelichting	Deze instelling voorkomt dat Outlook-objectmodellenscripts worden uitgevoerd. Het uitvoeren van dergelijke scripts kan een beveiligingsrisico vormen, omdat kwaadwillende scripts toegang kunnen krijgen tot gevoelige gegevens binnen de organisatie.
Handleiding	List of settings for the Microsoft 365 Apps for Enterprise security baseline in Intune - Microsoft Intune | Microsoft Learn

4.5 Microsoft Excel

Het instellen van beveiligingsmaatregelen voor Microsoft Excel helpt om risico's zoals schadelijke macro's of exploits via kwaadaardige bestanden te beperken. **Test de instellingen altijd vooraf in een gecontroleerde omgeving voordat ze breed worden uitgerold, om de impact op functionaliteit en gebruikerservaring te beoordelen.**

Block Macros from Running in Office Files from the Internet	
Configuratie-niveau	L1
Intune	Apps > Policies for Office apps
Aanbevolen configuratie	• Maak een policy • Kies de juiste scope • Zoek naar de configuratie in de titel • Selecteer: Microsoft recommended baseline
Toelichting	Deze instelling voorkomt dat macro's worden uitgevoerd in Office-bestanden die afkomstig zijn van het internet. Wanneer deze instelling is ingeschakeld, worden macro's geblokkeerd, zelfs als de optie "Alle macro's inschakelen" is geselecteerd in het Macro-instellingen gedeelte van het Trust Center. Gebruikers ontvangen een melding dat de macro's zijn geblokkeerd.
Handleiding	List of settings for the Microsoft 365 Apps for Enterprise security baseline in Intune - Microsoft Intune | Microsoft Learn

Block Excel XLL Add-ins that come from an Untrusted Source	
Configuratie-niveau	L3
Intune	Apps > Policies for Office apps
Aanbevolen configuratie	• Maak een policy • Kies de juiste scope • Zoek naar de configuratie in de titel • Selecteer: Microsoft recommended baseline
Toelichting	Deze instelling voorkomt dat Excel XLL-add-ins worden uitgevoerd als ze afkomstig zijn van een niet-vertrouwde bron. Als je deze instelling inschakelt, kun je ervoor kiezen om de add-ins volledig te blokkeren. Als je deze instelling uitschakelt of niet configureert, kunnen gebruikers de standaardinstellingen overschrijven door het register te wijzigen.
Handleiding	List of settings for the Microsoft 365 Apps for Enterprise security baseline in Intune - Microsoft Intune | Microsoft Learn

Prevent Excel from Running XLM Macros	
Configuratie-niveau	L4
Intune	Apps > Policies for Office apps
Aanbevolen configuratie	• Maak een policy • Kies de juiste scope • Zoek naar de configuratie in de titel • Selecteer: Microsoft recommended baseline
Toelichting	Deze instelling voorkomt dat Excel (XLM) macro's worden uitgevoerd. Als je deze instelling inschakelt, kunnen XLM-macro's niet in Excel worden uitgevoerd, maar als je de instelling uitschakelt of niet configureert, kunnen ze wel uitgevoerd worden.
Handleiding	List of settings for the Microsoft 365 Apps for Enterprise security baseline in Intune - Microsoft Intune | Microsoft Learn

Require that Application Add-ins are Signed by Trusted Publisher	
Configuratie-niveau	L4
Intune	Apps > Policies for Office apps
Aanbevolen configuratie	• Maak een policy • Kies de juiste scope • Zoek naar de configuratie in de titel • Selecteer: Microsoft recommended baseline
Toelichting	Deze instelling controleert of add-ins voor Office 2016-toepassingen digitaal moeten worden ondertekend door een vertrouwde uitgever. Als je deze instelling inschakelt, controleert Excel de digitale handtekening van elk add-in en schakelt het add-in uit als deze niet ondertekend is door een vertrouwde uitgever, waarbij de gebruiker wordt geïnformeerd.
Handleiding	List of settings for the Microsoft 365 Apps for Enterprise security baseline in Intune - Microsoft Intune | Microsoft Learn

4.6 Microsoft Edge

Dit hoofdstuk biedt een beginpunt voor het configureren van de applicatie-harding van Microsoft Edge, met als doel de beveiliging van de browser te versterken. We maken gebruik van de Security Baseline for Microsoft Edge om een basisniveau van bescherming te garanderen, door een beperkte selectie van instellingen toe te passen die specifiek gericht zijn op het verbeteren van de browserbeveiliging. Voor configuraties waarvoor geen specifieke optie in deze handleiding is opgenomen, dient de instelling op "Not Configured" te blijven, om onbedoelde wijzigingen te voorkomen. Alle configuratiewijzigingen moeten vooraf worden gevalideerd voordat ze voor alle gebruikers worden toegepast.

Allow users to proceed from the HTTPS warning page	
Configuratie-niveau	L1
Intune	Endpoint security > Security Baseline > Security Baseline for Microsoft Edge
Aanbevolen configuratie	Disable
Toelichting	Deze instelling bepaalt of gebruikers een waarschuwing pagina zien wanneer ze sites bezoeken met SSL-fouten in Microsoft Edge. Als je deze policy inschakelt of niet configureert (standaard), kunnen gebruikers de waarschuwing pagina's negeren, terwijl het uitschakelen van de policy voorkomt dat gebruikers door deze waarschuwingen heen klikken.
Handleiding	List of settings for the Microsoft Edge security baseline in Intune - Microsoft Intune | Microsoft Learn

Control which Extensions Cannot be Installed	
Configuratie-niveau	L3
Intune	Endpoint security > Security Baseline > Security Baseline for Microsoft Edge
Aanbevolen configuratie	Enabled (Voeg een lijst met toegestane extensions toe)
Toelichting	Deze instelling maakt het mogelijk om specifieke extensies te blokkeren die gebruikers niet kunnen installeren in Microsoft Edge. Wanneer deze policy wordt ingezet, worden alle extensies op de lijst uitgeschakeld en kunnen gebruikers ze niet opnieuw inschakelen; als een extensie van de lijst wordt verwijderd, wordt deze automatisch opnieuw ingeschakeld waar deze eerder was geïnstalleerd.
Handleiding	List of settings for the Microsoft Edge security baseline in Intune - Microsoft Intune | Microsoft Learn

Configure Edge TyposquattingChecker	
Configuratie-niveau	L1
Intune	Endpoint security > Security Baseline > Security Baseline for Microsoft Edge
Aanbevolen configuratie	Enable
Toelichting	Deze instelling stelt je in staat om te configureren of de Edge TyposquattingChecker ingeschakeld moet worden. De TyposquattingChecker biedt waarschuwingsberichten om gebruikers te beschermen tegen mogelijke typosquatting-websites. Typosquatting is een techniek waarbij kwaadwillenden profiteren van typfouten in webadressen om valse websites te creëren die lijken op legitieme sites, met als doel persoonlijke gegevens te stelen.
Handleiding	List of settings for the Microsoft Edge security baseline in Intune - Microsoft Intune | Microsoft Learn

Allow Basic authentication for HTTP	
Configuratie-niveau	L3
Intune	Endpoint security > Security Baseline > Security Baseline for Microsoft Edge
Aanbevolen configuratie	Disable
Toelichting	Deze instelling bepaalt of Basic-authenticatie wordt toegestaan via onveilige HTTP-verbindingen. Als je deze policy inschakelt of niet configureert (standaard), wordt Basic-authenticatie via niet-beveiligde HTTP-verbindingen toegestaan, terwijl het uitschakelen van de policy alleen beveiligde HTTPS-verbindingen toestaat voor Basic-authenticatie
Handleiding	Available Microsoft Defender SmartScreen settings | Microsoft Learn

Configure Microsoft Defender SmartScreen	
Configuratie-niveau	L2
Intune	Endpoint security > Security Baseline > Security Baseline for Microsoft Edge
Aanbevolen configuratie	Enabled
Toelichting	Deze instelling stelt je in staat om Microsoft Defender SmartScreen in te schakelen. Microsoft Defender SmartScreen biedt waarschuwingsberichten om gebruikers te beschermen tegen mogelijke phishing-aanvallen en schadelijke software.
Handleiding	Available Microsoft Defender SmartScreen settings | Microsoft Learn

Configure Microsoft Defender SmartScreen to Block Potentially Unwanted Apps	
Configuratie-niveau	L2
Intune	Endpoint security > Security Baseline > Security Baseline for Microsoft Edge
Aanbevolen configuratie	Enabled
Toelichting	Deze instelling stelt je in staat om het blokkeren van mogelijk ongewenste apps met Microsoft Defender SmartScreen in te schakelen. Dit blokkeert waarschuwingen voor apps zoals adware en coin miners
Handleiding	Available Microsoft Defender SmartScreen settings | Microsoft Learn

Prevent Bypassing Microsoft Defender SmartScreen Prompts for Sites	
Configuratie-niveau	L2
Intune	Endpoint security > Security Baseline > Security Baseline for Microsoft Edge
Aanbevolen configuratie	Enabled
Toelichting	Deze instelling bepaalt of gebruikers de waarschuwingen van Microsoft Defender SmartScreen over mogelijk schadelijke websites kunnen negeren.
Handleiding	Available Microsoft Defender SmartScreen settings | Microsoft Learn

Prevent bypassing Microsoft Defender SmartScreen Warnings about Downloads	
Configuratie-niveau	L3
Intune	Endpoint security > Security Baseline > Security Baseline for Microsoft Edge
Aanbevolen configuratie	Enabled
Toelichting	Deze instelling stelt je in staat te bepalen of gebruikers Microsoft Defender SmartScreen-waarschuwingen over niet-geverifieerde downloads kunnen negeren
Handleiding	Available Microsoft Defender SmartScreen settings | Microsoft Learn

4.7 Adobe

Het configureren van beveiligingsinstellingen voor Adobe-software helpt om risico's zoals schadelijke PDF-bestanden, ongeautoriseerde scriptuitvoering en exploits via kwetsbaarheden te verminderen. Test de instellingen altijd vooraf in een gecontroleerde omgeving voordat ze breed worden uitgerold, om de impact op functionaliteit en gebruikerservaring te beoordelen.

Block Adobe Reader from Creating Child Processes	
Configuratie-niveau	L2
Intune	*Devices > Windows > Compliance*
Aanbevolen configuratie	• Maak een policy • Zoek naar de configuratie in de titel • Selecteer: Block
Toelichting	Deze instelling voorkomt dat Adobe Reader nieuwe child processen creëert, wat kan helpen om aanvallen zoals code-executie via kwetsbaarheden in Adobe Reader te blokkeren. Het blokkeren van child processen helpt de beveiliging te verbeteren, omdat het moeilijker wordt voor kwaadaardige software om zich te verspreiden of een aanvallen uit te voeren.
Handleiding	Attack surface reduction rules reference - Microsoft Defender for Endpoint | Microsoft Learn

Bijlage I – Configuratiestatus checklist

Level	Configuration Control	Status
L1	Block Macros from Running in Office Files from the Internet (H 4.3 & 4.5)	
	Set default file block behavior (H 4.3)	
	Allow users to proceed from the HTTPS warning page (H 4.6)	
	Configure Edge TyposquattingChecker (H 4.6)	
L2	Configure Microsoft Defender SmartScreen to Block Potentially Unwanted Apps (H 4.6)	
	Prevent Bypassing Microsoft Defender SmartScreen Prompts for Sites (H 4.6)	
	Prevent Bypassing Microsoft Defender SmartScreen Warnings about Downloads (H4.6)	
	Configure Microsoft Defender SmartScreen (H 4.6)	
	Block Adobe Reader from Creating Child Processes (H 4.7)	
L3	Allow Basic authentication for HTTP (H 4.6)	
	Prevent Users from Customizing Attachment Security Settings (H 4.4)	
	Block Excel XLL Add-ins that come from an Untrusted Source (H 4.5)	
	Control which Extensions Cannot be Installed (H 4.6)	
L4	Require that application add-ins are signed by Trusted Publisher (H 4.3 & 4.5)	
	Outlook Security Mode (H 4.4)	
	Prevent Excel from Running XLM Macros (H 4.5)	
	VBA Macro Notification Settings (H 4.3)	
L5	Do not Allow Outlook object model Scripts to Run for Public Folders (H 4.4)	
	Disable Trust Bar Notification for Unsigned Application Add-ins and Block them (H 4.3)	
	Scan Encrypted Macros in Word Open XML Documents (H 4.3)	

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