TLP:GREEN

IMPLEMENTATIEPLAN

Monitoring & Detectie – SOC Operational Readiness - Patchmanagement

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 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 IT-architecten, IT-beheerders, Security vertegenwoordigers en functionarissen betrokken bij informatiebeveiliging.

1 Documentgegevens

1.1 Documenthistorie

Versie	Datum	Omschrijving
V1.0	19-02-2025	Initiële versie
V1.1	07-07-2026	Referenties geactualiseerd

1.2 Referenties

Document	Link
Patchmanagement Procesmodel	Zie "OR-4, Patchmanagement Procesmodel" onder SOC Operational Readiness - Producten
VSSR-kennisdocumenten	VSSR (ncsc.nl)

1.3 Definities

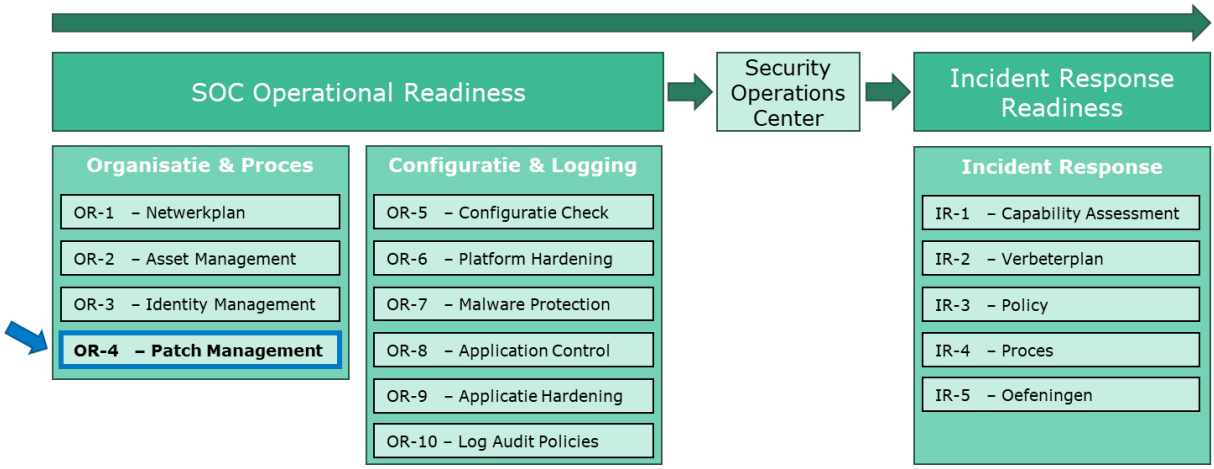
Ter verduidelijking van de terminologie en begrippen die in dit document worden gebruikt is er een verzameling van definities te vinden op Woordenboek - Cyberveilig Nederland.

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 **Organisatie & Proces** 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 Tabel 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 **Implementatieplan** voor **Patch Management** (OR-4), binnen **Organisatie & Proces**, behandelt.

Organisatie & Proces	Configuratie & Logging
Procesmodel	Configuratiehandleiding
Implementatieplan	Implementatieplan (generiek of specifiek)
Inventarisatiesheet	Progressie checklist

Tabel 1 - Miniproducten breakdown

3 Inleiding

Effectief patchmanagement is essentieel om de IT-infrastructuur van een organisatie te beschermen tegen cyberdreigingen en softwarefouten. Dit stappenplan schetst een eenvoudige implementatiewijze in een aantal stappen dat is afgestemd op kleine tot middelgrote organisaties. Het te implementeren patchmanagementproces heeft als doel kwetsbaarheden tijdig op te lossen zodat een SOC geen (onnodige) tijd kwijt is met het aandacht geven aan bekende kwetsbaarheden.

De te nemen stappen hebben een directe relatie met het procesmodel voor patchmanagement. De eerste keer dat patchmanagement gebruikt gaat worden zullen de stappen in dit plan leiden tot de implementatie van het beschreven proces.

Ook heeft dit stappenplan een relatie met andere processen, waarbij assetmanagement een belangrijk onderdeel is. Bij iedere patch wordt een afweging gemaakt tussen het belang van de asset waar zicht een kwetsbaarheid bevindt, het risico wat de kwetsbaarheid in zicht heeft en het risico van de patchimplementatie die de kwetsbaarheid moet verhelpen.

4 Stappenplan voor patchmanagement

Het doel van dit document is om kleine tot middelgrote organisaties te begeleiden bij het effectief opzetten van hun patchmanagementproces, waarbij snelle resultaten in de bescherming van de assets het uitgangspunt is.

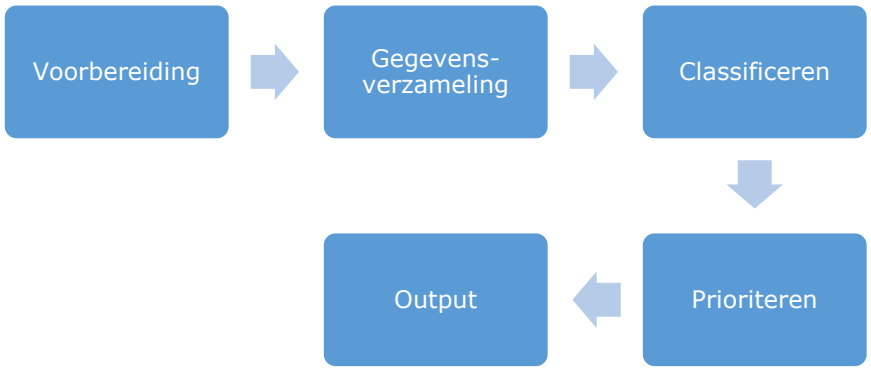
Het stappenplan:

1. Inventarisatie en prioritering van assets
   - Het inventariseren, classificeren en prioriteren van de assets op basis van hun risico voor gefaseerde implementatie.
2. Identificatie van patches
   - Het actief uit meerdere bronnen identificeren van patches die gebruikt kunnen worden om kwetsbaarheden te verwijderen.
3. Evaluatie en goedkeuring van patches
   - Het beoordelen van de belangrijkheid van een patch en het verkrijgen van goedkeuring van de asset-eigenaar om het te mogen implementeren.
4. Plannen van patchimplementatie
   - Het effectief en efficiënt plannen van de patchimplementatie in een vast stramien.
5. Uitvoering van noodprocedure voor spoedpatches
   - Het mogelijk maken om patches met onmiddellijke ingang te kunnen implementeren.
6. Patch implementatie
   - Het risico gebaseerd implementeren van patches.
7. Patch verificatie
   - Het vaststellen van de succesvolle implementatie van de patches.
8. Documentatie en rapportage
   - Het vastleggen en rapporteren van de beschikbare en wel en niet geïmplementeerde patches.
9. Evaluatie en doorlopende verbetering
   - Het evalueren van de patchimplementatie en het periodiek verbeteren ervan.

4.1 Inventarisatie en prioritering van assets

Doel: Het doel van deze stap is inzichtelijk te krijgen welke assets software bevatten die kwetsbaarheden kunnen hebben die gepatcht moeten worden. Het overzicht moet daarom goed doorzoekbaar zijn om snel te kunnen zien of je door een gepubliceerde kwetsbaarheid geraakt kunt worden. De prioritering van de assets geeft de mogelijkheid om gefaseerd het proces te implementeren waarbij het risico van de asset de bepalende factor is. Het is van belang om de gehele keten van software tot en met de software in de fysieke systemen (firmware) in kaart te brengen omdat kwetsbaarheden in alle schakels van deze keten in de code kunnen voorkomen.

Implementatiestappen



Figuur 1 - 1 Inventarisatie en prioritering van assets

Voorbereiding

- Maak waar mogelijk gebruik van bestaande gegevensverzamelingen uit het assetmanagementproces.
- Gebruik software zoals CMDB-oplossingen (Configuration Management Database) om het ontdekken en volgen van assets te automatiseren.

Gegevensverzameling

Maak een goed doorzoekbaar overzicht van de assets:

- Hardware-assets: Documenteer alle servers, werkstations, laptops, mobiele apparaten, netwerkapparaten (routers, switches, firewalls) en IoT-apparaten.
- Software-assets: Documenteer alle besturingssystemen, applicaties (zowel kant-en-klaar als op maat ontwikkeld) en middleware.
- Firmware: Documenteer ook de ingesloten systemen zoals databasemanagementsystemen en firmwareversies voor hardware-assets.
- Virtuele assets: Documenteer ook alle relevante virtuele machines, containers en cloudgebaseerde bronnen mee.

Classificeren

Classificeer de assets:

- Per type: Scheid assets in categorieën zoals infrastructuur, applicaties, databases, enz.
- Per bedrijfsfunctie: Groepeer assets op basis van de bedrijfsprocessen die ze ondersteunen.
- Op nalevingsvereisten: Identificeer assets die onderworpen zijn aan regelgevende normen zoals AVG en BIO.

- Beoordeel het risico van de assets voor de bedrijfsprocessen op basis van beschikbaarheid, integriteit en vertrouwelijkheid (BIV).
- Zorg ervoor dat alle assets worden verantwoord, waardoor het risico op niet-gepatchte kwetsbaarheden wordt verkleind.

Prioriteren

Prioriteer de assets:

- Kritieke systemen: Markeer systemen die essentieel zijn voor de bedrijfscontinuïteit, zoals financiële systemen, klantendatabases en productieservers.
- Houders van gevoelige gegevens: Geef prioriteit aan assets die vertrouwelijke of bedrijfseigen informatie opslaan of verwerken.
- Internetgerichte systemen: Identificeer systemen die zijn blootgesteld aan externe netwerken, waardoor hun kwetsbaarheid voor aanvallen toeneemt.
- Resource-optimalisatie: Richt patchinspanningen op assets die het grootste risico vormen als ze worden gecompromitteerd. Dit zijn doorgaans assets die een generieke functie hebben zoals domain controllers, firewalls, load balancers, gateways of stepping stones, communicatiesoftware en software voor het delen van informatie (b.v. SharePoint) waardoor bij compromittering meteen een groot risico voor de organisatie kan vormen.

Output

- Een bijgewerkte assetinventaris met risico, classificatie, prioritering en categorieën die een basis biedt voor gefaseerde patch management implementatie.

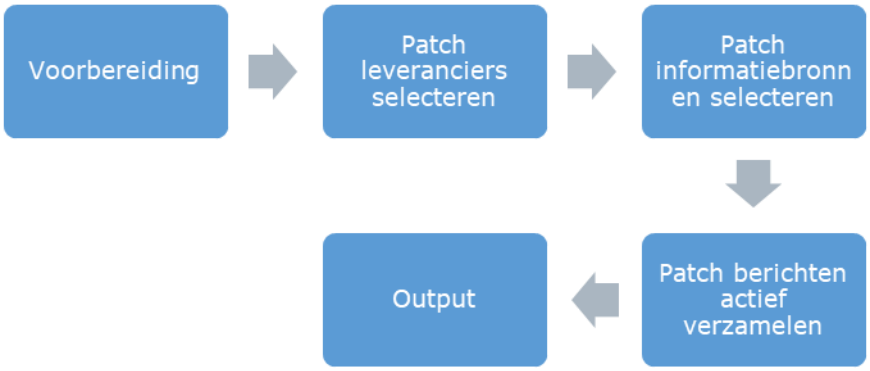
Aanwijzingen

- Regelmatige audits: Plan periodieke beoordelingen om de inventaris nauwkeurig en up-to-date te houden.
- Betrokkenheid van belanghebbenden: Betrek systeemeigenaren en afdelingshoofden bij het verifiëren van assetdetails en classificaties.

4.2 Identificatie van patches

Doel: Het doel van de identificatie van patches is het zo snel mogelijk beschikbaar krijgen van de middelen om kwetsbaarheden te verhelpen voordat die door kwaadwillende uitgebuit wordt.

Implementatiestappen



Figuur 2 - Identificatie van patches

Voorbereiding

- Specifieke rollen: Wijs specifieke medewerkers aan om patchinformatie te controleren en te verspreiden.
- Gebruik de classificering en risico-prioritering uit stap 1 om de snelheid en volledigheid van de patches te kunnen sturen.

Patch leveranciers selecteren

Leveranciers patchberichten monitoren:

- Abonnementsservices: Meld u aan voor e-mailwaarschuwingen of nieuwsbrieven van leveranciers zoals Microsoft, Adobe, Oracle en hardwarefabrikanten.
- Leverancierssportalen: Controleer regelmatig de websites en portals van leveranciers op updates.

Patch informatiebronnen selecteren

Op de hoogte blijven van beschikbare patches en kwetsbaarheidsinformatie:

- Beveiligingsbulletins: Volg bulletins van gerenommeerde beveiligingsorganisaties (bijv. US-CERT, ENISA, NCSC, SANS Institute) en van de leveranciers en/of fabrikanten van de assets (bijv. Microsoft, Linux, en Oracle patchberichten).
- Community fora: Neem deel aan brancheforums en discussiegroepen om op de hoogte te blijven van opkomende bedreigingen.

Patch berichten actief verzamelen

- Tijdige updates: Het snel identificeren van nieuwe patches vermindert de kans op blootstelling aan kwetsbaarheden.
- Door op de hoogte blijven van informatie over beschikbare patches en kwetsbaarheidsinformatie kunnen beveiligingsincidenten voorkomen worden.

Output

- Verzamelde informatie over beschikbare patches voor de relevante assets en informatie over kwetsbaarheden die (nog) niet gepatcht kunnen worden.

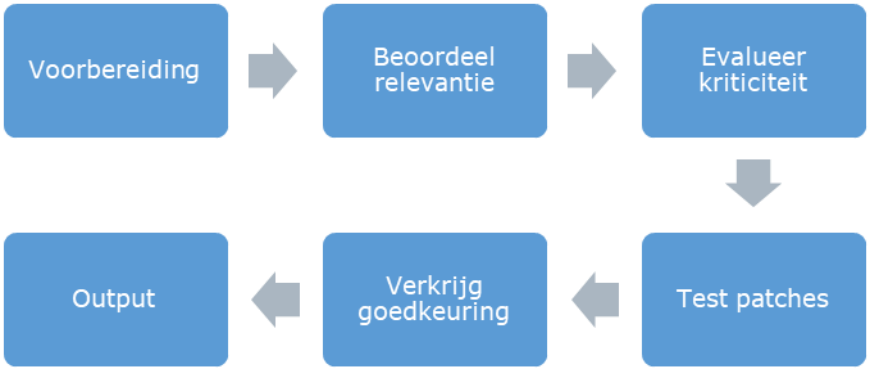
Aanwijzingen

- Geaggregeerde feeds: gebruik RSS-feeds of geautomatiseerde tools om patchmeldingen te consolideren in één dashboard.

4.3 Evaluatie en goedkeuring van patches

Doel:Het doel van de evaluatie en goedkeuring is dat niet iedere patch even relevant is waardoor er een prioriteit aangegeven kan worden en patches kunnen ook onwenselijk zijn vanuit beschikbaarheid van systemen gedurende een periode.

Implementatiestappen



Figuur 3 - Evaluatie en goedkeuring van patches

Voorbereiding

- Voor deze stap zijn de assetinventaris en de verzamelde patches nodig. De patches hebben een relatie naar de assets nodig.

Beoordeel de relevantie

- Toepasbaarheidscontrole: Bepaal of de patch van invloed is op software- of hardwareversies die binnen uw omgeving worden gebruikt.
- Afhankelijkheidsanalyse: Identificeer eventuele afhankelijkheden tussen patches binnen de lijst met componenten van een systeem of gelijktijdige vereiste updates.

Evalueer bedrijfsrisico

- Classificaties: Gebruik door de leverancier verstrekte classificatieniveaus ten aanzien van de ernst van de te patches kwetsbaarheid en vergelijk ze met industriestandaards zoals CVSS-scores.

- Risicobeoordeling: Overweeg de mogelijke impact van het niet toepassen van de patch op de bedrijfsvoering en beveiliging. Let hierbij op dat een CVSS-score uitgaat van een systeem wat verder niet beschermd is.

Test patches

- Testen van de patch: Implementeer patches in een testomgeving die productie-instellingen waar mogelijk repliceert.
- Compatibiliteitstests: Zorg ervoor dat patches niet in strijd zijn met bestaande applicaties of configuraties door de applicatiebeheerders te laten testen.
- Prestatietests: Controleer op eventuele verslechtering van de systeemprestaties na de patch implementatie.

Verkrijg goedkeuring

- Wijzigingsbeheerproces: Volg de interne procedures om formele goedkeuring te krijgen van de systeemeigenaar.
- Gedocumenteerde goedkeuringen: Houd een register bij van goedkeuringen en van afkeuringen voor compliance- en auditdoeleinden.
- Zorg ervoor dat bij afkeuring het risico door de systeemeigenaar gedragen wordt.

Output

- Geteste en goedgekeurde patches die geïmplementeerd kunnen worden.

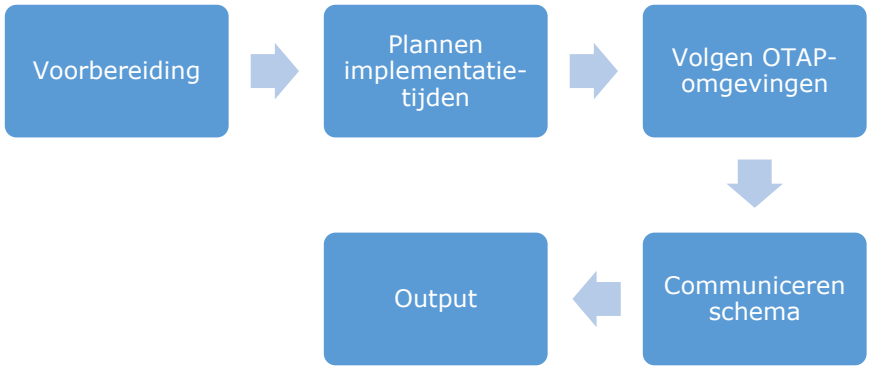
Aanwijzingen

- Voorkom onderbrekingen: Testen helpt systeemuitval of applicatiestoringen als gevolg van incompatibele patches te voorkomen.
- Compliance: Zorgt voor naleving van intern beleid en externe regelgevende instanties.
- Beleid voor patchmanagement: Ontwikkel duidelijke criteria voor workflows voor patchevaluatie en goedkeuring.
- Noodprotocollen: Stel versnelde processen in voor kritieke patches die niet kunnen wachten op standaard goedkeuringscycli.

4.4 Plannen van patch implementatie

Doel:Het plannen heeft als doel een gecontroleerde gang naar productie van de patches te realiseren die zowel zo snel als mogelijk is en verstoringen minimaliseert.

Implementatiestappen



Figuur 4 - Plannen van patch implementatie

Voorbereiding

- Gebruik de lijst met geteste goedgekeurde patches.
- Ga voor de snelheid uit van de classificatie van de patches voor de bedrijfsprocessen en de risico score (CVSS) die deze hebben meegekregen.
- De gebruikers kunnen werk bespaard worden door het plannen van implementatie rond het niet beschikbaar zijn van het systeem (regulier onderhoud tijdsbestek).

Plannen implementatietijden

- Onderhoudsvensters: Plan patches tijdens perioden met weinig gebruik om de impact op de gebruiker te minimaliseren en zo kort mogelijk na uitbrengen van standaard patch-releases (b.v. Microsoft patch Tuesday).
- Coördinatie van de zakelijke agenda: Vermijd piekperiodes, het einde van het kalenderjaar of grote bedrijfsevenementen.

Volgen OTAP-omgevingen

- Ontwikkeling (O): Eerste tests door ontwikkelaars.
- Testen (T): Unit-, integratie- en performancetesten.
- Acceptatie (A): Gebruikersacceptatietesten om functionaliteit te valideren.
- Productie (P): Definitieve implementatie naar live systemen.

Communiceren schema

- Voorafgaande kennisgeving: Geef belanghebbenden voldoende tijd voordat ze worden geïmplementeerd.
- Gedetailleerde plannen: Deel de omvang van updates, getroffen systemen en verwachte vermindering van de beschikbaarheid.

Output

- Een gecommuniceerde en onderbouwde planning van de implementatie van de patches die door de volgorde nog een extra test in zicht heeft voordat deze in productie komt.

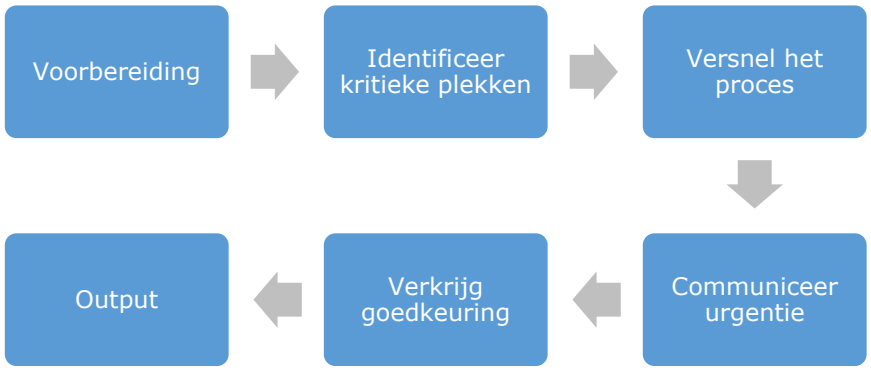
Aanwijzingen

- Operationele continuïteit: Vermindert het risico op onverwachte verstoringen van bedrijfsprocessen.
- Geautomatiseerde planningstools: Gebruik software die implementaties kan automatiseren volgens vooraf gedefinieerde schema's.
- Noodplannen: Bereid terugdraaiprocedures (fall-back) voor in geval van mislukte implementaties.

4.5 Uitvoering van noodprocedure voor spoedpatches

Doel: Noodprocedure is om bij geval van zeer ernstige kwetsbaarheden de beschikbare patch direct te kunnen implementeren zonder te hoeven wachten op testresultaten en op goedkeuringen die normaal tijdens geplande overleggen worden afgegeven.

Implementatiestappen



Figuur 5 - Uitvoering van noodprocedure voor spoedpatches

Voorbereiding

- Vanuit een patchbeleid van de organisatie moet het duidelijk zijn wat onder een patch verstaan wordt die middels de noodprocedure geïmplementeerd moet worden.
- Vooraf gedefinieerde noodprotocollen: Zorg voor duidelijke richtlijnen voor het omgaan met dringende patches, inclusief rollen en verantwoordelijkheden.
- Integratie van incidentrespons: Coördineer met incidentresponsteams voor een uniforme aanpak wanneer ontdekt is dat een kwetsbaarheid al geëxploiteerd is in de organisatie.

Identificeer kritieke plekken

- Geëxploiteerde kwetsbaarheden: Besteed speciale aandacht aan patches die actief geëxploiteerde kwetsbaarheden verhelpen.
- Naleving van regelgeving: Geef prioriteit aan patches die compliance-gerelateerde beveiligingslacunes aanpakken.

Versnel het proces

- Gestroomlijnde goedkeuring: Gebruik procedures voor het beheer van noodwijzigingen om standaardvertragingen te omzeilen. Dus wel het wijzigingenbeheer proces volgen maar niet wachten tot reguleer overleg door direct contact op te nemen met de belanghebbenden.
- Onmiddellijk testen: Voer snelle maar grondige tests uit die gericht zijn op kritieke functionaliteit.

Communiceer urgentie

- Executive Briefings: Informeer het senior management over de risico's en vereiste acties.
- Gebruikerswaarschuwingen: Informeer eindgebruikers over mogelijke gevolgen of vereiste acties van hun kant.

Verkrijg goedkeuring

- Verkrijg een mondelinge en een e-mail goedkeuring voor de versnelde implementatie van de patch en de hiervoor noodzakelijke systeemtijd.

Output

- Goedgekeurde versnelde of directe implementaties van patches.

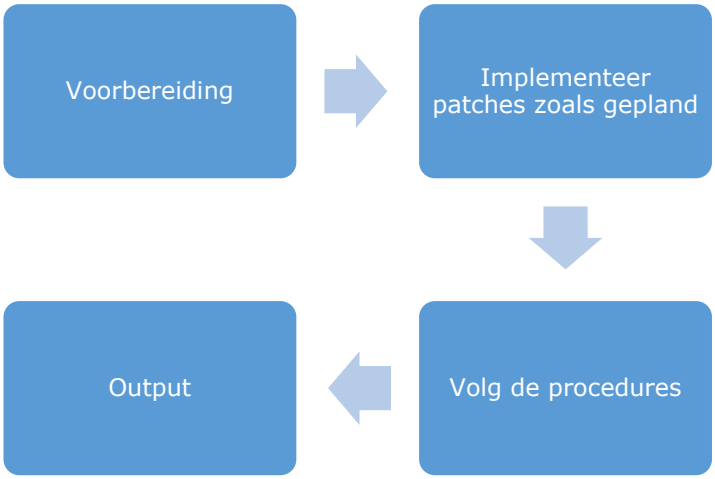
Aanwijzingen

- Risicovermindering: Snelle actie beperkt de mogelijkheid voor aanvallers om kwetsbaarheden uit te buiten.
- Naleving van de regelgeving: Zorgt voor naleving van wetten en normen die tijdige oplossing van kwetsbaarheden vereisen.

4.6 Uitvoeren van patchimplementatie

Doel: Snel en efficiënt patches implementeren volgens een gecontroleerde standaard werkwijze om fouten te minimaliseren.

Implementatiestappen



Figuur 6 - Uitvoeren van patchimplementatie

Voorbereiding

- De goedgekeurde patches kunnen gedistribueerd worden naar de systemen voorafgaand aan de implementatie.

Implementeer patches zoals gepland

- Uitvoering: Implementeer de patches volgens het implementatieplan.
- Monitoring: Houd het implementatieproces in de gaten voor eventuele onmiddellijke problemen.

Volg de procedures

- Standard Operating Procedures (SOP's): Houd u aan gedocumenteerde methoden voor consistentie en het verminderen van het risico op fouten.
- Beveiligingscontroles: Zorg ervoor dat beveiligingsmaatregelen (zoals antivirus of firewalls) niet per ongeluk worden uitgeschakeld.

Output

- Aantoonbaar geïmplementeerde patches op de relevante systemen.

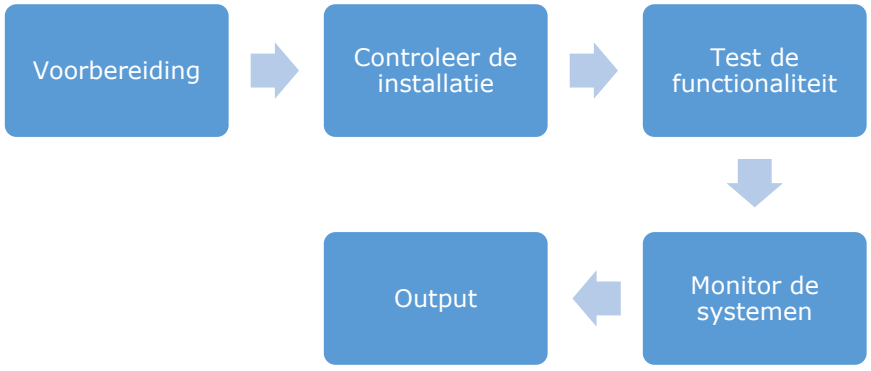
Aanwijzingen

- Gebruik implementatietools: Gebruik gecentraliseerde patchmanagementsystemen voor efficiëntie.
- Back-upsystemen: Zorg altijd voor recente back-ups voordat u wijzigingen aanbrengt in kritieke systemen.
- Naleving: Patch implementatie logging toont naleving van interne controles en externe regelgeving aan.

4.7 Verificatie van patches

Doel: Procesmatige, tijdige en geverifieerde patch-implementatie of volgens proces geïnitieerde terugdraai van patches bij verstoringen.

Implementatiestappen



Figuur 7 - Verificatie van patches

Voorbereiding

- Verkrijg de logging en feedback van de systeembeheerders en of applicatiebeheerders over de implementatie van de patches.
- Zorg dat duidelijk is welke medewerkers de functionaliteit zullen testen en hoe ze dit doen.
- Moedig gebruikers aan om eventuele problemen onmiddellijk te melden.

Controleer de installatie

- Geautomatiseerde verificatie: gebruik scripts of hulpprogramma's om de succesvolle implementatie van patches te bevestigen.
- Fysieke controles: Controleer kritieke systemen handmatig op bevestiging van patches.

Test de functionaliteit

- Testen van gebruikersacceptatie: Laat eindgebruikers valideren dat hun applicaties correct functioneren.
- Systeemprestatiecontroles: Bewaak belangrijke prestatie-indicatoren om afwijkingen te detecteren.

Monitor de systemen

- Real-time monitoring: Gebruik monitoringtools om de systeemstatus te observeren.
- Logboekanalyse: controleer systeem- en toepassingslogboeken op fouten of waarschuwingen.

Output

- Succesvol gepatchte functionele systemen en systemen die niet konden patchen of niet meer volledig functioneren.

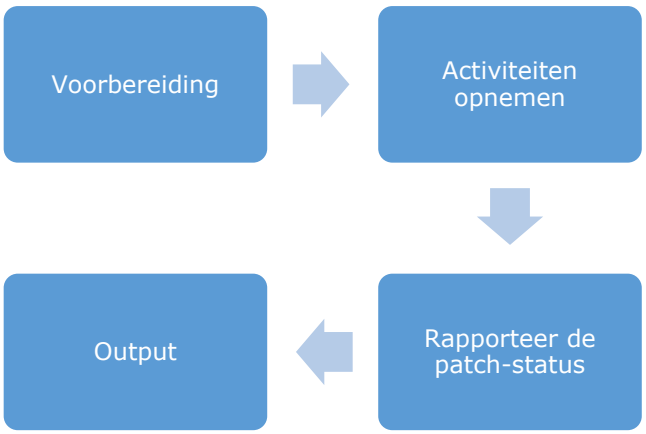
Aanwijzingen

- Zekerheid: Bevestigt dat de patches correct zijn aangebracht en effectief zijn.
- Vroegtijdige opsporing van problemen: Identificeert en pak problemen aan voordat ze van invloed zijn op de bedrijfsvoering.
- Verificatierapporten: Documenteer verificatieresultaten voor verantwoording.

4.8 Documentatie en rapportage

Doel: Doel is inzichtelijk te houden welke kwetsbaarheden wel of niet zijn verholpen door de implementatie van patches en vastlegging van de reden van het niet geven van goedkeuring voor de implementatie.

Implementatiestappen



Figuur 8 - Documentatie en rapportage

Voorbereiding

Verzamel alle informatie die inzicht geeft in het risico wat de organisatie loopt ten aanzien van kwetsbaarheden. Dit zijn:

- Bekende kwetsbaarheden;
- Kwetsbaarheden die actief geëxploiteerd worden;
- Beschikbare patches;
- Patches waarvoor geen goedkeuring verkregen is;
- Patches die met een noodprocedure geïmplementeerd zijn;
- Patches die succesvol geïmplementeerd zijn;
- Patches die teruggedraaid zijn; en,
- Risico acceptaties van de systeemeigenaren.

Activiteiten opnemen

- Gedetailleerde logboeken: Houd bij wie de patching heeft uitgevoerd, wanneer en op welke systemen. Houd ook bij welke goedkeuringen niet zijn gegeven inclusief de reden en de acceptatie van het risico door de asset-eigenaar.
- Problemen en oplossingen: Documenteer eventuele problemen die zich hebben voorgedaan en de stappen die zijn ondernomen om ze op te lossen.

Rapporteer de patch-status

- Managementrapporten: Geef samenvattingen aan het IT-management en de systeemeigenaren over patch-compliance en eventuele openstaande kwetsbaarheden.
- Nalevingsrapporten: Bereid de documentatie voor die nodig is voor audits en regelgevende instanties.

Output

- Transparantie: Houdt alle belanghebbenden op de hoogte van de beveiligingsstatus en de nalevingsstatus.
- Verantwoording: Biedt een audittrail voor alle patchmanagementactiviteiten.

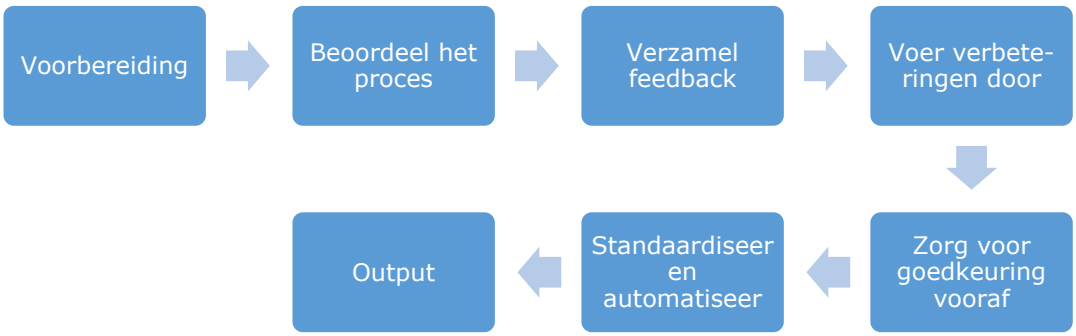
Aanwijzingen

- Gebruik gecentraliseerde systemen: Implementeer een ticketing- of wijzigingsbeheersysteem om activiteiten bij te houden.
- Regelmatige updates: Plan periodieke rapportage om voortdurend op de hoogte te blijven.

4.9 Evaluatie en doorlopende verbetering

Doel: Doel is voortdurende aanscherping en automatisering van de patch-processen teneinde steeds kortere periodes te realiseren waarin systemen kwetsbaar zijn.

Implementatiestappen



Figuur 9 - Evaluatie en doorlopende verbetering

Voorbereiding

- Zorg dat u een actuele beschrijving hebt van het patchmanagement proces als uitgangspunt voor de verbetering.
- Zorg dat u een patch managementbeleid hebt als norm waartegen u de procesvoering beoordeeld of evalueert.

Beoordeel het proces

- Evaluaties na de implementatie: Analyseer de effectiviteit van het patchmanagementproces na elke cyclus.
- Key Performance Indicators (KPI's): Evalueer statistieken zoals de implementatietijd van patches, slagingspercentages en nalevingsniveaus.

Verzamel feedback

- Input van het personeel: Vraag om suggesties van IT-personeel over procesverbeteringen.
- Gebruikersenquêtes: Verzamel feedback van eindgebruikers over eventuele problemen die ze ondervinden.

Verbeteringen doorvoeren

- Beleidsupdates: Herzie het beleid voor patchmanagement om de geleerde lessen weer te geven.
- Trainingsprogramma's: Zorg voor aanvullende training op basis van geïdentificeerde kennislacunes.

Zorg voor goedkeuring vooraf

- Verkrijg goedkeuring van de beheersorganisatie en asset-eigenaren om standaard patches door te voeren op vaste momenten waarbij i.p.v. een goedkeuring alleen gedurende een korte periode het patchproces gestopt kan worden wanneer testen van de patch problemen geeft.

Standaardiseer en automatiseer

- Verminder de afhankelijkheid van menselijke interactie door zoveel mogelijk delen va het proces (evaluatie, testen, implementeren, monitoren en rapporteren) te standaardiseren en te automatiseren.

Output

- Een effectiever patchmanagement en daarmee een robuustere verdediging tegen kwetsbaarheden.
- Een efficiënter patchmanagement door beter gestroomlijnde processen met besparing in tijd en middelen.

Aanwijzingen

- Stel regelmatige beoordelingsintervallen in: Voer elk kwartaal of na grote patchcycli beoordelingen uit.
- Benchmarking: Vergelijk de prestaties met industriestandaards of eerdere perioden.
- Cloud: In de cloud zal de cloud provider in een PAAS- en een SAAS- [1] omgeving de patching al van uw organisatie overnemen. Beheersorganisaties moeten zich hier al op voorbereiden door minder afhankelijk te worden van testen van patches.

[1] Platform As A Service (PAAS) en Software As A Service (SAAS)

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)

Februari 2025