TLP:GREEN

PROCESMODEL

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

1.3 Definities

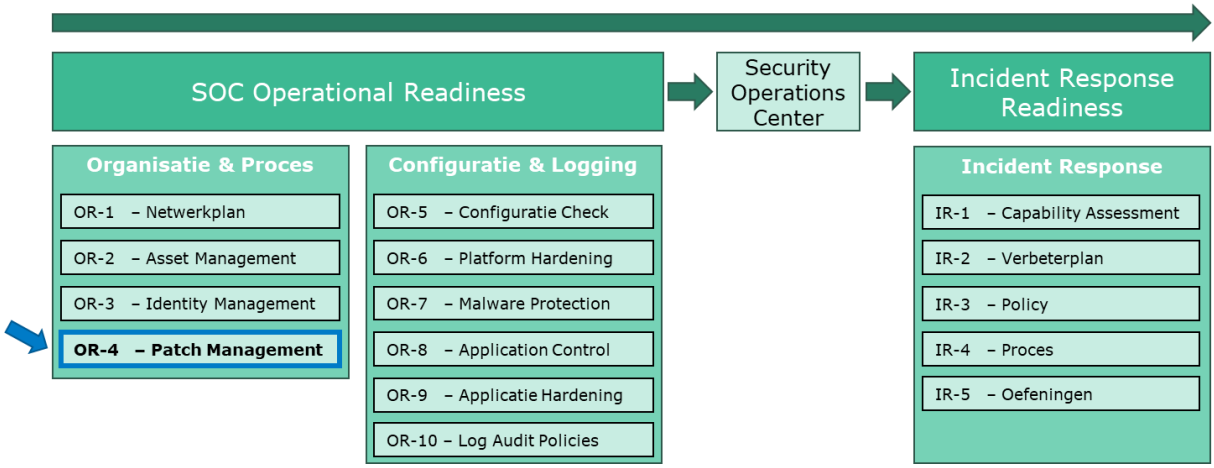
Ter verduidelijking van de terminologie en begrippen die in dit document worden gebruikt is er een verzameling van definities te vinden op Woordenboek - Cyberveilig Nederland.

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 **procesmodel** 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 Patchmanagement

Dit hoofdstuk beschrijft een generiek procesmodel voor het patchmanagementproces, met als doel een werkend proces binnen de organisatie te creëren. Dit proces dient als basis om de meeste kwetsbaarheden van een organisatie te verhelpen, waarna het SOC effectieve detectiesystemen kan inrichten.

3.1 Inleiding

Patchmanagement is een gestructureerde aanpak voor het updaten van software op computers, servers en andere apparaten om kwetsbaarheden te verhelpen, fouten te corrigeren en de prestaties te verbeteren. Zie het als het bijwerken van apps op je smartphone of computerprogramma's om ze soepel en veilig te laten werken.

Effectief patchmanagement is essentieel om de IT-infrastructuur van een organisatie te beschermen tegen cyberdreigingen en softwarefouten. Deze inleiding schetst een patchmanagementproces dat is afgestemd op kleine tot middelgrote organisaties. Dit patchmanagementproces heeft als doel kwetsbaarheden tijdig op te lossen zodat een Security Operations Center (SOC) geen (onnodige) tijd kwijt is met het aandacht geven aan bekende kwetsbaarheden.

Deze handleiding schetst een eenvoudig patchmanagementproces met acht belangrijke stappen. Door met deze essentiële stappen te beginnen, kunt u uw beveiliging snel verbeteren en vervolgens in de loop van de tijd op deze basis voortbouwen.

De handleiding verdeelt het patchmanagementproces in een achttal activiteiten die in detail worden toegelicht. Tevens worden de verantwoordelijkheden van de stappen in een RACI-model in hoofdstuk 4.5 beschreven en worden verdere nuttige aanwijzingen gegeven die helpen in de implementatie.

Verwacht wordt dat de organisatie een gecontroleerd proces voor changemanagement heeft die gebruikt wordt bij het implementeren van patches in de omgevingen. Het is aan te bevelen patchimplementaties als een standaard wijzigingsverzoek in het changemanagementproces op te nemen. Hiermee worden beide processen op elkaar afgestemd.

3.2 Beschrijving en uitleg van het proces

Om een compleet beeld te geven, wordt eerst het algemene patchmanagementproces uitgelegd. Hiermee wordt een solide fundament gelegd voor het optimaal ondersteunen van de SOC-activiteiten.

Het patchmanagementprocesmodel is afgestemd op kleine tot middelgrote organisaties. Het richt zich op het opzetten van een effectief patchmanagementproces zonder in te gaan op technische implementatiedetails. Het model helpt organisaties snel resultaten te behalen door te concentreren op de meest relevante onderdelen van patchmanagement.

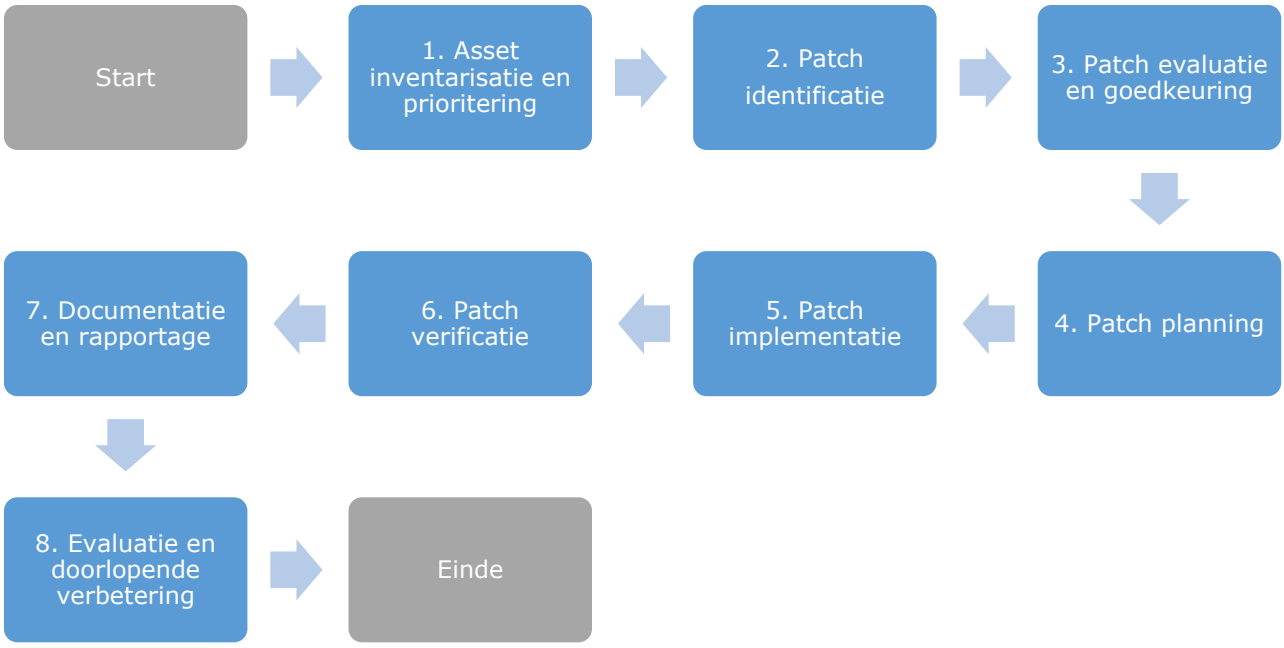
Om het patchmanagementproces effectief en efficiënt te kunnen implementeren zijn er randvoorwaarden die ingevuld moeten worden:

- **Formuleer beleid voor patchmanagement.**
  Dit is een randvoorwaarde voor het selecteren en prioriteren van patches en het aansluiten op berichtgeving van kwetsbaarheden en beschikbare patches, die in dit proces moeten worden meegenomen. Aanwijzingen hiervoor komen vanuit organisaties zoals het NCSC ten aanzien van berichten over kwetsbaarheden en vanuit de BIO overheid toelichtingen.
- **Zorg dat asset management is ingericht.**
  Dit is een randvoorwaarde om een classificatie te kunnen geven aan de kwetsbaarheden en de patches op basis van de impact die deze hebben op de beveiliging.

3.3 Patchmanagementproces flowchart

Hierna wordt een illustratie gegeven van de procesflow van patchmanagement. Het geeft de volgorde aan van de processtappen die moeten worden doorlopen bij een eerste implementatie van het proces.

De processtap 1 is randvoorwaardelijk om patchmanagement te kunnen implementeren. Processtappen 2 t/m 7 zullen bij iedere patch-cyclus worden herhaald en processtap 8 zal periodiek plaatsvinden om het proces als geheel te beoordelen en te verbeteren.



Figuur 1 - Procesflow patchmanagement

3.4 Beschrijving van de processtappen

Het patchmanagementproces bestaat uit de volgende stappen:

1. Inventarisatie en prioritering van assets
2. Identificatie van patches
3. Evaluatie en goedkeuring van patches
4. Plannen van patchimplementatie
5. Uitvoering van patchimplementatie
6. Verificatie van patches
7. Documentatie en rapportage
8. Evaluatie en doorlopende verbetering

Elke stap is ontworpen om patches efficiënt en effectief toe te passen, met een focus op het minimaliseren van risico's en het ondersteunen van SOC-activiteiten.

Als er voor een eerste minimale implementatie van het proces wordt gekozen zullen in ieder geval de processtappen 2, 4 en 5 moeten worden uitgevoerd.

De evaluatie en goedkeuring (stap 3) helpen bij het voorkomen van onnodige fouten doordat eigenaren van assets nog niet hebben kunnen testen. De verificatie en documentatie (stappen 6 en 7) zijn een extra zekerheid tegen problemen die patches kunnen geven en de zekerheid dat ze daadwerkelijk geïmplementeerd zijn.

3.5 Gedetailleerde beschrijving processtappen

Hierna worden per processtap aangegeven wat de benodigde informatie is om de stap uit te voeren (input), welke activiteiten of transformaties er plaatsvinden en vervolgens welke resultaten (output) de activiteit heeft.

3.5.1 Inventarisatie en prioritering van assets

Doel: Identificeren van alle assets die gepatcht moeten worden en het bepalen van de volgorde van patchimplementatie op basis van een risicobeoordeling.

Beschrijving: Stel een uitgebreide inventaris op van alle IT-assets, inclusief infrastructuur, middleware, applicaties en firmware. Prioriteer assets op basis van hun kritieke aard en blootstelling aan risico's.

Input:

- Bestaande asset-inventaris.
- Netwerkdiagrammen.
- Risicobeoordelingen.
- Business impact analysis beoordelingen.

Activiteiten:

- Werk de asset-inventaris bij en valideer deze.
- Classificeer assets op type en belangrijkheid (bijvoorbeeld systemen die direct aan het internet gekoppeld zijn).
- Beoordeel het risiconiveau van elk asset.
- Prioriteer assets voor patchmanagement op basis van risico en bedrijfsimpact.

Output:

- Bijgewerkte en geprioriteerde actielijst.
- Assets met een risicoclassificatie.

3.5.2 Patch identificatie

Doel: Zorgen dat de organisatie op de hoogte blijft van nieuwe patches die kwetsbaarheden in activa aanpakken.

Beschrijving: Monitor en identificeer beschikbare patches van leveranciers op basis van hun periodieke releaseschema's.

Input:

- Asset database met risico geclassificeerde assets.
- Notificaties van leveranciers.
- Beveiligingsbulletins.
- Publiek beschikbare kwetsbaarheidsdatabases.

Activiteiten:

- Monitor regelmatig nieuwe kwetsbaarhedenberichten en patchreleases.
- Stel een lijst op van relevante patches voor de assets van de organisatie.

Output:

- Lijst met geïdentificeerde patches die van toepassing zijn op de assets van de organisatie.

3.5.3 Patch evaluatie en goedkeuring

Doel: Zorgen dat patches relevant zijn en geen nadelige effecten hebben op systeemfunctionaliteit.

Beschrijving: Beoordeel patches op toepasbaarheid, belangrijkheid en mogelijke impact op systemen. Verkrijg goedkeuringen voor implementatie.

Input:

- Lijst met geïdentificeerde patches en hun beschrijvingen.
- Asset configuraties.

Activiteiten:

- Evalueer de relevantie tot de assets van iedere patch.
- Beoordeel het risico van de patch en het risico van de kwetsbaarheid.
- Test de patches in een gecontroleerde omgeving (b.v. een testomgeving).
- Beoordeel de potentiële impact op de IT-operations.
- Verkrijg goedkeuring van de asset eigenaren en eventueel andere belanghebbenden.

Output:

- Lijst met goedgekeurde en geteste patches.
- Risico assessment rapporten.

3.5.4 Patch planning

Doel: Het organiseren van de patchimplementatie op een gecontroleerde manier om verstoringen in de bedrijfsvoering te minimaliseren. Hierbij is het gewenst om de patches zo kort mogelijk na publicatie te implementeren. (Denk aan Microsoft Patch Tuesday!) Omdat van tevoren bekend is wanneer de patches gepubliceerd worden kunnen er al afspraken gemaakt worden met de asset eigenaren over een standaard patch-tijdslot welke in een patch-policy vastgelegd worden.

Beschrijving: Plan de implementatie van goedgekeurde patches in verschillende omgevingen volgens het OTAP-model (Ontwikkel, Test, Acceptatie, Productie).

Maak ook afspraken om buiten de normale planning een emergency-patch te kunnen implementeren. (Zie additionele aanwijzingen)

Input:

- Lijst van goedgekeurde patches.
- Geprioriteerde assets.
- Planning van bedrijfsactiviteiten.

Activiteiten:

- Bepaal het optimale tijdstip voor de patchimplementatie a.d.h.v. het risico van de kwetsbaarheid en de impact op de te patchen asset.
- Plan patches eerst in niet-productie-omgevingen (ontwikkel, test- en acceptatieomgevingen) en daarna in productie.
- Coördineer met belanghebbenden om de impact op bedrijfsactiviteiten te minimaliseren.
- Communiceer het patchschema naar alle betrokken partijen.

Output:

- Patch implementatieplan.
- Communicatieplan.

3.5.5 Patch implementatie

Doel: Toepassen van patches op systemen om geïdentificeerde kwetsbaarheden te mitigeren.

Beschrijving: Voer de implementatie van goedgekeurde patches uit volgens het geplande schema.

Input:
- Patchimplementatieplan.
- Goedgekeurde patches.
- Implementatietools en scripts.

Activiteiten:
- Implementeer patches eerst in een niet-productie-omgeving.
- Controleer op problemen en los deze op voordat u doorgaat.
- Voer patches stapsgewijs uit in Ontwikkel-, Test-, Acceptatie- en Productieomgevingen.
- Monitor het implementatieproces op fouten of problemen.

Output:
- Gepatchte systemen.
- Implementatie logs

3.5.6 Patch verificatie

Doel: Waarborgen van de integriteit en operationele stabiliteit van gepatchte systemen.

Beschrijving: Controleer of patches succesvol zijn toegepast en of systemen correct functioneren.

Input:

- Implementatie logs.
- Systeemprestatiegegevens.
- Terugkoppeling van gebruikers.

Activiteiten:

- Controleer systeem-statussen en logs op fouten.
- Voer functionaliteitstests uit om ervoor te zorgen dat systemen naar verwachting werken.
- Verzamel terugkoppeling van eindgebruikers en monitoringtools.
- Documenteer eventuele problemen en start een herstelproces indien nodig.

Output:

- Verificatierapporten.
- Probleem logs (indien aanwezig).

3.5.7 Documentatie en rapportage

Doel: Bijhouden van gegevens voor naleving en het vergemakkelijken van audits.

Beschrijving: Documenteer alle activiteiten met betrekking tot patchmanagement en rapporteer de status aan relevante belanghebbenden.

Input:

- Implementatielogs.
- Verificatierapporten.
- Patchschema's.

Activiteiten:

- Werk records en databases voor patchmanagement bij.
- Bereid rapporten voor met details over patchimplementatie en verificatieresultaten.
- Archiveer records volgens organisatorisch beleid.

Output:

- Bijgewerkte patchmanagementdocumentatie.
- Rapporten voor belanghebbenden.
- Nalevingsdocumentatie ten aanzien van de patchpolicies.

3.5.8 Evaluatie en continue verbetering

Doel: Het verhogen van de efficiëntie en effectiviteit van het patchmanagementproces over tijd.

Beschrijving: Beoordeel regelmatig het patchmanagementproces en implementeer verbeteringen.

Input:

- Prestatie indicatoren van het proces.
- Feedback van belanghebbenden.
- Auditbevindingen.

Activiteiten:

- Analyseer de prestatie indicatoren met betrekking tot patchmanagement.
- Verzamel feedback van IT-personeel, eindgebruikers en management.
- Identificeer verbeterpunten of optimalisaties.
- Werk beleid, procedures en documentatie bij waar nodig.
- Bied training of middelen aan om verbeteringen te ondersteunen.

Output:

- Verbeterd patchmanagementproces.
- Bijgewerkte documentatie.
- Trainingsmaterialen.

3.6 RACI-Matrix en gebruik

De volgende RACI-matrix definieert de rollen en verantwoordelijkheden voor elke stap van het patchmanagementproces. Het verduidelijkt wie in elke fase verantwoordelijk, aansprakelijk, geraadpleegd en geïnformeerd (RACI) is, zodat alle teamleden hun specifieke taken en samenwerkingspunten begrijpen. Deze matrix dient als leidraad om de communicatie te stroomlijnen en de efficiëntie van de workflow voor patchmanagement te verbeteren.

R (Responsible) : Verantwoordelijk voor de uitvoering van de taak.
A (Accountable) : Eindverantwoordelijk voor de taak en het resultaat.
C (Consulted) : Geeft advies of input voor de taak.
I (Informed) : Wordt op de hoogte gehouden van de voortgang en resultaten.

Proces Stappen	IT Asset Manager	IT Manager	Systeembeheerder	Operations Team	Asset tester	Security Officer	Systeem eigenaar	Leverancier	SOC Team	Compliance Officer	Leidinggevende	Gebruikers
1. Inventarisatie en prioritering van assets	R	A				C	C		I			
2. Patch identificatie		A	R			C		C	I			
3. Patch evaluatie en goedkeuring		A	R		C	C	C					
4. Patch planning		A	R	C			C				I	I
5. Patch implementatie		A	C	R			C					I
6. Patch verificatie		A		C	R	I	C					I
7. Documentatie en rapportage		A	R			C			I	C	I	
8. Evaluatie en continue verbetering		R/A				C				C	I	I

Figuur 2 - RACI Matrix

Hierna geven wij in een viertal stappen aan hoe u de RACI-matrix in uw organisatie kunt opzetten en implementeren.

1. Identificeer de rollen in uw organisatie die onderdeel zijn van het patchproces. In een grote organisatie met complexe IT-systemen zullen de meeste van deze rollen aanwezig zijn. In een kleine organisatie die het meeste heeft uitbesteed zullen er minder rollen zijn en delen hiervan bij de externe dienstverlener aanwezig zijn. Er zijn ook stakeholders in andere processen die hier niet benoemd zijn, zoals de Change Manager en de Change Analist. Hiervoor verwijzen we naar het changemanagementproces.
   - IT Asset manager: De persoon die eigenaar is van de te patchen assets.
   - IT Manager: De person die eindverantwoordelijk is het beheer.
   - Systeembeheerder: De person die de patch implementeert.
   - Security Officer: De person verantwoordelijk voor informatiebeveiliging.
   - Systeem eigenaar: Eigenaar van het informatiesysteem.
   - Compliance Officer: Verantwoordelijk voor het naleven van de BIO.
   - Leidinggevende: Persoon die vanuit het bedrijfsproces belanghebbende is.
   - Gebruiker: De persoon die dit asset gebruikt.
   - Leverancier: De vertegenwoordiging van de leverancier die patches levert.
   - SOC Team: Het Security Operating Center team.

2. Communiceer de RACI-matrix en stem deze af:
   - Deel de matrix met de belanghebbenden en stem dit af.
   - Zorg ervoor dat iedereen zijn rol kent en instaat is deze uit te voeren.

3. Integreer het proces en de processtappen in de IT-beheersing van uw organisatie:
   - Gebruik de matrix als referentie om de taken uit te voeren en te plannen.
   - Integreer de processtappen in de IT-beheerhandleidingen en de bijbehorende tooling.

4. Evalueer en verbeter regelmatig:
   - Pas de matrix aan wanneer er wijzigingen in de rollen of de procesuitvoering zijn.
   - Her-beoordeel de verantwoordelijkheden in de evaluatie.

4 Additionele aanwijzingen

4.1 Uitbestede omgevingen

Contract Management:

- Neem vereisten voor patchmanagement op in contracten met leveranciers.
- Specificeer verwachtingen voor patchfrequentie en rapportage.
- Maak gebruik van de tooling (ICO-Wizard [1]) die de overheid beschikbaar heeft gesteld.

Leverancier Management:

- Toezicht houden op de naleving van de verplichtingen van leveranciers op het gebied van patchmanagement.

4.2 Typen IT-componenten

Infrastructuur:

- Geef prioriteit aan het patchen van servers, netwerkapparaten en andere systemen die ingezet worden voor beveiliging.

Middleware:

- Voeg databases, applicatieservers en andere middleware toe naarmate een hoger volwassenheid in patch management wordt bereikt.

Applicaties:

- Focus op kritieke toepassingen, met name toepassingen die toegankelijk zijn via internet.

Firmware:

- Verwaarloos firmware-updates voor hardware niet, aangezien deze aanzienlijke kwetsbaarheden kunnen verhelpen.

4.3 Prioritering

Risico-gebaseerde aanpak:

- Geef prioriteit aan patchen op basis van het risico en de potentiële impact van kwetsbaarheden.

Internetgerichte systemen:

- Adresseer systemen die aan het internet worden blootgesteld als eerste omdat die onderdeel zijn van het aanvalsoppervlak voor uw organisatie.

4.4 Noodprocedure Securitypatching

Proces standaardisatie:

- Houd uw proces voor het patchen in noodgevallen zo veel mogelijk gelijk aan uw normale proces om verwarring en fouten te voorkomen.
- Dit betekent dat dezelfde stappen gevolgd moeten worden, maar ze sneller moeten worden uitgevoerd. Realiseer je hierbij dat na publicatie van de patches hackers niet meer dan een paar uur nodig hebben om de kwetsbaarheid die je gaat verhelpen, geautomatiseerd te misbruiken.

Reactiesnelheid:

- Definieer duidelijk wat een emergency- of spoed-patch is, die met een noodprocedure moet worden geïmplementeerd, zodat iedereen weet wanneer snel moet worden gehandeld.
- Zorg voor een plan om het proces te versnellen wanneer dat nodig is. Het NCSC en uw leveranciers geven hierbij richtlijnen.

[1] https://www.bio-overheid.nl/ico-wizard

4.5 Communicatie

Betrokkenheid van belanghebbenden:

- Houd alle belanghebbenden op de hoogte tijdens het patchmanagementproces.

Transparantie:

- Geef duidelijke en tijdige informatie over patchschema's en mogelijke gevolgen.

4.6 Automatisering

Automatiseren van het patchen:

- De beheerstooling van endpoints en servers heeft doorgaans mogelijkheden om patches geautomatiseerd te implementeren. Door dit ook zo met de asset-eigenaren af te spreken kan de tijdsduur waarin de organisatie kwetsbaar is aanmerkelijk verkort worden.

Transformatie:

- Wanneer de organisatie naar een Cloud gebaseerde oplossing transformeert zal het patchen op infrastructuur al geautomatiseerd door de cloud provider worden uitgevoerd afhankelijk van de clouddienst (IAAS[2], PAAS of SAAS).

4.7 Zorg voor een vangnet

Periodieke kwetsbaarhedenscan

- Zorg voor een periodieke scan van de assets op kwetsbaarheden zodat zekerheid ontstaat dat patches ook daadwerkelijk geïmplementeerd zijn en er geen assets of patches buiten de procesvoering vallen.

[2] Infrastructure As A Service, Platform As A Service of Software As A Service

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