

Patchmanagementproces

Voorbeelddocument

Versie: Februari 2025



**Let op: verwijder deze pagina voor gebruik**

**Over dit voorbeelddocument**

**Dit voorbeelddocument helpt je met het maken van een patchmanagementproces. Elke school en elk schoolbestuur is anders. Pas het proces daarom aan aan jouw eigen situatie.**

**Aanpassen van dit voorbeelddocument**

Let bij het aanpassen van het document op het volgende:

* Bij hoofdstukken en paragrafen zijn soms toelichtingen geplaatst. Verwijder deze voordat je de procesbeschrijving definitief maakt.
* Deze procesbeschrijving gaat ervan uit dat taken, rollen en functies die nodig zijn om het proces uit te voeren bij de juiste personen belegd zijn. Is dit niet zo? Ga dan eerst naar fase 1 van het Groeipad.
* Geel gearceerde teksten moet je vervangen door eigen tekst.

**Totstandkoming**

Dit voorbeelddocument is samengesteld door Kennisnet. Binnen het programma Digitaal Veilig Onderwijs bundelen het ministerie van OCW, Kennisnet, SIVON, de PO-Raad en de VO-raad hun krachten voor een onderwijssector waarin iedere leerling digitaal veilig kan leren en medewerkers digitaal veilig kunnen werken.

**Sommige rechten voorbehouden**

Hoewel aan dit document de uiterste zorg is besteed, aanvaardt Kennisnet geen aansprakelijkheid voor eventuele fouten of onvolkomenheden. Ook aanvaardt Kennisnet geen enkele aansprakelijkheid voor schade van welke aard dan ook, ontstaan uit het (onjuiste) gebruik van dit document.



Dit template is opgesteld door Kennisnet en verschijnt onder de licentie [*Creative Commons Naamsvermelding 4.0 Nederland*](https://creativecommons.org/licenses/by/4.0/legalcode.nl).

**Vragen?**

Heb je vragen over dit voorbeelddocument? Kijk voor meer informatie op [*normenkaderibp.kennisnet.nl/groeipad*](file:///Users/jhgerrits/Documents/1.%20Kennisnet%20voorbeeldocumenten/normenkaderibp.kennisnet.nl/groeipad)of stuur een mail naar *ibp@kennisnet.nl**.*

**Documentgeschiedenis**

***Toelichting***

* *Geef hier aan wie het document vaststelt. Dat kan bijvoorbeeld de proceseigenaar zijn, maar ook het bestuur.*
* *Geef aan of het document openbaar, vertrouwelijk of geheim is en wie het in die gevallen mogen zien.*

**Revisies**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Auteur** | **Review** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Vaststelling**

|  |  |  |  |
| --- | --- | --- | --- |
| **Naam** | **Functie** | **Versie** | **Datum** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Documentclassificatie**

|  |  |
| --- | --- |
| **Classificatie** | **Beschrijving** |
| Openbaar | Dit document mag zonder beperkingen worden gedeeld |
| Vertrouwelijk | Dit document mag worden gedeeld met medewerkers van <naam schoolbestuur en eventuele andere organisaties> |
| Geheim | Dit document is exclusief bestemd voor de volgende personen: <bijv. leden MT>. |

**Inhoudsopgave**

[1 Inleiding 5](#_Toc191393175)

[2 Doelstelling 5](#_Toc191393176)

[2.1 Reikwijdte 5](#_Toc191393177)

[3 Processtappen 5](#_Toc191393178)

[3.1 Risicobeoordeling en prioritering 6](#_Toc191393179)

[3.2 Testen van patches 6](#_Toc191393180)

[3.3 Implementeren van patches 7](#_Toc191393181)

[3.4 Monitoring en rapportage 7](#_Toc191393182)

[4 Procesrollen en verantwoordelijkheden 8](#_Toc191393183)

# Inleiding

Patchmanagement is een essentieel proces om kwetsbaarheden in systemen, applicaties en hardware te verhelpen. Het doel is om de beveiliging, stabiliteit, en prestaties van IT-omgevingen te waarborgen door het tijdig testen en implementeren van patches. Deze procesbeschrijving beschrijft de stappen, rollen en verantwoordelijkheden die nodig zijn voor effectief patchbeheer.

# Doelstelling

De doelstellingen van deze procesbeschrijving zijn:

* Het minimaliseren van beveiligingsrisico’s door kwetsbaarheden tijdig te verhelpen.
* Het waarborgen van de continuïteit en betrouwbaarheid van IT-systemen.
* Het voldoen aan compliance-eisen, zoals ISO 27001, NEN 7510 en het Normenkader IBP.

## Reikwijdte

Deze procesbeschrijving is van toepassing op alle IT-systemen, applicaties en hardware die eigendom zijn van of beheerd worden door <vul naam organisatie in>, inclusief systemen die door leveranciers worden onderhouden. Het proces omvat:

* Servers, werkstations, netwerkapparatuur, en randapparatuur.
* Besturingssystemen, applicaties, en middleware.
* Kritieke infrastructuur en cloudservices.

Wanneer IT volledig is uitbesteed, wordt van de full-service IT-partij verwacht dat zij de operationele verantwoordelijkheden voor patchbeheer uitvoert in overeenstemming met de contractuele afspraken en SLA’s. <Naam organisatie> behoudt echter de eindverantwoordelijkheid voor:

* Het monitoren van de naleving van beveiligings- en compliance-eisen.
* Het beoordelen van rapportages over patchbeheer en kwetsbaarheden.
* Het escaleren van eventuele problemen indien nodig.

# Processtappen

Het patchmanagementproces bestaat uit vier stappen die er samen voor zorgen dat kwetsbaarheden binnen <vul naam organisatie in> goed beheerd worden. Dit proces geeft ons als organisatie inzicht in de systemen en applicaties die risico’s kunnen opleveren, stelt ons in staat om deze risico’s te beoordelen en prioriteren, en zorgt ervoor dat patches effectief worden geïmplementeerd en gecontroleerd. Door dit proces te volgen, kunnen we de beveiliging van onze IT-omgeving verbeteren en een gedegen afweging maken over prioriteiten en aanpak. Het patchmanagementproces bestaat uit de volgende vier processtappen:

1. Risicobeoordeling en prioritering
2. Testen van patches
3. Implementeren van patches
4. Monitoring en rapportage

Hieronder lichten we elke stap toe:

## Risicobeoordeling en prioritering

Deze stap heeft als doel inzicht te krijgen in de risico’s en impact van beschikbare patches, zodat de organisatie gefocust kan handelen door prioriteit te geven aan de meest kritieke kwetsbaarheden. Een gestructureerde risicobeoordeling zorgt ervoor dat de meest urgente patches als eerste worden behandeld, wat helpt om beveiligingsrisico’s te minimaliseren en de continuïteit van systemen te waarborgen.

Acties

1. Beoordeel elke beschikbare patch op:
* **Kriticiteit:** ernst van de kwetsbaarheid.
* **Impact:** potentiële schade als de kwetsbaarheid wordt misbruikt.
* **Afhankelijkheden:** hoeveel andere systemen of processen worden beïnvloed?
1. Prioriteer patches in vier categorieën: **kritiek**, **hoog**, **gemiddeld** of **laag**.
2. Documenteer de prioriteit en deadlines voor implementatie in het patchbeheerregister.

Uitkomst
Een gestructureerde prioriteitenlijst van patches met deadlines voor implementatie.

## Testen van patches

Het testen van patches is bedoeld om te garanderen dat ze compatibel en stabiel zijn voordat ze worden geïmplementeerd in de productieomgeving. Door patches eerst in een gecontroleerde testomgeving te testen, kunnen mogelijke problemen zoals systeemuitval of conflicten met andere applicaties worden voorkomen. Dit vermindert risico’s en zorgt voor een soepele implementatie in de productieomgeving.

Acties

1. Test de patch in een gesimuleerde of testomgeving die zoveel mogelijk lijkt op de productieomgeving.
2. Controleer:
* De functionele werking van de systemen.
* De compatibiliteit met andere systemen en applicaties.
* Mogelijke performanceproblemen na implementatie.
1. Stel een herstelplan op voor eventuele problemen tijdens de implementatie in productie.

Uitkomst
Geteste patches die klaar zijn voor implementatie in de productieomgeving, inclusief een herstelplan.

## Implementeren van patches

Het implementeren van patches in de productieomgeving moet zorgvuldig worden uitgevoerd om verstoringen te minimaliseren en risico’s effectief te beheersen. Een goed geplande en veilige implementatie zorgt ervoor dat kwetsbaarheden tijdig worden aangepakt zonder negatieve impact op de continuïteit van systemen.

Acties

1. Stel een implementatieplanning op. Hou hierbij rekening met de prioriteiten en beschikbaarheid van systemen.
2. Voer kritieke patches binnen de gestelde deadlines uit. Bijvoorbeeld binnen 48 uur voor kritieke kwetsbaarheden.
3. Monitor de implementatie en leg eventuele afwijkingen vast.
4. Communiceer met gebruikers over de mogelijke impact, zoals downtime of wijzigingen in functionaliteit.

Uitkomst
Patches zijn succesvol geïmplementeerd in de productieomgeving zonder verstoringen.

## Monitoring en rapportage

Na implementatie is het belangrijk om te controleren of patches correct zijn geïnstalleerd en effectief zijn in het verhelpen van kwetsbaarheden. Monitoring biedt inzicht in resterende risico’s, terwijl rapportage helpt bij het beoordelen van de voortgang en naleving van het patchmanagementproces.

Acties

1. Monitor gepatchte systemen om te controleren of de kwetsbaarheid is verholpen en het systeem stabiel functioneert.
2. Stel een periodieke rapportage op (bijvoorbeeld maandelijks of per kwartaal) met:
* Het aantal geïmplementeerde patches
* Status van kwetsbaarheden en risico's
* Eventuele uitzonderingen
* Aanbevolen vervolgacties en geplande acties
1. Deel de rapportage met relevante stakeholders, zoals het management en de proceseigenaar.

Uitkomst
Gemonitorde systemen en een rapportage die inzicht biedt in de status van het patchbeheer.

# Procesrollen en verantwoordelijkheden

|  |  |
| --- | --- |
| **Rol** | **Verantwoordelijkheden** |
| **Eerste lijn** |
| Bestuur, directie, schoolleiding   | * Goedkeuren van beleidsrichtlijnen voor patchmanagement.
* Toewijzen van middelen voor effectief patchbeheer.
* Toezicht houden op de naleving van patchmanagement.
 |
| Systeemeigenaar  | * Identificeren van systemen waarvoor zij verantwoordelijk zijn.
* Prioriteren van patches op basis van risico’s en impact.
* Escaleren van problemen of risico’s naar de proceseigenaar.
 |
| IT-medewerker  | * Implementeren van patches volgens planning.
* Testen van patches in een gecontroleerde omgeving.
* Documenteren van uitgevoerde patches en resterende risico’s.
 |
| **Tweede lijn** |
| Proceseigenaar   | * Ontwikkelen en beheren van het patchmanagementproces.
* Toezicht houden op naleving van het proces door de eerste lijn.
* Escaleren van afwijkingen naar het management.
 |
| IBP-adviseur, CISO, ISO   | * Ondersteunen bij het prioriteren van patches.
* Adviseren over de impact van niet-gepatchte kwetsbaarheden.
* Onafhankelijke audits uitvoeren.
 |
| **Extern** |
| Leverancier  | * Leveren van tijdige en veilige patches.
* Communiceren van risico’s die verband houden met kwetsbaarheden.
* Ondersteunen bij implementatie van patches.
 |