TASKFORCE
Bestuur & Informatieveiligheid Dienstverlening

# Patch management

Een operationeel product op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR)

Rijksoverheid VNG Vereniging van Nederlandse Gemeenten Interprovinciaal Overleg ip MANIFESTgroep UNIE VAN WATERSCHAPPEN

## Colofon

Onderhavig operationeel product, behorende bij de Baseline Informatiebeveiliging Rijksdienst (BIR), is mogelijk gemaakt door de Taskforce Bestuur en Informatieveiligheid Dienstverlening (Taskforce BID). Het product is gebaseerd op het operationele product ‘Patch management voor gemeenten’ behorende bij de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Dit product is ontwikkeld door de Informatiebeveiligingsdienst voor gemeenten (IBD).

## Leeswijzer

Dit document is een van de operationele producten op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR).

### Doel

Dit document beschrijft de beleidsuitgangspunten ten aanzien van informatiebeveiliging voor een invulling van het patch management beleid door organisaties binnen de Rijksoverheid. Deze uitgangspunten over informatiebeveiliging zijn afkomstig uit de BIR en het beleid voldoet daarmee aan de BIR.

### Doelgroep

Dit document is van belang voor het verantwoordelijke lijnmanagement voor wat betreft de aanvulling van het informatiebeveiligingsbeleid voor patch management. Het management, de CISO/IBF en de ICT-organisatie zijn allen betrokken bij de uitvoering en controle op het patch management.

### Reikwijdte

Dit document heeft voornamelijk betrekking op maatregel 12.6 van de Baseline Informatiebeveiliging Rijksdienst (BIR). Het document gaat in op personele, organisatorische en technische informatiebeveiligingsaspecten die organisaties binnen de Rijksoverheid dienen te overwegen in relatie tot patch management.

### Relatie met overige producten

- Baseline Informatiebeveiliging Rijksdienst (BIR). Tactisch Normenkader (TNK)
- Voorschrift Informatiebeveiliging Rijksdienst (VIR:2007)
- Informatiebeveiligingsbeleid
- Configuratiebeheer
- Hardening beleid

## Inhoudsopgave

# 1 Inleiding

De Baseline Informatiebeveiliging Rijksdienst (BIR) heeft de onderstaande maatregelen beschreven die te maken hebben met patchen van systemen in verband met het verminderen van risico's als gevolg van benutting van gepubliceerde technische kwetsbaarheden. Zie hiervoor hoofdstuk 12.6 van de BIR.

Patch management is het proces waarmee patches op gecontroleerde, beheerste (risico beperkende) wijze kunnen worden uitgerold. Patches zijn doorgaans kleine programma's die aanpassingen maken om fouten op te lossen of verbeteringen aan te brengen in bestaande programmatuur en/of hardware. Patch management wordt meestal uitgevoerd door de verantwoordelijke ICT-organisatie. Patch management kan worden uitgevoerd met speciale tooling die de gehele infrastructuur inventariseert en het patchproces ondersteunt (vulnerability scanning tools en patch tooling). Zie hiervoor ook de aanwijzing hardening voor organisatie binnen de Rijksoverheid.

Patch management wordt ook beschreven in het whitepaper Patch management van het Nationaal Cyber Security Center (NCSC) (2008), link:
https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/patchmanagement.html

## 1.1 Doelstelling patch management

Het doel van patch management is tweeledig:

1. Het inzichtelijk maken van de actuele stand van kwetsbaarheden en toegepaste patches binnen de beheerde informatievoorziening,
2. Het op een zo efficiënt mogelijke wijze en met zo min mogelijk verstoringen creëren van een stabiele (veilige) informatievoorziening.

Patch management is gericht op het verminderen van risico's als gevolg van benutting van gepubliceerde technische kwetsbaarheden.

Leveranciers van software en hardware geven regelmatig informatie over gevonden zwakheden in hun systemen, met daarbij een aanwijziging hoe deze zwakheid te bestrijden.

Door de steeds complexere samenhang van de infrastructuur is het niet altijd de beste oplossing om iedere patch door te voeren. Met een 'defense in depth'[1] strategie kan beter worden bepaald waar en wanneer patches worden doorgevoerd of waar en wanneer alternatieve oplossingen kunnen worden ingezet. Met 'defense in depth-strategie' kan bijvoorbeeld worden bepaald dat een systeem met een kwetsbaarheid niet via internet benaderbaar mag zijn, of dat een bepaalde services gestopt zou moeten worden. Door de 'defense in depth-strategie' wordt de kans kleiner dat van een kwetsbaarheid misbruik kan worden gemaakt.

[1] Defence in Depth of verdediging in de diepte is een concept waarbij meerdere lagen van security maatregelen worden gebruikt binnen een IT systeem met de bedoeling om het uitbuiten van een kwetsbaarheid tegen te gaan.

*Goed uitgevoerd patch management is essentieel om de twee bovenstaande doelstellingen te kunnen realiseren.*

## 1.2 Aanwijzing voor gebruik

Deze handreiking beschrijft een mogelijke aanpak van patch management. Het sluit aan bij bestaande ICT-beheerframework van overheidsorganisaties. Afsluitend wordt een voorbeeld gegeven voor aanvullend beleid voor patch management.

Om te voldoen aan de maatregel 12.6 van de BIR moet aan de volgende eisen worden voldaan:

1. Er is een proces ingericht voor het beheer van technische kwetsbaarheden; dit omvat minimaal periodieke penetratietests, risicoanalyses van kwetsbaarheden en patching.
2. Van softwarematige voorzieningen van de technische infrastructuur kan (bij voorkeur geautomatiseerd) gecontroleerd worden of de laatste updates (patches) in zijn doorgevoerd. Het doorvoeren van een update vindt niet geautomatiseerd plaats, tenzij hier speciale afspraken over zijn met de leverancier.
3. Indien een patch beschikbaar is, dienen de risico's verbonden met de installatie van de patch te worden geëvalueerd (de risico's verbonden met de kwetsbaarheid dienen vergeleken te worden met de risico's van het installeren van de patch).
4. Updates/patches voor kwetsbaarheden waarvan de kans op misbruik hoog is en waarvan de schade hoog is worden zo spoedig mogelijk doorgevoerd, echter minimaal binnen één week. Minder kritische beveiligingsupdates/-patches moeten worden ingepland bij de eerst volgende onderhoudsronde.

# 2 Patch managementprocessen

Patch managementprocessen dienen effectief en efficiënt uitgevoerd te worden, waarbij patch management geen op zichzelf staand proces is. Er wordt hier vanuit gegaan dat binnen de organisatie (ICT-)beheerprocessen zijn ingericht. Het heeft de voorkeur om het patch managementproces te laten aansluiten bij deze bestaande ICT-beheerprocessen. Dit maakt de implementatie van patch management makkelijker. Patch management haakt aan bij de volgende, al dan niet ITIL, beheerprocessen binnen organisaties:

### *Technisch beheer*

Het technisch beheerproces wordt uitgevoerd door technisch beheerders. Afhankelijk van de grootte van de organisatie kunnen hier specialisten zijn per systeemsoort of meerdere systemen worden door enkele personen technisch beheerd.

### *Netwerkbeheer*

Netwerkbeheerders beheren het netwerk van de organisatie. Afhankelijk van de omvang van de organisatie kan dat ook verenigd zijn in de afdeling technisch beheer.

### *Configuratie management*

Configuratie Management houdt zich bezig met het bijhouden van alle ICT-componenten van de organisatie. Deze informatie is cruciaal om vast te stellen of een patchadvies van toepassing is op de ICT-infrastructuur en applicaties.

### *Servicedesk*

De servicedesk ontvangt (beveiligings)incidenten en service calls, maar is ook betrokken bij communicatie rondom ICT-updates naar de eindgebruikers.

### *Wijzigingsbeheer*

Het wijzigingsbeheerproces is ervoor om wijzigingen op een beheerste wijze in de apparatuur en applicaties door te voeren.

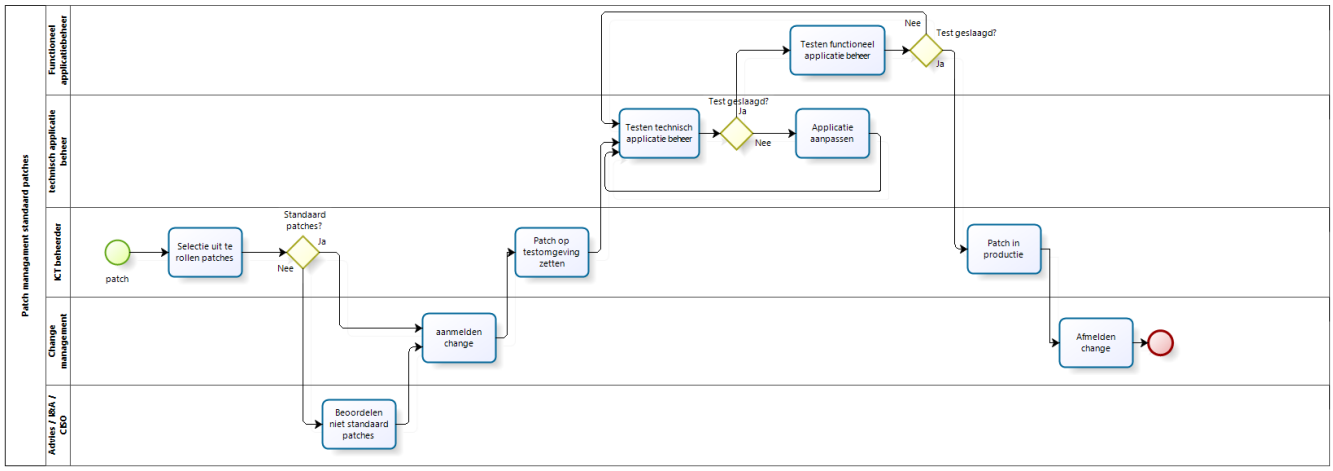
### *Technisch en functioneel applicatiebeheer*

Het technisch applicatiebeheer houdt zich voornamelijk bezig met de technische kant van applicaties, bijvoorbeeld de apparatuur waar de applicatie op draait. De functioneel applicatiebeheerders houden zich bezig met de functionele werking en (bron)gegevens, maar ook met vertalen van functionele eisen en wensen, onderhoud van de applicatie, etc.

## 2.1 Reguliere patches

Binnen ICT-beheerafdelingen hebben ICT-beheerders zelf een verantwoordelijkheid voor het bijhouden van hun vakgebied en nieuws rondom hun eigen specialisatie. Dat wil zeggen dat reguliere leverancierspatches volgens een standaard proces geïmplementeerd zouden moeten worden.

Het doorvoeren van patches zou als volgt onderdeel kunnen uitmaken van reguliere beheersprocessen:




Volgens het bovenstaande proces krijgt de ICT-beheerder informatie dat er een patch voorhanden is voor een systeem om een bepaalde zwakheid te dichten.

Heeft de patch geen invloed op de bedrijfsvoering, dan kan deze naar het change proces om als change verder behandeld te worden. In het geval een patch wel invloed heeft of dit is niet duidelijk, dan dit te worden overlegd met de CISO/informatiemanager en/of de systeemeigenaar hoe verder te gaan. Dit overleg leidt tot het doorvoeren van de patch als change, of het niet-doorvoeren van de patch, bijvoorbeeld doordat het doorvoeren vraagt om een aanpassing van een bedrijfsapplicatie. Indien de informatiemanager of systeemeigenaar vraagt om uitstel, wordt de informatiemanager/systeemeigenaar verantwoordelijk voor het doorvoeren van de patch in een latere fase.

Vanuit het change proces en na het uitvoeren van een impact assesment betreffende de change, zal de betreffende ICT-beheerder de patch op de testomgeving van de geraakte systemen installeren.

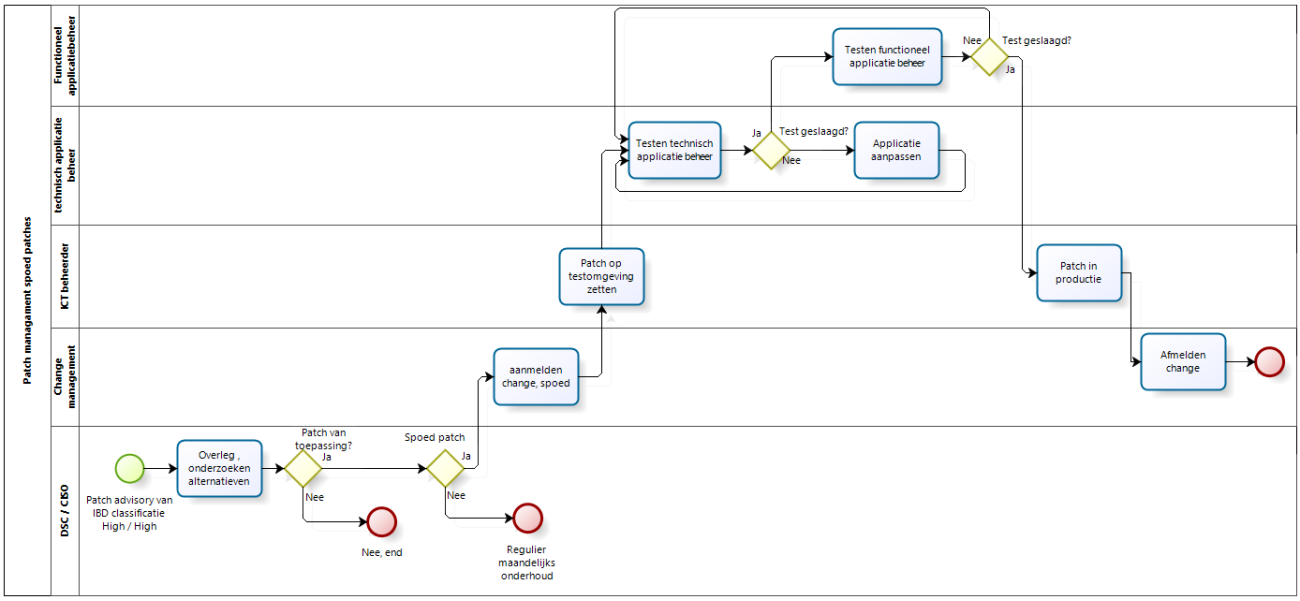
Testen worden uitgevoerd door de technisch applicatiebeheerders. Na een succesvolle test dienen de verantwoordelijken voor ketentesten en de functioneel applicatiebeheerders, eventueel aangevuld met enkele eindgebruikers, te testen of de systemen in samenhang nog werken zoals is afgesproken. Deze testen dienen goed gedocumenteerd te zijn en van alle testen dient een testverslag te worden gemaakt. De roll back, ook bij implementatie van de patch, is een aandachtspunt. Na een succesvolle update dient de configuratiedatabase te worden bijgewerkt met de nieuwe versienummers. Van alle uitgevoerde en niet uitgevoerde patches wordt een logboek bijgehouden.

## 2.2 Spoed-patches

Vanuit een Computer Emergency Response Team (CERT), zoals het NCSC, kunnen adviezen over kwetsbaarheden binnenkomen bij de afgesproken contactpersoon van de organisatie. Bij een hoge kans op misbruik en een hoge kans op schade is het belangrijk

beschikbare, zogenaamde, spoed-patches zo snel mogelijk door te voeren. Voor alle patches dient beoordeeld te worden of het via een regulier change proces geïmplementeerd kan worden, of dat een spoedproces nodig is.

Het implementatieproces voor spoed-patches zou er als volgt kunnen uitzien:




Volgens het bovenstaande proces komt het advies van een CERT, zoals het NCSC, binnen bij de contactpersoon van de organisatie.

Er wordt overleg gevoerd met de relevante beheerders/partijen. Eventueel wordt de configuratiedatabase geraadpleegd om vast te stellen of de patch nog wel van toepassing is. Binnen dit overleg kan ook worden bepaald of andere mitigerende maatregelen te nemen zijn om patching eventueel op een later moment uit te kunnen voeren.

Blijft de noodzaak tot een spoed-patch bestaan, dan dient het wijzigingsproces verkort doorlopen te worden. Hierbij dient de patch altijd te worden getest. Na succesvol patchen zijn de systemen weer up-to-date. De configuratiedatabase wordt bijgewerkt met de nieuwe versienummers.

# 3 Controle op de werking van het patch proces en rapportage

Om vast te stellen of er nog bekende zwakheden in de eigen ICT-infrastructuur of applicaties aanwezig zijn, kan een zwakhedenscan of vulnerability scan (laten) worden uitgevoerd. Meestal wordt daarbij speciale tooling gebruikt. Deze tooling kent van iedere soort hardware en software wat de laatste updates zijn en kan ook toetsen op het aanwezig zijn van bekende zwakheden. Het resultaat is dan een rapport met alle mogelijke aanbevelingen welke geprioriteerd zijn op belangrijkheid. Met dit rapport kunnen gericht patches worden geïnstalleerd of systemen worden vervangen voor nieuwere versies.

De vulnerability scan kan worden uitgevoerd door een ICT'er of bijvoorbeeld de CISO binnen de organisatie. Het uitvoeren van een vulnerability scan is geen hacking of het uitvoeren van een pentest. De vulnerability scan is een belangrijk onderdeel in het onderhouden van de informatieveiligheid binnen de eigen ICT-infrastructuur. Elke verandering van apparatuur en/of software kan nieuwe zwakheden introduceren.

Het is aan te bevelen om eerdere scanrapportages te bewaren om verschillen te ontdekken. In ieder geval moet dit gedaan worden voor belangrijke systemen. Alle veranderingen in systemen (open netwerkpoorten, toegevoegde services) dienen onderzocht te worden. Aangepaste open netwerkpoorten en aangepaste services kunnen een belangrijke indicator zijn voor het aanwezig zijn van malware, een ondernomen hack poging of een niet geautoriseerde change.

## 3.1 Verschil vulnerability scan en pentest

| | **Vulnerability Scan** | **Penetratie Test** |
|---|---|---|
| **Hoe vaak uitvoeren** | Zo vaak als mogelijk, als onderdeel van normale werkzaamheden | Indien nodig |
| **Rapportage** | Uitvoerig rapport met alle zwakheden/issues per systeem | Alleen over het te onderzoeken systeem of functie |
| **Resultaat** | Lijsten met bekende zwakheden per systeem | Onderzoek naar onbekende zwakheden en risico's |
| **Door wie** | Security/ICT-specialist met ervaring met de juiste tooling | Specialist |
| **Kosten** | Eigen uren en product kosten | Afhankelijk van diepgang en controlepunten |

## Bijlage: Voorbeeld ‘Patch managementbeleid <organisatie>’

Het patch managementbeleid van de overheidsorganisatie geeft richting aan de wijze waarop de organisatie maatregelen wenst te treffen voor een adequate inrichting en uitvoering van patch management. De organisatie onderschrijft het belang van patch management omdat het niet op een gestructureerde wijze bijhouden van patches voor overheidssystemen er voor kan zorgen dat de kwetsbaarheid van die systemen toeneemt. Dit beleid is van toepassing op iedereen die binnen de organisatie een rol heeft in het uitvoeren van patch management.

De volgende uitgangspunten zijn vastgesteld voor overheidsorganisatie en deze zijn ontleend aan het informatiebeveiligingsbeleid van de Rijksoverheid, de Code voor Informatiebeveiliging (NEN/ISO 27002:2007) en de BIR:

1. Er is een proces ingericht voor het beheer van kwetsbaarheden en patching van (systeem)software binnen de organisatie.
2. Van softwarematige voorzieningen van de technische infrastructuur kan (bij voorkeur geautomatiseerd) gecontroleerd worden of de laatste updates (patches) in zijn doorgevoerd. Het doorvoeren van een update vindt niet geautomatiseerd plaats, tenzij hier speciale afspraken over zijn gemaakt met de leverancier.
3. Indien een patch beschikbaar is, dienen de risico's verbonden aan de installatie van de patch te worden geëvalueerd. De risico’s van de kwetsbaarheid dienen op te wegen tegen de risico’s verbonden aan het installeren van de patch. Bij deze evaluatie worden op zijn minst de CISO en de systeemeigenaar betrokken.
4. De technische integriteit van programmapakketten en infrastructurele programmatuur wordt gecontroleerd door middel van een hashingmechanisme en een controlegetal van de leverancier, dat via een vertrouwd kanaal is verkregen.
5. Alle patches dienen voor installatie te worden getest.
6. Behoudens de door de leverancier goedgekeurde updates worden er geen wijzigingen aangebracht in programmapakketten en infrastructurele programmatuur.
7. Updates/patches voor kwetsbaarheden waarvan de kans op misbruik hoog is en waarvan de schade hoog is, worden zo spoedig mogelijk doorgevoerd, echter minimaal binnen één week. Minder kritische beveiligings-updates/patches moeten worden ingepland bij de eerst volgende onderhoudsronde van het systeem.
8. Als een systeem gepatcht is, wordt de systeemdocumentatie bijgewerkt naar de laatste stand van zaken en de configuratiemanagement database wordt geüpdate met de nieuwe versienummers van componenten.
9. Van alle uitgevoerde en niet-uitgevoerde patches wordt een logboek bijgehouden.

Aldus vastgesteld door de directie van *[organisatie]* op *[datum]*,

[Naam. Functie] [Naam. Functie]

_____ _____