Auditdienst Rijk
Ministerie van Financiën

Patchmanagement bij Infrastructuur en Waterstaat (IenW)

Definitief

Colofon

Titel	Patchmanagement bij Infrastructuur en Waterstaat (IenW)
Uitgebracht aan	Hoofddirecteur Financiën, Management en Control (FMC) / Chief Information Officer (CIO)
Datum	21 november 2019
Kenmerk	2019-0000192788
Bijlagen	5

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

Aanleiding opdracht

Aanleiding

In de beslisnota van de hoofddirecteur Financiën Management en Control (FMC) (d.d. 8 november 2017) aan de CIO-raad van het ministerie Infrastructuur en Waterstaat (IenW) is verzocht om de vaststelling van een generiek patchmanagementproces voor geheel IenW en deze na vaststelling op intranet te publiceren. In deze nota verwoordt de hoofddirecteur, dat de CIO-raad IenW van 7 juni 2017 constateert dat er binnen de organisatieonderdelen van IenW wel een patchbeleid is, maar dat momenteel generiek patchbeleid voor heel IenW rondom het doorvoeren van de patches ontbreekt. Dit heeft voor FMC geleid tot de actie om dit voor IenW breed op gaan te stellen. De intentie van het besluit om vaststelling van het generiek patchmanagementproces is dat elk organisatieonderdeel het generiek proces als basis hanteert bij eigen implementatie van patchmanagement en daarbij organisatie of systeem specifieke afspraken documenteert binnen de eigen managementsystematiek. De CIO-raad IenW heeft positief gereageerd op de beslisnota en heeft ingestemd met de voorgestelde acties.
Een andere actie die in de beslisnota is opgenomen is het verzoek van de hoofddirecteur voor een IenW breed ADR-onderzoek naar de implementatie van de procedure. Dit rapport is hiervan de uitwerking.

De opdrachtgever heeft aangegeven de implementatie van het patchmanagementproces en de regie hierop (binnen het organisatieonderdeel en richting leveranciers) bij een select aantal organisatieonderdelen van IenW te willen laten onderzoeken. Voor inzicht in de wijze waarop het organisatieonderdeel patchmanagent heeft vormgegeven, al dan niet op basis van het generieke patchmanagementproces IenW, heeft de opdrachtgever onderstaande organisatieonderdelen en kritische systemen geselecteerd:

- Inspectie Leefomgeving en Transport (ILT), Empic Medical
- Koninklijk Nederlands Meteorologisch Instituut (KNMI), KDC (data.knmi.nl)
- Rijkswaterstaat (RWS), cluster bedienen object (industriële automatisering)

Doelstelling

De doelstelling van het onderzoek is de opdrachtgever inzicht te bieden in de opzet (documentatie) en het bestaan (uitvoering) van de implementatie van en de regie op patchmanagement bij enkele organisatieonderdelen van IenW.

De onderzoeksvragen bij deze doelstelling luiden:

1. Welke controlemaatregelen hebben de organisatieonderdelen getroffen met betrekking tot de implementatie van en de regie op patchmanagement?
2. In hoeverre sluiten deze maatregelen aan op het generieke patchmanagementproces IenW?
3. Hoe verhouden deze maatregelen zich tot de eisen uit BIR2017?

Het antwoord op onderzoeksvraag één en twee is opgenomen in hoofdstuk 1. Met beantwoording van vraag één is onderzoeksvraag drie ook direct beantwoord. Voor onderzoeksvraag drie is namelijk inzicht benodigd in de maatregelen die door een organisatieonderdeel op het gebied van patchmanagement zijn genomen. Het beeld dat daaruit ontstaat dient te worden getoetst aan de normen uit de BIR2017, om vervolgens hun onderlinge verhouding te kunnen duiden. Bij beantwoording van onderzoeksvraag één is reeds inzicht gegeven in de genomen maatregelen, waarbij de aangetroffen situatie is getoetst aan (een selectie van) eisen uit de BIR2017. In hoofdstuk 2 is de verantwoording van het onderzoek opgenomen. De bijlagen bevatten de resultaten per onderzocht organisatieonderdeel, het generiek patchmanagementproces IenW en de ontvangen documentatie.

Centrale boodschap

Een goed ingericht patchmanagementproces draagt dus bij aan een veilige digitale omgeving. ADR is gevraagd een onderzoek uit te voeren naar de implementatie en de regie op dit proces bij enkele organisatieonderdelen van IenW.
Voorafgaand aan het onderzoek heeft de opdrachtgever aangegeven dat er met betrekking tot de status van patchmanagement bij de organisatieonderdelen geen goede of foute situatie bestaat in de beantwoording van de onderzoeksvragen. Elk antwoord is goed, want biedt hulp om - indien nodig - op de goede wijze te verbeteren. Dit rapport moet bijdragen aan het verschaffen van inzicht of verbetering nodig of wenselijk is.

Uit dit onderzoek komt naar voren dat in het generieke patchmanagementproces IenW het merendeel van het aantal elementen worden benoemd van het totaal aan elementen dat voorgesteld wordt om in een patchmanagementproces op te nemen.

Zowel ILT als KNMI geven aan het generieke patchmanagentproces IenW te hebben overgenomen. Uit dit onderzoek komt naar voren dat beide organisaties dat niet gemotiveerd hebben vastgelegd. Ook blijkt niet of ILT en KNMI het generieke patchmanagementproces onverkort hebben overgenomen of dat zij het patchproces in enige mate hebben aangepast en uitgewerkt naar de eigen organisatie. Volgens de beslisnota van de hoofddirecteur FMC (d.d. 8 november 2017) aan de CIO-raad van het ministerie IenW was een motivatie van hoe organisaties zijn omgegaan met het generieke patchmanagementproces IenW namelijk wel gewenst.

Uit dit onderzoek komt verder het beeld naar voren dat bij de organisaties ILT en KNMI het beleid en de informatie- en sturingslijnen over de regie van patchmanagement onduidelijk zijn én er geen duidelijke monitoring over de uitvoering van patches plaatsvindt. Control op uitvoering van het patchmanagementproces is niet aangetoond, alsook of software & patches afdoende beheerst worden geïnstalleerd en de beveiligingscomponenten van deze software sterk zijn ingericht.
In de praktijk wordt het patchlevel ten aanzien van de onderzochte informatiesystemen KDC en Empic Medical, bij resp. KNMI en ILT wel actueel bijgehouden.

Ten aanzien van RWS bestaat dit beeld niet. RWS heeft aangetoond dat voor de onderzochte systemen/projecten gewerkt wordt volgens een gedocumenteerd patchproces, dat bij uitbesteding RWS hierop zelf toezicht houdt en dat het patchproces is uitgebreid ten behoeve van industriële automatisering. Binnen dit onderzoek is gekeken naar de objecten Gaasperdammertunnel en Beatrixsluis. Een probleem dat RWS op dit moment heeft, is dat er nog wel een aantal oude contracten zijn waar het gewenste beheersregime van RWS nog niet van kracht is.

1 Bevindingen

In dit hoofdstuk zijn de feitelijke bevindingen opgenomen en wordt in gegaan op onderzoeksvraag 1 en 2.

Onderzoeksvraag 1: Welke controlemaatregelen hebben de organisatieonderdelen getroffen met betrekking tot de implementatie en regie van het proces patchmanagement?

1.1 Implementatie van generiek patchmanagementproces

Met de implementatie van het generieke patchmanagementproces wordt bedoeld dat de organisatieonderdelen van IenW het generieke proces implementeren door dit als basis te hanteren en indien nodig organisatie of systeem specifieke afspraken te documenteren binnen de eigen managementsystematiek. Als onderdeel van de toetsing op implementatie is ADR gevraagd het generieke patchproces te toetsen op de aanwezigheid van de voornaamste elementen van een patchmanagementproces (zie bijlage 2 vraag 1).

1.1.1 Generiek patchmanagement IenW bevat 12 van 17 voornaamste elementen

Voor het generieke patchmanagementproces IenW (bijlage 1) is bekeken of elementen uit de richtlijnen van de NCSC en Taskforce met betrekking tot patchmanagement zijn vast te stellen in het generieke proces dat IenW voor patchmanagement heeft opgesteld.

De aanwezigheid van onderstaande elementen in het proces is nagegaan:

1. Inleiding
2. Proceseigenaar, -input en –output
3. Kritische Prestatie Indicatoren
4. Procesflow(diagram)
5. Reguliere en Urgente (security) patches
6. Constatering kwetsbaarheid
7. Patch benodigd
8. Impact bepaling
9. Communicatie
10. Patchregistratie
11. IJking van beveiligingsadviezen
12. Vaststellen actieplan
13. Testen en uitrollen *(a)* & betrekken diverse (OTAP)omgevingen (*b*)
14. Bijwerken documentatie
15. Evaluatie
16. Aansluiting op bestaande beheerprocessen
17. Taken en verantwoordelijkheden & RACI-matrix

Van deze elementen komen twee aspecten niet terug in het generiek proces:

3. Kritische Prestatie Indicatoren (KPI's)
Een expliciete benoeming van wat voor het patchmanagementproces de KPI's zijn is niet beschreven. Wel is een beschrijving van het doel opgenomen:

- Zorgen dat de organisatie en de systeemeigenaar inzicht heeft op de actuele stand van kwetsbaarheden en toegepaste patches binnen de beheerde infrastructuur en/of het informatiesysteem.
- Zorgen dat op een efficiënte wijze met zo min mogelijk verstoringen een dienst of product kan worden geleverd doordat een stabiel (veilig) systeem wordt gecreëerd of blijft behouden.

13b. Betrekken diverse (OTAP) omgevingen
Een expliciete benoeming over uitrollen naar diverse (OTAP)omgevingen is niet opgenomen. In de procesbeschrijving is wel in processtap 3 *Vastleggen besluit patch* opgenomen dat "Voorafgaand aan het inzetten van de patch wordt deze, indien mogelijk getest".

Van de nagelopen elementen komen de volgende drie aspecten deels terug in het generiek patchmanagementproces IenW:

12. Vaststellen actieplan
Het maken van een actieplan is niet expliciet opgenomen. Wel wordt verwezen naar en aangehaakt bij het proces wijzigingsbeheer als middel om patches door te voeren.

13a. Testen en uitrollen
Dit element is summier opgenomen en niet expliciet als processtap. In de procesbeschrijving is wel in processtap 3 *Vastleggen besluit patch* opgenomen dat "Voorafgaand aan het inzetten van de patch wordt deze, indien mogelijk getest". Zie ook punt 13 hierboven.
De wijze van uitrollen is opgenomen in de vorm van het besluit door de eigenaar van een systeem (in overleg met een deskundige/adviseur beveiliging), toetsing op het beste moment/datum van uitvoering en beschikbaarheidseisen van systemen.

17. RACI-matrix
In het generiek patchmanagementproces IenW is het element taken en verantwoordelijkheden opgenomen, alsook de rollen (eigenaar informatiesysteem/beheer) en de bijbehorende beschrijving van deze rollen. Een aanvullende matrix waarin de rollen zijn gekoppeld aan de kenmerken Responsible (verantwoordelijk), Accountable (eindverantwoordelijk), Consulted (geraadpleegd) en Informed (geïnformeerd) is niet opgenomen.

1.1.2 *Implementatie bij organisatieonderdelen van generiek patchmanagementproces IenW loopt uiteen*

ILT en KNMI
Volgens mededeling heeft het management van zowel ILT als KNMI het centrale generieke patchproces IenW geaccordeerd en overgenomen. Hiervan is geen vastlegging aangetroffen. In de praktijk wordt het patchlevel ten aanzien van de onderzochte twee informatiesystemen bij KNMI en ILT wel actueel bijgehouden. Wij hebben niet kunnen vaststellen dat ILT en KNMI het eigen patchproces in praktijk volgens het generieke patchmanagementproces IenW uitvoeren. Een opvolging hiervan of afwijking van het generiek proces blijkt namelijk niet uit de aangeleverde documenten. Het generieke patchproces IenW is bij ILT en KNMI voor de onderzochte systemen in opzet en bestaan niet verder uitgewerkt.

RWS
RWS heeft het generieke IenW-patchproces overgenomen en uitgebreid, gezien de eisen die gesteld worden aan beheer en onderhoud van de industriële automatisering in kunstwerken (bruggen, tunnels, sluizen en viaducten) en welke op veel vlakken afwijken van het patchproces van kantoorautomatisering. Beheer en onderhoud zoals die van de waterwegen worden uitgevoerd door de aannemers en zijn contractueel vastgelegd. Een van de eisen aan de aannemer is dat softwarewijzigingen & patches via een OTAP-straat worden uitgevoerd. Het toezicht op de uitvoering hiervan wordt gedaan door RWS zelf, via systeem gerichte contractbeheersing en/of inspecties. Voor de uitvoering van patchmanagement heeft RWS een richtlijn vervaardigd.

1.2 Regie op patchmanagement

Met regie op patchmanagement wordt bedoeld dat (het management van) de organisatieonderdelen van IenW aantoonbare en navolgbare controlemaatregelen hebben geïmplementeerd om beheersing van hun patchproces (welke idealiter zoveel als mogelijk aansluit op het generieke patchproces van IenW) te waarborgen. Het patchmanagementproces dient te zijn gekoppeld aan een patchbeleid waarin de uitgangspunten voor het patchmanagementproces zijn vastgelegd. Het patchbeleid is onderdeel van een (integraal) informatiebeveiligingsbeleid. Informatiebeveiliging schept daarmee kaders en randvoorwaarden voor patchbeleid.

Onder controlemaatregelen van patchmanagement wordt onder andere verstaan:

- Een systeem heeft een eigenaar, een regiehouder;
- Er is een proces gedefinieerd, waarin controles zijn vast gelegd.
    - Indien het proces door derden wordt uitgevoerd dan is met die partij een service level agreement, convenant of een contract afgesloten, waarin onder andere het patchproces, impactbepaling, testen, logging, de communicatie en verantwoording hierover is beschreven;
    - Indien de organisatie zelf verantwoordelijk is voor de uitvoering van patchmanagement (bijvoorbeeld voor onderhoud van een applicatie) dan is bovenstaande in een document beschreven en door het management geaccordeerd.

1.2.1 In control ILT en KNMI op patchbeleid en informatiebeveiligingsgebeurtenissen niet aangetoond (normen 5.1.1, 5.1.2 en 12.1.1)

Doel van beleid is het voorzien in processen en maatregelen om te kunnen acteren als er een onverwachte informatiebeveiligingsgebeurtenis optreedt. Indien zo'n incident optreedt, dient er door het management gemonitord en bijgestuurd te worden. Bij zowel ILT als KNMI is er geen documentatie aangeleverd waaruit blijkt dat ze ten aanzien van informatiebeveiligingsgebeurtenissen in opzet en bestaan in control zijn. Er is geen documentatie ontvangen die de stelselmatige beoordeling van het beleid op beveiligingsbeleid(afspraken) aantoont. Er is geen doorvertaling aangetroffen van het beveiligingsbeleid naar de te beschermen systemen en applicaties van deze organisaties (wat dient extra beveiligd te worden en wat niet) en daaraan gekoppeld patchbeleid. Een beveiligingsbeleid is een voorwaarde voor het kunnen uitvoeren en inrichten van patchbeleid
Bij ILT is geen actueel documentatiebeheer aangetroffen. De status en versies van ontvangen documenten waren onduidelijk of gedateerd. ILT geeft verder aan dat een (herijking van) patchbeleid, als onderdeel van informatiebeveiliging, niet aanwezig is. Op dit moment is KNMI bezig met een integraal beveiligingsplan om issues op te pakken, waarvan het patchbeleid onderdeel is.

1.2.2 Zicht op patches bij ILT en KNMI deels aanwezig (norm 12.1.1)

Het is belangrijk zicht te hebben op informatiebeveiligingswijzigingen en patches die de essentiële informatiesystemen van de organisatie beter beveiligen. Uit het onderzoek komt naar voren dat ILT en KNMI hier deels inzicht in hebben en in de uitvoering voornamelijk steunen op hun Shared Service Organisaties. Informatie- en sturingslijnen met betrekking tot monitoring van informatiebeveiligingswijzigingen en patches behoeven aandacht.

1.2.3 Beheersing van te installeren software & patches en de beveiliging hiervan bij ILT en KNMI niet aangetoond (norm 12.5.1)

Hacking van informatiesystemen geeft risico's t.a.v. de bedrijfsvoering van de organisatie. Daarom worden er eisen gesteld aan installatieprocedures en de sterkte van software tegen ongewenst misbruik door bijvoorbeeld hardening van systemen en vulnerability scanning toe te passen. Uit de antwoorden van ILT en KNMI blijkt dat er wel controle is op gebruikte accounts, maar dat niet is aangetoond dat software & patches beheerst worden geïnstalleerd en de beveiliging van het onderzochte informatiesysteem sterk is ingericht om ongewenst gebruik te voorkomen.

1.2.4 *Onduidelijk zicht op controle en monitoren van leveranciers of die voldoen aan de beveiligingseisen en tijdige patching (norm 15.2.1)*

Uit de aangeleverde informatie blijkt niet dat KNMI, ILT en RWS zicht hebben of de leveranciers voldoen aan de beveiligingseisen en indien nodig op tijd patches uitvoeren. RWS geeft wel aan dat bij realisatie van industriële automatisering via Toetsen (Systeem gerichte contractbeheersing) er getoetst wordt of de aannemer de industriële automatisering beveiligd oplevert (inclusief relevante patches).

1.2.5 *Beheer van technische kwetsbaarheden bij ILT en RWS behoeft aandacht (norm 12.6.1)*

Wij hebben van ILT geen evaluaties, SLA's, contracten, rapportages ontvangen aan de hand waarvan wij konden vaststellen of en hoe technische kwetsbaarheden van informatiesystemen worden beheerst en hoe patching wordt toegepast om de risico's die gepaard gaan met technische kwetsbaarheden te mitigeren.
Controle bij RWS op de realisatie van industriële automatisering gebeurt via toetsen. RWS heeft hiervoor het Systeem gerichte Contract Beheersing (SCB) ontwikkeld. Indien een kunstwerk (bruggen, tunnels, sluizen en viaducten) wordt opgeleverd dan vindt er een verificatie en validatie plaats ten aanzien van de gestelde eisen van cybersecurity. Om te controleren of het wijzigingsbeheer & patching door de ondernemer die het kunstwerk beheert voldoende wordt uitgevoerd, vinden er (naast SCB) toetsen zoals IMPAKT en FIT plaats. Een probleem dat RWS op dit moment heeft, is dat er nog een aantal oude contracten zijn waar het gewenste beheersregime van RWS nog niet van kracht is.

1.2.6 *Zicht op (de response op) informatiebeveiligingsincidenten deels aanwezig (normen 16.1.2 en 16.1.5)*

Als er een beveiligingsincident plaats vindt dan wil je hiervan op de hoogte zijn, zodat er desgewenst aanvullende (organisatorische of technische) maatregelen genomen kunnen worden. Zicht op beveiligingsincidenten zijn relevant en kunnen een trigger zijn voor het doorvoeren van patches. Dit ter voorkoming van eventuele consequenties voor de beherende organisatie en het ontstaan van imagoschade aan de verantwoordelijke uitbestedende organisatie. Uit de aangeleverde informatie blijkt dat:

- ILT op dit gebied geen (patch)beleid heeft aangetoond. Daarbij hanteert ILT wel een registratiemethodiek, maar is het onduidelijk of er analyses en rapportages worden vervaardigd.
- KNMI klantrapportages ontvangt, waarin incidenten gemeld staan. Onduidelijk is of de incidenten gecategoriseerd zijn, zodat consequent inzichtelijk wordt of er in een bepaalde periode sprake is geweest van beveiligingsincidenten. Er is aangegeven dat er indien nodig geëscaleerd wordt. Een beschrijving van hoe dit proces in de praktijk verloopt, wie er betrokken worden en of patching heeft plaatsgevonden is niet ontvangen.

1.3 Aansluiting op generiek patchmanagementproces onduidelijk

Onderzoeksvraag 2: In hoeverre sluiten deze maatregelen aan op het generieke patchmanagementproces IenW?

Vastgesteld is dat bij de organisatieonderdelen met betrekking tot het patchmanagementproces de rollen eigenaren en beheerders worden onderscheiden en dat er gewerkt wordt met Service Level Agreements, welke worden afgesloten met dienstleveranciers. Ook wordt wijzigingenbeheer onderscheiden. Deze onderdelen sluiten aan op het generieke patchmanagementproces IenW. Voor andere aspecten zoals registreren en beoordelen patch, verantwoording afleggen en beheer documentatie is door KNMI en ILT niet aantoonbaar gemaakt in hoeverre getroffen maatregelen aansluiten op het generieke patchmanagementproces IenW. KNMI en ILT wijken hiermee af van het generieke patchmanagentproces IenW. RWS uitgezonderd ontbreekt het bij ILT en KNMI aan een (actueel) patchbeleid en –proces.

2 Verantwoording onderzoek

2.1 Werkzaamheden en afbakening

De uitgevoerde werkzaamheden waren gericht op het inzichtelijk maken van de aangetroffen situatie met betrekking tot het patchmanagement bij enkele organisatieonderdelen van IenW en hierover te rapporteren.

Conform de opdrachtbevestiging (2018-0000214182, d.d. 6 december 2018) zijn de objecten van onderzoek getoetst aan een door de ADR en gedelegeerde opdrachtgever vastgesteld referentiekader met betrekking tot patchmanagement, welke is gebaseerd op BIR2017 normen (bijlagen 2-4).

Het onderzoek is door de ADR uitgevoerd in de periode 1 januari 2019 t/m 1 mei 2019.

Onze belangrijkste werkzaamheden gedurende de onderzoeksperiode voor de beoordeling in opzet en bestaan betroffen:

- Het verkrijgen van inzicht in relevante kenmerken van de organisatie en geselecteerde systemen;
- Het houden van interviews met verantwoordelijke functionarissen;
- Het kennis nemen en beoordelen van documentatie en de resultaten van uitgevoerde interne controles en eigen waarnemingen.

De systemen waarvoor de door de organisatie getroffen maatregelen zijn onderzocht omvatte:

- Inspectie Leefomgeving en Transport (ILT), Empic Medical
- Koninklijk Nederlands Meteorologisch Instituut (KNMI), KDC (data.knmi.nl)
- Rijkswaterstaat (RWS), hoofdvaarwegen netwerk – cluster bedienen object (SCADA/PLC, industriële automatisering)

2.2 Beantwoordingswijze onderzoeksvragen

Hieronder gaan wij in op de wijze waarop de onderzoeksvragen uit de opdrachtbevestiging zijn beantwoord.

1. *Welke controlemaatregelen hebben de organisatieonderdelen getroffen met betrekking tot de implementatie en regie van het proces patchmanagement?*

   Deze onderzoeksvraag betreft de onderdelen implementatie van het patchmanagementproces gebaseerd op het generieke patchmanagementproces IenW en de regie door organisatieonderdelen op het proces van doorvoeren van patches.
   Voor de beantwoording van het eerste deel (implementatie) van de onderzoeksvraag is gebruik gemaakt van door de opdrachtgever opgegeven specifieke vragen, waaronder "*Bevat het generieke patchmanagementproces de voornaamste ingrediënten"* en "*Hoe is de lokale implementatie van het patchmanagementproces bij de organisatieonderdelen verlopen?*" (zie hiervoor de matrices in de bijlagen 2 t/m 4).
   Bij de beantwoording van het tweede deel (regie) van de onderzoeksvraag is gebruik gemaakt van een selectie van eisen uit de BIR2017 gericht op patchmanagement. De geselecteerde eisen en daarmee de te toetsen normen zijn door de opdrachtgever aangereikt (zie hiervoor tevens de matrices in de bijlagen 2 t/m 4).

   Als onderdeel van onderzoeksvraag één heeft de opdrachtgever met betrekking tot de implementatie van patchmanagement de aanvullende vraag gesteld of in het generieke patchmanagementproces IenW inhoudelijk de juiste zaken staan (zie vraag 1 in de bijlagen 2-4).

Voor het inzichtelijk maken van deze vraag zijn tijdens het onderzoek de richtlijnen van de NCSC[1] en Taskforce[2] Bestuur en Informatieveiligheid Dienstverlening op het gebied van informatiebeveiliging/(patch)beheerprocessen gehanteerd. Zowel de NCSC en de Taskforce zijn binnen de rijksoverheid vooraanstaande partijen wiens richtlijnen door rijksoverheid organisaties regelmatig worden opgevolgd.

Met betrekking tot het patchmanagementproces is vastgesteld of de elementen uit de richtlijnen van de NCSC en Taskforce zijn gebruikt in het generieke patchmanagementproces IenW.

Hierbij zijn wij de aanwezigheid nagegaan van onderstaande elementen:

- Inleiding
- Proceseigenaar, -input en –output
- Kritische Prestatie Indicatoren
- Procesflow(diagram)
- Reguliere en Urgente (security) patches
- Constatering kwetsbaarheid
- Patch benodigd
- Impact bepaling
- Communicatie
- Patchregistratie
- IJking van beveiligingsadviezen
- Vaststellen actieplan
- Testen en uitrollen & betrekken diverse (OTAP)omgevingen
- Bijwerken documentatie
- Evaluatie
- Aansluiting op bestaande beheerprocessen
- Taken en verantwoordelijkheden & RACI-matrix

2. *In hoeverre sluiten deze maatregelen aan op het generieke patchmanagementproces IenW?*

   Voor de beantwoording van deze vraag is bekeken of aspecten uit het generieke patchmanagementproces IenW herkenbaar zijn in de door de organisatieonderdelen getroffen controlemaatregelen. Hierbij is gekeken naar de aspecten patchbeleid en –proces, rollen, registratie en beoordelen patch, besluitvorming, rapportage en evaluatie patch, alsook Service Level Agreements, wijzigingenbeheer en documentbeheer.

3. *Hoe verhouden deze maatregelen zich tot de eisen uit BIR2017?*

   Voor de beantwoording van deze vraag is inzicht benodigd in de maatregelen die door een organisatieonderdeel op het gebied van patchmanagement zijn genomen. Het beeld dat daaruit ontstaat dient te worden getoetst aan de normen uit de BIR2017 om vervolgens hun onderlinge verhouding te kunnen duiden. Bij beantwoording van onderzoeksvraag één wordt reeds inzicht gegeven in de genomen maatregelen waarbij de aangetroffen situatie per organisatieonderdeel is getoetst aan een selectie van eisen uit de BIR2017. Onderzoeksvraag drie is daarmee indirect ook beantwoord en daarom in dit rapport verder niet expliciet uitgewerkt.

2.3 Gehanteerde onderzoekstandaard

Deze opdracht is uitgevoerd in overeenstemming met de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing.

---

[1] https://www.ncsc.nl/binaries/content/documents/ncsc-nl/actueel/whitepapers/patchmanagement/1/Whitepaper%2BPatchmanagement.pdf
[2] https://www.cip-overheid.nl/wp-content/uploads/2018/01/BID-Operationale-producten-BIR-002-Implementatie-BIR-v1.0.pdf

Ten tijde van rapportage waren bovenstaande documenten niet meer op internet beschikbaar, maar zijn wel aanwezig in het onderzoeksdossier.

In dit rapport wordt geen zekerheid verschaft, omdat er geen assurance-opdracht is uitgevoerd.

2.4 Hoor en wederhoor

De bevindingenmatrices (zoals opgenomen in bijlagen 2-4) zijn begin mei 2019 met de auditees van deze opdracht via de e-mail afgestemd, te weten:

- ILT: Sr. Adviseur Integrale beveiliging en Privacy-bescherming/ Functioneel Beheerder
- KNMI: Beveiligings- en privacycoördinator
- RWS: Coördinator Security by Design IV en IA

Tevens zijn vragen en het commentaar van ILT op de bevindingen in een separate bijeenkomst op 6 mei 2019 nog nader door ILT en ADR besproken.
Hierbij moet worden vermeld dat afstemming van de bevindingen met ILT werd bemoeilijkt door het vertrek van de Sr. Adviseur Integrale beveiliging en Privacy-bescherming tijdens het onderzoek. Een geschikte en tijdige vervanger was op het moment van de eerste afstemming van de bevindingen niet beschikbaar. Hierdoor konden de bevindingen alleen worden afgestemd met de Functioneel Beheerder. Tijdens het opmaken van de conceptrapportage zijn de bevindingen alsnog afgestemd met een tweede Beveiligingscoördinator/Privacy coördinator van ILT.

Het conceptrapport is op 25-6-2019 afgestemd met de contactpersoon van de opdrachtgever, de Senior Adviseur integrale beveiliging, IenW/FMC/DBOI.

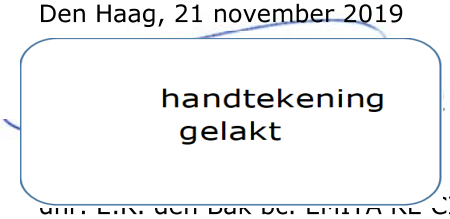
2.5 Verspreiding rapport

De opdrachtgever, mw. drs. H.J. Beentjes (hoofddirecteur FMC/CIO), is eigenaar van dit rapport.

De ADR is de interne auditdienst van het Rijk. Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen. In de ministerraad is besloten dat het opdrachtgevende ministerie waarvoor de ADR een rapport heeft geschreven, het rapport binnen zes weken op de website van de rijksoverheid plaatst, tenzij daarvoor een uitzondering geldt. De minister van Financiën stuurt elk halfjaar een overzicht naar de Tweede Kamer met de titels van door de ADR uitgebrachte rapporten en plaatst dit overzicht op de website.

3 Ondertekening

Den Haag, 21 november 2019



drs. E.K. den Bak RE CISSP

Senior IT Auditor
Auditdienst Rijk

4 Managementreactie

"Wij hebben deze audit laten uitvoeren in het kader van de PDCA, de check fase. De resultaten geven aan dat de implementatie van het generieke patchmanagement proces over de hele linie nog niet op het noodzakelijke niveau is. De resultaten van het rapport hebben we besproken in het beveiligingsberaad. De organisaties die patchmanagement nog niet op orde hebben, zijn aan zet om maatregelen nemen om invulling te geven aan het verbeteren. Dit zal worden besproken in de CIO-raad. Op het naleven van de afspraken zullen we toetsen.

ILT en RWS geven hieronder hun managementreactie op de bevindingen die betrekking op hun organisaties hebben.

ILT herkent zich in het beeld dat dit rapport schetst over het patchproces gezien vanuit ILT. Aangezien ILT in hoge mate afhankelijk is van de ketenpartners SSC en DICTU v.w.b. patching, hebben wij ten dele invloed op dit proces. E.e.a. zou wellicht beter kunnen worden vastgelegd in SLA's die we met die partijen hebben, maar in hoeverre SSC en DICTU dat ook willen/ kunnen/ doen is dan nog maar de vraag. ILT is een initiatief gestart om haar Hosting en Technisch Beheer mogelijk bij andere leveranciers onder te brengen. Dit zal betekenen dat het inrichten van de benodigde Applicatie Management processen binnen ILT, inclusief het patchmanagementproces, prominent onderdeel wordt van dat traject.

De CISO van RWS geeft het volgende aan: herken mij in deze conclusie.
RWS heeft de afgelopen jaren het generieke IenW patchproces overgenomen, uitgebreid en 'vertaald' naar de omgeving van RWS. Dat wil zeggen dat naast het patchproces op de kantoorautomatisering RWS geïnvesteerd heeft in het beleid van patchen voor de industriële automatisering in de objecten (tunnels, bruggen, sluizen, kering etc.)
Gelet RWS het beheer en onderhoud van deze objecten heeft uitbesteedt aan marktpartijen, zijn aanvullende eisen t.a.v. patchen in de (model)contracten opgenomen. Alle nieuw aangegane contracten bevatten deze eisen. Voor bestaande (lopende) contacten is geïnventariseerd bij welke contracten deze aanvullende eisen konden worden opgenomen. De financiële consequenties van het aanpassen van lopende contracten wordt meegenomen in de integrale afweging om de eisen alsnog contractueel op te laten nemen. Het is een kwestie van tijd dat alle (langlopende) contracten de nieuwe aanvullende eisen bevatten. In de tussentijd zet RWS verschillende instrumenten (o.a. Functionele Inspectie en Testen, monitoring op het Beveiligd Werken RWS, Systeemgerichte contractbeheersing en interne audits) in. Tot slot wil ik ook aangeven dat monitoring door het Security Operations Center op de objecten is geïntensiveerd naar aanleiding van het Algemene Rekenkamer rapport 'Cybersecurity Digitale dijkverzwaring'."

15 november 2019, hoofddirecteur FMC/CIO (opdrachtgever)