



> Retouradres Postbus 16292 2500 BG Den Haag

Ministerie van Infrastructuur en Waterstaat
t.a.v. de minister, de heer M.G.J. Harbers
Postbus 20904
2500 EX Den Haag

Adviescollege ICT-toetsing

Muzenstraat 95
Den Haag
Postbus 16292
2500 BG Den Haag
adviescollegeicttoetsing.nl

Contactpersoon

info@adviescollegeicttoetsing.nl

Kenmerk

2024-0000317167

Uw kenmerk

ILT-2023-10681

Datum 27 mei 2024
Betreft Definitief BIT-advies Onderhoud en Beheer Holmes

Geachte heer Harbers,

U heeft het Adviescollege ICT-toetsing verzocht een onderzoek uit te voeren naar het onderhoud en beheer van het zaakstelsel Holmes van de Inspectie Leefomgeving en Transport (ILT). De eigenaar van het zaakstelsel Holmes is de directeur Toezicht en Opsporing. Ons advies kan als volgt worden samengevat:

De inspecteurs van ILT gebruiken het systeem Holmes-Centraal ter ondersteuning van de uitvoering van haar toezicht- en opsporingstaken. Een deel van de inspecteurs gebruikt aanvullend de Holmes Onderweg App (HOA). Aan onderhoud en beheer van Holmes wordt ongeveer 4 miljoen euro per jaar besteed.

Conclusie

De belangrijkste conclusie uit de toets is dat Holmes de inspecteurs goed ondersteunt, maar dat zonder verbeteringen aan het onderhoud en beheer van Holmes het systeem zijn waarde voor ILT zal verliezen. Wij hebben het volgende geconstateerd:

- A. Holmes-Centraal biedt een waardevolle basis voor doorontwikkeling.
- B. De informatiebeveiliging schiet tekort.
- C. Regie op doorontwikkeling Holmes ontbreekt.

Advies

Om ervoor te zorgen dat Holmes waardevol blijft voor de uitvoering van toezicht en opsporing, adviseren wij de volgende maatregelen.

- 1. Verbeter de informatiebeveiliging.
- 2. Verbeter de regie op het onderhoud en beheer.

Hieronder vindt u eerst een korte beschrijving van het zaakstelsel Holmes. Daarna werken we bovenstaande conclusie en advies nader uit. In de bijlage vindt u de details van het zaakstelsel Holmes en over ons onderzoek.

KORTE OMSCHRIJVING VAN HOLMES

De Inspectie Leefomgeving en Transport (ILT) bestaat uit de dienst Omgeving en Dienstverlening, verantwoordelijk voor de uitgifte van vergunningen, en de dienst Toezicht en Opsporing, verantwoordelijk voor toezicht op het naleven van wet- en regelgeving door burgers en bedrijven. ILT richt zich op ongeveer 160

onderwerpen, waaronder geluidsoverlast in de luchtvaart, vaartijden in de binnenvaart, vervoer van gevaarlijke stoffen en energielabels van woningen. Voor de inspecties en voor haar opsporingstaken gebruikt de dienst het systeem Holmes sinds 2010. Holmes bestaat uit twee onderdelen: Holmes-Centraal (HC) en de Holmes-Onderweg app (HOA). In HC leggen circa 800 inspecteurs resultaten van inspecties en de daarbij horende vervolgacties vast. Dit is inclusief gegevens die mogelijk deel uit gaan maken of deel uitmaken van een strafdossier. Daarnaast wordt HC gebruikt voor het plannen van inspecties en worden documenten met betrekking tot inspecties opgesteld. HOA is een mobiele applicatie waarmee inspecteurs ter plaatse hun inspectieresultaten registreren en vastleggen, en gegevens uit bijvoorbeeld het handelsregister van de Kamer van Koophandel (KVK) ophalen. De vragenlijsten in HC en HOA worden los van elkaar onderhouden.

Het functioneel beheer van Holmes ligt bij ILT. Technisch beheer van HC is belegd bij DICTU, het applicatiebeheer van HC ligt bij ILT. Technisch en applicatiebeheer van HOA wordt extern uitgevoerd door softwareleverancier Capptions. HOA maakt gebruik van de Amazon Public Cloud om gegevens te verwerken voordat ze naar HC gestuurd worden.

De jaarlijkse kosten voor onderhoud en beheer van Holmes bedragen circa 4 miljoen euro.

CONCLUSIE: MET MEER AANDACHT KAN HOLMES NOG JAREN MEE

Holmes is een waardevol systeem voor ILT. Inspecteurs gebruiken HC en HOA om resultaten van inspecties en de daarbij behorende acties (bijvoorbeeld interventies en het opmaken van inspectierapporten) vast te leggen. HC is flexibel opgezet en kan met voldoende lifecyclemanagement nog jaren mee.

Wij zien wel tekortkomingen op het gebied van informatiebeveiliging en de regie op het onderhoud en beheer. Verbeteringen op deze punten zijn nodig om Holmes veilig te maken en de waarde voor ILT nu en in de toekomst te behouden.

A. Holmes-Centraal biedt een waardevolle basis voor doorontwikkeling

Het is van belang dat Holmes aanpasbaar is en ook in de toekomst kan voldoen aan veranderende eisen aan het toezicht die voortkomen uit veranderingen in regelgeving en de behoeften van ILT en haar omgeving. HOA is sinds 2023 in gebruik. Door het gebrek aan historische data over het beheer en aanpassingen kunnen we wat betreft HOA nog geen uitspraken doen over de geschiktheid voor doorontwikkeling. Wij denken dat de afgelopen jaren hebben laten zien dat HC aanpasbaar is en van voldoende kwaliteit is. Dit blijkt uit het volgende:

- HC is betrouwbaar en functioneel:
 - Er zijn de laatste jaren geen grote problemen opgetreden bij het gebruik van Holmes. De incidenten die gebruikers rapporteren, worden merendeels binnen de gestelde termijn opgelost.
 - Door de gekozen opzet van HC worden veel verschillende inspecties ondersteund. Zo kunnen de vragenlijsten voor de verschillende onderwerpen van inspectie per afdeling worden gemaakt.
- HC is onderhoudbaar gebleken:
 - Er is voldoende kennis bij het ILT-ontwikkelteam aanwezig om HC te onderhouden en door te ontwikkelen.
 - De broncode van HC is gestructureerd opgezet en leesbaar.

- De afgelopen jaren is het systeem succesvol aangepast aan nieuwe eisen, zoals bijvoorbeeld de aansluiting op het nieuwe Digitale Stelsel Omgevingswet of wijzigingen in de wet- en regelgeving van de ILT. Deze wijzigingen hebben na implementatie niet geleid tot incidenten. Ook de functionele wijzigingen, die worden doorgevoerd op verzoek van de product owner, leiden niet tot noemenswaardige incidenten.

B. De informatiebeveiliging schiet tekort

Ondanks dat Holmes een waardevolle basis biedt voor doorontwikkeling, zien wij een aantal risico's. ILT heeft geen inzicht in de risico's op het gebied van informatiebeveiliging en privacy in het gebruik en het beheer van Holmes. Daarbij valt op dat Rijkskaders, zoals de Baseline Informatiebeveiliging Overheid (BIO) en het Rijksbreed Cloudbeleid 2022, onvoldoende worden gerespecteerd. ILT heeft geen risicoanalyse van Holmes gemaakt om na te gaan welke informatiebeveiligingsrisico's er zijn en welke maatregelen getroffen zouden moeten worden. Holmes is op dit moment onveilig:

- Een urgent probleem is het ontbreken van noodzakelijke waarborgen voor gegevensbescherming in HOA ten behoeve van de verwerking van persoonsgegevens. ILT heeft hierover geen sluitende contractuele afspraken gemaakt met de leverancier. Zo ontbreekt een verwerkersovereenkomst die de Algemene verordening gegevensbescherming (AVG) voorschrijft.
- Er is te weinig aandacht voor de beveiliging van HC waardoor gegevens onvoldoende zijn beschermd.
- Er is geen ontwerp voor toegangsbeveiliging van gebruikers, noch voor HC noch voor HOA. Hierdoor kan niet worden vastgesteld of de software de toegangseisen van ILT voldoende afdwingt.
- Ontwikkelaars kunnen privacygevoelige productiegegevens inzien waarvoor ze geen toestemming hebben. Het intern ontwikkelde script om productiedata te anonimiseren is onvolledig. Bovendien wordt het script niet consequent aangepast bij wijzigingen.

C. Regie op doorontwikkeling Holmes ontbreekt

Het IG-team¹ heeft weinig aandacht voor de doorontwikkeling van Holmes waardoor het risico ontstaat dat Holmes over vijf jaar niet meer past bij de ambities van ILT. Dit blijkt uit het volgende:

- De directie Toezicht en Opsporing, die het grootste belang heeft bij een goed werkend Holmes, is onvoldoende betrokken bij de doorontwikkeling van Holmes om de regie te kunnen voeren:
 - Er is geen ontwikkelagenda voor Holmes waardoor de strategische doelstellingen van ILT niet vertaald worden naar functionele aanpassingen in Holmes. Dit gaat ten koste van het oplossen van bestaande bewerkelijke workarounds.
 - De directie Toezicht en Opsporing heeft weinig invloed op de ontwikkeling van systemen. Er zijn bijvoorbeeld meerdere systemen om inspecties te plannen en om documenten met inspectieresultaten te genereren, ondanks dat deze additionele functionaliteit ook aanwezig is in Holmes.
- ILT kijkt onvoldoende naar de impact van nieuwe aanpassingen, ondanks dat ILT hiervoor een verkenningsproces heeft. Tijdens dit proces worden

¹ De Inspecteur-Generaal en zijn vier directeuren.

alternatieve oplossingsrichtingen onvoldoende afgewogen en wordt de impact op onderhoud en beheer onvoldoende in beeld gebracht. We zien dat aan de volgende voorbeelden:

- In 2023 heeft ILT een analyse gemaakt hoe de HOA te implementeren. In deze analyse zijn geen alternatieven afgewogen, zoals een voor de hand liggend alternatief om de HC-schermen geschikt te maken voor een mobiel apparaat. Het gevolg hiervan is dat alle vragenlijsten zowel in HC als in HOA moeten worden aangemaakt en dat deze bij wijzigingen in wet- en regelgeving dus twee keer moeten worden aangepast.
- ILT ontwikkelt nieuwe koppelingen, bijvoorbeeld om bedrijfsgegevens van de KVK op te halen en daarmee te zorgen voor een eenduidige registratie. Echter, bestaande registraties (met een andere naamgeving) worden niet in lijn gebracht met de door de KVK vastgelegde naamgeving. Hierdoor worden de ambities voor datagestuurd inspecteren bemoeilijkt.
- Regie op de ontwikkelaanpak ontbreekt. Hierdoor ontstaan de volgende tekortkomingen:
 - Een architectuurbeschrijving ontbreekt, waardoor architectuurkeuzes door de ontwikkelaars gemaakt moeten worden. Dit heeft geresulteerd in technische schuld die lastig is op te lossen vanwege het ontbreken van documentatie en ontwerpen. Bovendien heeft dit geleid tot ontwikkelde functionaliteit die niet in gebruik genomen kon worden.
 - Ontwikkelaars beschikken over onvoldoende ontwikkelgereedschappen. Er is geen ontwikkelstraat waarmee het ontwikkelproces zoveel mogelijk wordt geautomatiseerd. Het testen, accepteren en het uitleveren van nieuwe versies moet handmatig uitgevoerd worden en is tijdrovend. Hierdoor is ILT weinig flexibel en afhankelijk van de beschikbaarheid van medewerkers van DICTU. Hersteltijd van fouten kan hierdoor oplopen tot meerdere dagen.
 - Monitoring van kosten, doorlooptijden (inclusief het oplossen van informatiebeveiligingsproblemen), datakwaliteit en resultaten van ontwikkeling vindt niet plaats. Monitoring is ook lastig doordat geconstateerde problemen en wijzigingsverzoeken niet consistent worden geregistreerd en bijgehouden in de beheersystemen.

ADVIES: ZORG DAT HOLMES ZIJN WAARDE BEHOUDT

Holmes is een applicatie waarmee de inspectie haar Toezicht en Opsporing in principe nog jaren kan ondersteunen. Om dit mogelijk te maken adviseren wij om de volgende verbeteringen in gang te zetten.

1. Verbeter de informatiebeveiliging

Het in orde maken van de informatiebeveiliging van Holmes moet een top prioriteit voor de ILT zijn. We adviseren ILT een verbeterplan te maken dat invulling geeft aan de volgende aanbevelingen:

- Los het urgente informatiebeveiligingsrisico van HOA zo spoedig mogelijk op. Is dat niet mogelijk, overweeg dan HOA (tijdelijk) uit te zetten:
 - Beoordeel voor eind juni 2024 welke maatregelen genomen moeten worden om verantwoord gebruik te blijven maken van HOA. Voer deze maatregelen voor eind september 2024 uit.
 - Plan direct daarna een penetratietest voor HOA en los de bevindingen met een hoog risico onmiddellijk op.

- Leg vast hoe aan de BIO wordt voldaan en maak een *data protection impact assessment*² voor Holmes, zowel voor HC als voor HOA. Dit maakt duidelijk welke maatregelen moeten worden genomen om persoonsgegevens te beschermen.
- Versterk de informatiebeveiligingsorganisatie:
 - Zorg voor structurele borging van informatiebeveiliging en privacy door in elk geval reguliere beveiligingschecks in het ontwikkelproces en in de ontwikkelstraat op te nemen en planmatig aan nieuwe en toekomstige richtlijnen, zoals de *Network and Information Security directive* (NIS2), te voldoen. Zorg er ook voor dat degene die hiervoor verantwoordelijk is incidenten zonder andere tussenkomst rapporteert aan de inspecteur-generaal.
 - Zorg dat iedere bij Holmes betrokken ICT-medewerker weet aan welke minimale eisen de beveiliging van Holmes moet voldoen.
 - Maak een overzicht van alle bekende beveiligingsproblemen, die door de directeur Toezicht en Opsporing moet worden gemonitord. Los deze beveiligingsproblemen op.
- Stel vast welke autorisatie- en authenticatie-eisen moeten gelden voor Holmes. Beoordeel daarna de huidige manier van autoriseren en authenticeren. Voer waar nodig aanpassingen door zodat het systeem aan de eisen voldoet. Zorg voor voldoende loginformatie en monitoring daarop.
- Laat de verantwoordelijke voor het verbeterplan maandelijks rapporteren aan de inspecteur-generaal over de voortgang van het verbeterplan tot de tekortkomingen zijn weggenomen.

2. Verbeter de regie op het onderhoud en beheer

Om ervoor te zorgen dat Holmes in de toekomst de toezicht- en opsporingstaken blijft ondersteunen en aansluit bij de strategische doelstellingen van ILT moet ILT de regie verstevigen:

- Beleg het opdrachtgeverschap en het inhoudelijk eigenaarschap voor Holmes bij de directeur Toezicht en Opsporing. Zorg dat de product owner een gemandateerd opdrachtgever is binnen die directie. Zorg dat de product owner bijgestaan wordt door iemand met voldoende ICT-kennis, om de balans tussen functionele en technische verbeteringen te bewaken.
- Stel een meerjarenvisie op voor Holmes, waarbij de activiteiten zijn afgestemd op de strategische agenda van ILT. Neem in deze meerjarenvisie in ieder geval mee:
 - de ambitie om datagestuurd te inspecteren;
 - een antwoord op de vraag hoe ILT om wil gaan met redundante functionaliteit van Holmes, die nu maar door een beperkte groep inspecteurs worden gebruikt (zoals het plannen van inspecties en het genereren van documenten).
- Beschrijf – in lijn met de meerjarenvisie – de doelarchitectuur van Holmes en neem hier in elk geval de doeltechnologieën en beveiligingseisen in mee. Beschrijf ook de stappen om de doelarchitectuur te bereiken vanuit die huidige architectuur.
- Verbeter de wijze waarop op dit moment de verkenning voor nieuwe functies wordt uitgevoerd. Geef daartoe meer aandacht aan verschillende oplossingsrichtingen. Weeg de consequenties op onderhoud en beheer, en de consequenties op informatiebeveiliging tegen elkaar af. Zorg dat wijzigingen

² Gegevensbeschermingseffectbeoordeling.

Datum
27 mei 2024

Kenmerk
2024-0000317167

worden afgestemd met DICTU, zodat wijzigingen passen binnen de grenzen van de infrastructuur die DICTU beheerd.

- Haal meer ICT-kennis op het gebied van softwareontwikkeling in huis, zodat ILT de ICT-risico's zelfstandig kan beoordelen
- Zorg voor een verbeterde doorontwikkeling door:
 - het inrichten van een efficiënte ontwikkelomgeving;
 - het verbeteren van het anonimiseren van productiedata; overweeg hierbij gebruik te maken van DICTU-gereedschap dat hiervoor is;
 - gebruik te maken van een afdoende geautomatiseerde regressietest;
 - het documenteren van ontwerpbeslissingen;
 - het monitoren van de voortgang van ontwikkeling, waarbij een consistente registratie van geconstateerde problemen en wijzigingsverzoeken noodzakelijk is.

Tot slot danken wij alle geïnterviewden voor hun medewerking en openheid. Wij hopen dat wij met dit advies een bijdrage kunnen leveren aan succesvolle inzet van Holmes, nu en in de toekomst.

Met de meeste hoogachting,
namens het Adviescollege ICT-toetsing,

w.g.

drs. H.J.A. van Osch
Voorzitter

w.g.

drs. S.J. van Amerongen
Secretaris-directeur

Bijlage

Informatie over de organisatie ILT en zaakstelsel Holmes die beoordeeld zijn in dit onderzoek.

Nr	Onderwerp	Toelichting
1.	Organisatie	Inspectie Leefomgeving en Transport (ILT)
2.	Maatschappelijke/beleidsdoelstelling	De Inspectie Leefomgeving en Transport (ILT) werkt aan maatschappelijk effect: het beperken van maatschappelijke schade (fysiek, gezondheid, milieu en economisch).
3.	Omvang organisatie	1600 medewerkers, waarvan 800 inspecteurs
4.	Informatiesystemen	<p>Holmes bestaat uit twee onderdelen:</p> <p>Holmes Centraal (HC) HC is bedoeld om de uitgevoerde inspectiewerkzaamheden op een gestructureerde, eenduidige en achteraf controleerbare wijze te documenteren (registratie). HC kan waar en wanneer nodig ingezet worden om verantwoording over de uitgevoerde werkzaamheden af te leggen (verantwoording). Daarnaast dient HC voor het analyseren van uitgevoerde inspecties en daarmee van het beeld van de naleving en van de maatschappelijke veiligheidsrisico's. Tot slot wordt informatie/data in HC gebruikt om afdelings- en organisatie doelstellingen alsmede werkprocessen verder aan te scherpen (sturing). HC is een webapplicatie. De inkomende en uitgaande documenten worden opgeslagen in Alfresco en zijn alleen bereikbaar via HC. Gegevens worden opgeslagen in een MS SQL database</p> <p>Holmes Onderweg applicatie (HOA) De HOA wordt gebruikt voor een aantal Inspectieonderwerpen op locatie waarbij basisgegevens (over het te controleren object, bedrijf of persoon) kunnen worden opgehaald en gegevens van een inspectie worden ingevoerd.</p>
5.	Opdrachtgever(s)/Eigenaar	Directeur Toezicht en Opsporing
6.	Housing en hosting	DICTU: Hosting en technisch applicatie-beheer HC met MS SQL server en Alfresco
7.	Applicatieonderhoud	ILT: HC DICTU: MS SQL, Alfresco Capptions: HOA ILT: Functioneel beheer HC, Alfresco, HOA
8.	Jaarlijks exploitatiebudget voor onderhoud en beheer	Circa 4 miljoen euro per jaar voor Holmes en HOA inclusief de diensten van DICTU en Capptions
9.	Omvang applicaties	HC: 2.400 FP in 2019 (de functies van HOA zijn hierin meegenomen, net als de functies van Alfresco)
10.	Huidige technologie/architectuur	HC:

Datum
27 mei 2024

Kenmerk
2024-0000317167

Nr	Onderwerp	Toelichting
		<ul style="list-style-type: none"> - Java / Spring op JBoss EAP, MS SQL server database; Angular gebruikersschermen - Productie: JBoss EAP domain op twee servers, MS SQL server cluster, Alfresco: Onbekend <p>HOA:</p> <ul style="list-style-type: none"> - Amazon public cloud, pakket van Capptions <p>Axway voor gegevenskoppelingen intern en extern</p> <p>Beheersystemen Jira en Topdesk voor onder andere bevindingenregistratie</p>
11.	Doeltechnologie/-architectuur	Niet aanwezig
12.	Gebruikte kaders voor beheerprocessen	Er wordt agile gewerkt. Er zijn geen kaders gesteld aan de beheerprocessen
13.	Leeftijd/Jaar ingebruikname systemen en lifecyclestatus	HC: in gebruik sinds 2010 HOA: in gebruik sinds 2022
14.	Financiering	Vanuit jaarlijkse exploitatiebudget voor ICT van ILT
15.	Gebruikers/afnemers	HC: circa 800 gebruikers (merendeels inspecteurs) HOA: circa 200 inspecteurs

Informatie over het uitgevoerde onderzoek

Nr	Onderwerp	Toelichting
1.	Type onderzoek	Beheer en Onderhoud; conform artikel 2, lid 2 sub a2 Instellingsbesluit Adviescollege ICT-toetsing
2.	Aanmelddatum	29-09-2023
3.	Start onderzoek	11-01-2024
4.	Afronden onderzoek	10-04-2024
5.	Datum concept advies	29-04-2024
6.	Datum definitief advies	27-05-2024
7.	Eerder onderzoek	Niet van toepassing
8.	Onderzoeksmethode	Themasessies, interviews, documentstudie, analyse administraties en GIT