Auditdienst Rijk
Ministerie van Financiën

departementaal VERTROUWELIJK

Quick scan SFTP koppelvlak CIMS

Opdrachtbevestiging

Versie	1.0
Datum	27 januari 2021
Status	Definitief

Volgende pagina verwijderd ivm blanco.

Colofon

Titel	Quick scan SFTP koppelvlak CIMS
Auteur(s)	5.1.2e
Bijlagen	1
Kenmerk	2021-0000016890
Inlichtingen	**Auditdienst Rijk** 5.1.2e 5.1.2e @minfin.nl

Volgende pagina verwijderd ivm blanco.

Inhoud

Volgende pagina verwijderd ivm blanco.

1 Inleiding

1.1 Aanleiding

Onder meer het ministerie van VWS en het RIVM zijn momenteel druk bezig met de voorbereiding van de COVID-19 vaccinatie voor de Nederlandse samenleving. In de Kamerbrief vaccinatiestrategie COVID-19[1] wordt registratie van vaccinatiegegevens als onderdeel van de uitvoering van de vaccinatie gezien. In dit kader heeft het RIVM een landelijk register opgezet, aangeduid als CIMS: Covidvaccinatie Informatie- en Monitoring Systeem.

RIVM heeft ADR medegedeeld dat de volgende uitgangspunten voor de vaccinatieregistratie worden gehanteerd:

1. Registratie aan de bron. De bron is het informatiesysteem van de uitvoerder die de prik zet.
2. De uitvoerder die de prik zet is verantwoordelijk voor juistheid en compleetheid van de registratie aan de bron, en voor tijdig aanleveren van de gegevens aan RIVM.
3. VWS maakt met de uitvoerders afspraken waarin verwerking door RIVM wordt toegestaan.
4. Bestanden met vaccinatiegegevens worden geautomatiseerd geproduceerd in de applicatie van de uitvoerder waarin de vaccinatie is vastgelegd en worden zonder handmatig ingrijpen (geautomatiseerd) verzonden naar CIMS van het RIVM conform de hiervoor aangeleverde specificaties.

Ten aanzien van punt 4 wordt opgemerkt dat vaccinatiegegevens door betrokken partijen (GGD'en, huisartsen en verpleegtehuizen en gehandicaptenzorg) op verschillende manieren kunnen worden aangeleverd bij RIVM ten behoeve van opname in CIMS. Een van de manieren is het aanbieden op het SFTP koppelvlak van CIMS. Verwachting is dat dit koppelvlak met name voor aanlevering van vaccinatiegegevens door verpleegtehuizen en gehandicaptenzorg zal worden gebruikt. Er worden circa 50 tot 60 gebruikers verwacht in de vorm van IT-leveranciers van verpleegtehuizen en gehandicaptenzorg.

1.2 Context

Met als doel CIMS snel in te kunnen richten heeft RIVM besloten om een kopie van Praeventis, een bestaand vaccinatie registratiesysteem, te maken. Het SFTP koppelvlak maakt hier onderdeel van uit. In technische zin betreft het een gevirtualiseerde server die is ingericht op basis van Red Hat Enterprise Linux. Deze virtuele server draait op een hypervisor (VMWare) die is geplaatst in het datacenter van RIVM. Het beheer van deze server vindt plaatst door SSC Campus, de ICT-organisatie van RIVM en KNMI.

---

1 https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2020/09/23/kamerbrief-vaccinatiestrategie-covid-19/kamerbrief-vaccinatiestrategie-covid-19.pdf

Op 15 december 2020 heeft een overleg plaatsgevonden tussen de betrokken programmamanager van VWS, NCSC en ADR. In dit overleg heeft de programmamanager ADR verzocht om een quick scan uit te voeren op het SFTP koppelvlak van het CIMS systeem, gericht op het aspect vertrouwelijkheid. Redenen die door RIVM hiervoor genoemd zijn:

- De op het SFTP koppelvlak aangeleverde data heeft een medisch vertrouwelijk karakter. In potentie betreft het een aanzienlijk deel van de Nederlandse bevolking waarvan vaccinatiegegevens worden aangeleverd op dit koppelvlak.
- De grote maatschappelijke impact van het COVID-19 vaccinatie traject.
- Het SFTP koppelvlak is de component van het CIMS systeem die benaderbaar is vanaf het internet (beschermd door een firewall).

2 Opdracht

2.1 Opdrachtgever en opdrachtnemer

Deze opdracht wordt door de Auditdienst Rijk (ADR) uitgevoerd in opdracht van de hee[5.1.2e].
Opdrachtnemer namens de ADR is de Accountdirecteur ADR voor OCW, SZW en VWS, de heer d[5.1.2e]

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

2.2 Doelstelling en onderzoeksvragen

De doelstelling van het onderzoek is om inzicht te geven in bevindingen ten aanzien van het kwaliteitsaspect 'vertrouwelijkheid' voor het koppelvlak CIMS op basis van SFTP door binnen beperkte tijd antwoord te geven op de volgende vragen:

1. Hoe is het koppelvlak CIMS op basis van SFTP op bij RIVM ingericht?
2. Welke bevindingen heeft ADR ten aanzien van de getroffen maatregelen voor het waarborgen van de vertrouwelijkheid van de vaccinatiedata die via het SFTP koppelvlak aan RIVM wordt aangeboden?

Bovenstaande vragen zullen worden beantwoord middels het uitvoeren van een quick scan. Voor de beantwoording van onderzoeksvraag twee wordt een tweesporen aanpak gehanteerd:

- onderzoek op basis van interviews, documentatie en kennisname van de configuratie van de server die voorziet in het SFTP koppelvlak (SFTP server);
- onderzoek middels de inzet van technische tooling waarmee het bestaan (de aanwezigheid) van beveiligingsmaatregelen kan worden vastgesteld (pentestwerkzaamheden).

Op verzoek van opdrachtgever wordt ook voorzien in een test van verbeteringen (verder: hertest) die RIVM realiseert naar aanleiding van bevindingen uit onderzoeksvraag twee.

In paragraaf 2.3 is de gedetailleerde beschrijving opgenomen van het object van onderzoek, afbakening en definities. In paragraaf 2.4 is het door ons gehanteerde referentiekader opgenomen.

2.3 Object van onderzoek, afbakening en definities

Het object van onderzoek is de CIMS SFTP server die door RIVM kan worden gebruikt voor ontvangst van detailinformatie over vaccinatie met verschillende COVID-19 vaccins van personen in Nederland aangeleverd door GGD-en, huisartsen, verpleegtehuizen en gehandicaptenzorg. De SFTP server heeft als DNS naam 'sftp.cims.rivm.nl' met IP adres 131.224.244.212. Het betreft een gevirtualiseerde Linux server waarop een SSH service draait die voorziet in de SFTP functionaliteit.

Belangrijke kwaliteitscriteria zijn in dit geval (in lijn met het VIR 2007) vertrouwelijkheid, integriteit en beschikbaarheid. Het criterium vertrouwelijkheid valt op verzoek van opdrachtgever binnen de scope van het onderzoek. De criteria integriteit en beschikbaarheid maken geen deel uit van het onderzoek. In het geval dat ADR gedurende het onderzoek bevindingen heeft die direct de integriteit of beschikbaarheid van data die via de SFTP server aan het RIVM ter beschikking wordt gesteld betreft, dan worden deze bevindingen wel gemeld.

Op meer detailniveau vallen de volgende onderwerpen in scope van het onderzoek:
- de (gevirtualiseerde) server waarop de SFTP server software draait (Red Hat Enterprise Linux);
- de SFTP server software op de server;
- de directe netwerkomgeving van de SFTP server. Specifiek wordt onderzoek gedaan naar het netwerkpad vanaf internet naar de SFTP server toe en van de SFTP server naar het interne netwerk;
- beheeronderwerpen die direct van het grootste belang zijn voor de vertrouwelijkheid van (de data op) de SFTP server: logische toegangsbeveiliging, logging- en monitoring en patch management.

Alle andere onderwerpen zijn buiten scope voor het onderzoek. Specifieke voorbeelden zijn:
- De virtualisatielaag waarop de SFTP server draait.
- Beheerprocessen (bij RIVM en leveranciers) voor zover niet in scope, zoals b.v. wijzigingenbeheer (inrichting van de SFTP server verkeert momenteel nog in de projectfase)

De hertest zal zich uitsluitend richten op de oorspronkelijke bevindingen die voortkomen uit de beantwoording van vraag 2. Het onderzoek heeft verder het karakter van een quick scan. Dit betekent dat het onderzoek wordt afgebakend in tijd en dat indien nodig onderzoekswerkzaamheden niet of met minder diepgang worden uitgevoerd om binnen de beschikbare tijd tot een afronding te komen. Indien nodig zal hierover tussentijds overleg met de contactpersoon bij de opdrachtgever plaatsvinden.

2.4 Referentiekader

Voor de beantwoording van onderzoeksvraag twee wordt in het kader van deze quick scan een beperkt referentiekader gehanteerd dat in deze paragraaf wordt beschreven. Voor onderzoek van configuratie en documentatie wordt een selectie uit het DigiD assessment kader (Norm ICT-beveiligingsassessments DigiD versie 2.0) gehanteerd[2]. Daar waar in het DigiD assessment kader wordt gesproken over webapplicatie of webserver wordt in deze context de SFTP server bedoeld.
De selectie is gemaakt op basis van de op dit moment actuele versie van het DigiD normenkader en op basis van de afbakening die geldt voor deze opdracht:

U/TV.01	De inzet van identiteit- en toegangsmiddelen levert betrouwbare en effectieve mechanismen voor het vastleggen en vaststellen van de identiteit van gebruikers, het toekennen van de rechten aan gebruikers,

[2] *Dit kader is op zijn beurt weer gebaseerd op de 'ICT-beveiligingsrichtlijnen voor webapplicaties' d.d. 1 september 2015 zoals gepubliceerd door het NCSC. Hierin zijn ook referentiecodes als U/TV.01 terug te vinden.*

	het controleerbaar maken van het gebruik van deze middelen en het automatiseren van arbeidsintensieve taken.
U/WA.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken. (privacy uitsluiten)
U/PW.03	De webserver is ingericht volgens een configuratie-baseline.
U/PW.05	Het beheer van platformen maakt gebruik van veilige (communicatie)protocollen voor het ontsluiten van beheermechanismen en wordt uitgevoerd conform het operationeel beleid voor platformen.
U/PW.07	Voor het configureren van platformen is een hardeningsrichtlijn beschikbaar.
U/NW.03	Het netwerk is gescheiden in fysieke en logische domeinen (zones), in het bijzonder is er een DMZ die tussen het interne netwerk en het internet gepositioneerd is.
U/NW.04	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen.
U/NW.05	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.
C.03	Vulnerability assessments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT componenten van de webapplicatie (scope).
C.04	Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope).
C.06	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.
C.07	De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICT systemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en de bevindingen gerapporteerd.
C.09	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen.

Voor de inzet van gespecialiseerde software voor het testen van de beveiliging (pentestwerkzaamheden) wordt geen expliciet normenkader gehanteerd, zie ook de volgende paragraaf 'Aanpak technische testen'. Een aantal breed in de markt gebruikte tools wordt ingezet. Hiermee heeft ADR goede ervaring. Deze tools zijn relevant voor het object van onderzoek en bevatten uitgebreide informatie over kwetsbaarheiden en te treffen beveiligingsmaatregelen.

2.5 Aanpak technische testen

Wij zullen door middel van geautomatiseerde en handmatige testen onderzoeken of het mogelijk is de functionaliteit van de SFTP server te misbruiken of binnen te dringen. De aanwezigheid van de beveiligingsmaatregelen wordt getest met behulp van gespecialiseerde software.

De belangrijkste onderwerpen die tijdens de (geautomatiseerde) testen aan de orde komen zijn:

- Bestands- en directory toegang. De op de server aanwezige bestanden bieden aanvallers mogelijk extra informatie om de server aan te vallen. Dit geldt zowel voor bestanden die alleen informatie bevatten als voor programma's voor test- of beheerdoeleinden. Tijdens de test wordt gezocht naar veel voorkomende bestanden en directories.
- Component afhankelijke kwetsbaarheden. Een SFTP server maakt veelal gebruik van verschillende componenten. Het bekend worden van kwetsbaarheden in deze componenten kan ertoe leiden dat de beveiliging van de server of data in het geding is. Tijdens de test worden bekende kwetsbaarheden getest op de verschillende componenten van de SFTP server.
- Beveiligingsmechanisme. De SFTP server kan gebruik maken van een beveiligingsmechanisme als vertrouwelijke en/of persoonlijke gegevens kunnen worden ingevoerd of geraadpleegd. De sterkte van dit mechanisme bepaalt voor een groot gedeelte het beveiligingsniveau van de SFTP server en data. Tijdens de test wordt onderzocht of een adequaat beveiligingsmechanisme is toegepast, of mogelijkheden aanwezig zijn om de beveiliging te omzeilen of om kwetsbaarheden van een gebruikt beveiligingsmechanisme aan te tonen.
- Beveiliging gegevenstransport. De verbinding met de SFTP server wordt vaak afgeschermd door middel van bijvoorbeeld gebruik van een public/private key zodat vertrouwelijke gegevens niet door derden kunnen worden onderschept. Het type en de configuratie van de toegepaste cryptografie bepalen voor een belangrijk gedeelte het beveiligingsniveau van de communicatie tussen gebruiker en de SFTP server.

De testwerkzaamheden zullen vanuit het technisch lab van de ADR-locatie in het ministerie van Financiën in Den Haag[3] worden uitgevoerd en zijn opgebouwd uit de volgende drie fasen.

Fase 1 - bestaat uit een verkenning van de SFTP server en de daarbinnen gebruikte technieken. De functionaliteit van de SFTP server wordt met een reguliere SFTP-client verkend waarbij ADR ook de beschikking krijgt over twee testaccounts. Daarnaast wordt middels openbare bronnen een beeld verkregen van de gebruikte technieken (passieve informatievergaring), zoals het type serverplatform en softwareversies.
Op basis van de bevindingen worden onze testprogramma's geconfigureerd, die worden gebruikt in fase 2.

Fase 2 - bestaat uit het (geautomatiseerd) testen van de SFTP server. Deze wordt handmatig en met behulp van onze testprogramma's gescand op kwetsbaarheden.

Fase 3 - is een analyse van de resultaten die onze testprogramma's hebben opgeleverd en mogelijke daarop gebaseerde vervolgacties. Het is mogelijk dat tests zogenaamde foutpositieven opleveren waarbij het lijkt dat een risico aanwezig is, terwijl dit in feite niet het geval is. Om foutpositieven zoveel mogelijk uit te sluiten, worden alle resultaten handmatig onderzocht.

[3] Via een remote desktop oplossing vanwege COVID-19 thuiswerkregels.

Het is niet de bedoeling om een Denial of Service (DoS) aanval te simuleren, het is echter mogelijk dat de server(s) door sommige tests performance problemen ondervinden. Om dit zoveel mogelijk te voorkomen zullen wij in contact staan met de verantwoordelijke beheerder(s) voor en tijdens de uitvoering.

2.6 Rapportage

Het eindproduct van deze opdracht is een onderzoeksrapport waarin de uitkomsten van de oorspronkelijk onderzoekswerkzaamheden en de hertest worden beschreven. Met dit rapport wordt geen zekerheid verschaft, omdat geen assurance-werkzaamheden worden uitgevoerd. Het rapport bevat daarom geen samenvattende conclusie of eindoordeel.

De opdrachtgever, de heer 5.1.2e , is eigenaar van de rapportage.

De ADR is de interne auditdienst van het Rijk. Het rapport over dit onderzoek 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 Uitvoering opdracht

3.1 Planning en werkzaamheden

De werkzaamheden voor dit onderzoek zijn grotendeels al in de tweede helft van december uitgevoerd als onderdeel van het vooronderzoek. Deze werkzaamheden bestonden uit:

- interviews met verantwoordelijk management en beheerders van de SFTP server gecombineerd met inzage in configuratie van SFTP server en bijbehorende netwerkomgeving;
- het testen van de beveiliging van de SFTP server middels gespecialiseerde software;
- analyse van de ontvangen en verzamelde informatie;
- communiceren concept bevindingen met RIVM.

In januari/februari 2021 worden de hertest werkzaamheden uitgevoerd in overleg met RIVM. Hierbij worden beknopt de in december uitgevoerde werkzaamheden herhaald, voor zover nodig voor herbeoordeling van de oorspronkelijke bevindingen. Daarna zullen wij zoals gebruikelijk:

- een concept rapportage opstellen;
- de concept rapportage afstemmen met betrokkenen;
- de rapportage als definitief uitbrengen;
- een beknopte opdrachtevaluatie uitvoeren.

3.2 Teamsamenstelling

Namens de ADR berust de verantwoordelijkheid voor deze opdracht bij de projectleider, de hee 5.1.2e die ook als contactpersoon zal fungeren. De ADR stelt ten behoeve van de uitvoering van dit onderzoek IT-auditors met voldoende kennis, ervaring en vaardigheden beschikbaar. Het onderzoeksteam bestaat uit de heer 5.1.2e en 5.1.2e . Waar nodig zullen ook andere collegae worden ingezet. Dit hangt nauw samen met de daadwerkelijke momenten van de uitvoering van de testen. De interne opdrachtgerichte kwaliteitsbeoordeling zal worden uitgevoerd door 5.1.2e 5.1.2e

3.3 Afspraken met de opdrachtgever

De hieronder opgenomen voorwaarden dragen bij aan een goed verloop en tijdige afronding van het onderzoek:

- tijdige ondertekening van opdracht en vrijwaringsverklaring; ook met derde partijen (in het kader van het vooronderzoek is de vrijwaringsverklaring al ondertekend);
- tijdige ontvangst van benodigde informatie;
- het tijdig toegang verschaffen tot de te testen applicatie(s) door middel van whitelisting en testaccounts, wanneer nodig voor het kunnen uitvoeren van de test;
- het informeren door de contactpersoon dan wel opdrachtgever van de betrokken functionarissen en eventuele derde partijen voordat de testen van start gaan;
- aanwezigheid en bereikbaarheid van beheerders tijdens de uitvoering van de testwerkzaamheden;

- de medewerking van betrokken functionarissen en eventuele derde partijen voor tijdige afstemming van de bevindingen en conceptrapportage;
- maken van back-up's van de SFTP server voor zover dit al niet regulier gebeurt en noodzakelijk is;
- Reactie op concept rapport dient binnen 14 dagen plaats te vinden. Na deze periode wordt het rapport definitief uitgebracht.

De opdrachtgever is verantwoordelijk voor bovenstaande voorwaarden en zorgt dat het onderzoek bekend gemaakt wordt bij de desbetreffende dienst-, organisatieonderdelen en onderaannemers/leveranciers.

3.4 Dossiervorming en geheimhouding

Deze opdracht wordt uitgevoerd in overeenstemming met de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing (IIA) (zie ook bij 2.1), het ADR Audit Charter (d.d. 17 april 2019, zie bijlage I) en conform de overige bij de ADR geldende kwaliteitsrichtlijnen. In het elektronische dossier van de ADR wordt alle evidence van het onderzoek opgenomen.

Bij de uitvoering van de opdracht is voor de medewerkers van de ADR het Reglement Gedragscode voor IT-auditors van NOREA van toepassing. Het Reglement Gedragscode schrijft onder andere voor dat verkregen vertrouwelijke gegevens alleen voor de vervulling van de opdracht mogen worden gebruikt.

4 Ondertekening

Ondergetekenden zijn deze opdracht overeengekomen en stemmen in met de inhoud van deze opdrachtbevestiging.

5.1.2e	5.1.2e
(Opdrachtgever)	*(Projectleider)*
~~.. januari 2021~~ 09/02/2021	27 januari 2021

5 Bijlage(n)

Volgende pagina verwijderd ivm blanco.