Auditdienst Rijk
Ministerie van Financiën

DEPARTEMENTAAL **VERTROUWELIJK**

Onderzoeksrapport Uitkomsten quick scan SFTP koppelvlak CIMS

Versie 1.0

Datum	18 maart 2021
Status	Definitief

Colofon

Titel	Onderzoeksrapport Uitkomsten quick scan SFTP koppelvlak CIMS
Auteur(s)	5.1.2e
Kenmerk	5.1.2e
Bijlagen	
Inlichtingen	**Auditdienst Rijk** 5.1.2e 5.1.2e @minfin.nl

Inhoud

Managementsamenvatting

Op verzoek van de Directeur-Generaal RIVM heeft Auditdienst Rijk (ADR) onderzoek gedaan naar het SFTP koppelvlak van CIMS (Covidvaccinatie Informatie- en Monitoring Systeem). Het onderzoek heeft zich met name gericht op het kwaliteitsaspect vertrouwelijkheid voor dit koppelvlak. Dit koppelvlak is een van de mogelijke manieren voor verschillende partijen om vaccinatiegegevens van Nederlandse burgers aan te leveren bij RIVM. Op basis van inzet van audittools en enkele interviews heeft ADR het onderzoek uitgevoerd in de vorm van een 'quick scan'. Dit heeft in de eerste ronde eind december 2020 geleid tot circa 15 bevindingen. Voor zover wij in de beperkte tijd die beschikbaar was hebben kunnen onderzoeken, leiden deze bevindingen niet direct tot toegang tot vaccinatiedata die wordt aangeleverd op de SFTP server. Wel brengen deze belangrijke beveiligingsrisico's met zich mee. Voorbeelden van bevindingen zijn:

1. Naast de primaire functie – het ontvangen van vaccinatiegegevens – wordt de SFTP server ook gebruikt als archief voor de aangeleverde databestanden. Aangezien deze SFTP server benaderbaar is vanaf internet, kan een enkel beveiligingslek op deze server een aanvaller ongeautoriseerd toegang geven tot vaccinatiedata van een langere periode.
2. Logging en monitoring is nog niet ingericht voor CIMS waardoor effectieve signalering van mogelijk misbruik nog niet kan plaatsvinden.
3. De SFTP server bevat oude configuratie aangezien CIMS een directe kopie is van een bestaand systeem van RIVM. Oude configuratie verhoogt de kans op bijvoorbeeld onbedoelde functionaliteit en menselijke fouten. Daarnaast verhoogt dit ook het aanvalsoppervlak.

Voor deze bevindingen zijn aanbevelingen geformuleerd, bijvoorbeeld om de SFTP server van de grond af opnieuw op te bouwen.

Begin februari heeft RIVM aangegeven een aantal verbeteringen te hebben gerealiseerd, mede op basis van de aanbevelingen van ADR. Belangrijkste verbetering is dat RIVM een nieuwe SFTP server heeft ingericht die voor de oude SFTP server is geplaatst. Voor deze oplossing is gekozen aangezien CIMS momenteel in productie is genomen en RIVM verbeteringen wil doorvoeren met zo min mogelijk kans op verstoringen. Op verzoek van RIVM heeft ADR een hertest uitgevoerd op die punten waarvan is aangegeven dat verbetering is gerealiseerd. Uit de hertest komt het beeld dat een aantal punten inderdaad is verbeterd, al levert een oplossing in enige mate ook weer een nieuw beveiligingsvraagstuk op.

De concept bevindingen van de hertest zijn besproken tussen RIVM en ADR. De bevindingen werden hierbij herkend door RIVM. Een gedeeld beeld is dat om alle bevindingen op te lossen een herontwerp van de hele keten van aanbieder van vaccinatiedata tot RIVM zou moeten worden onderzocht en gerealiseerd. Hierbij zou dan bijvoorbeeld end-to-end encryptie van vaccinatiedata kunnen worden toegepast.

1 Onderzoeksvraag 1: SFTP Koppelvlak CIMS in beeld

In deze paragraaf wordt de eerste onderzoeksvraag beantwoord: 'Hoe is het koppelvlak CIMS op basis van SFTP op hoofdlijnen ingericht?'. Hiertoe wordt in paragraaf 1.1.1 de oorspronkelijk onderzochte situatie beschreven in december 2020 en in paragraaf 1.1.2 de situatie ten tijde van het follow-up onderzoek naar de stand van 3 februari 2021.

1.1 Systeembeschrijving koppelvlak op hoofdlijnen – december 2020

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 vaccinatieregister opgezet, aangeduid als CIMS: Covidvaccinatie informatie- en Monitoring Systeem. CIMS is een kopie van een bestaand vaccinatieregistratiesysteem dat RIVM al een aantal jaar in gebruik heeft.

Op hoofdlijnen bestaat CIMS uit een database en bijbehorende programmatuur die in het interne netwerk van RIVM is geplaatst. Hierin wordt de relevante vaccinatiedata verzameld. Deze database wordt gevoed uit een aantal informatiebronnen[2], met name de informatiesystemen van de uitvoerders die het Covid-19 vaccin toedienen. Hierbij geldt als uitgangspunt dat de uitvoerder die de prik zet voor vaccinatie verantwoordelijk is voor de juistheid en de compleetheid van de registratie aan de bron en voor het tijdig aanleveren van de gegevens. Tevens wordt een subset van gegevens uit de Basisregistratie Personen (BRP) aangeleverd ten behoeve van CIMS.

Overdracht van vaccinatiedata uit informatiesystemen van uitvoerders naar CIMS kan op een aantal manieren plaatsvinden, bijvoorbeeld via het Landelijk Schakelpunt (LSP). RIVM heeft een voorkeur voor gebruik van besloten netwerken voor informatie-uitwisseling. Voor redenen die buiten de scope van dit onderzoek liggen is er ook voorzien in een optie om via internet data aan te leveren op een SFTP server als koppelvlak. Ons is medegedeeld dat RIVM verwacht dat deze optie met name zal worden gebruikt door de verpleegtehuizen en de gehandicaptenzorg. Dit betreft een relatief kleine stroom vaccinatie informatie. De eerdergenoemde informatie uit BRP wordt ook op deze server aangeleverd.

De CIMS SFTP server (verder: de server) is in technische zin een directe kopie van de betreffende component in het bestaande vaccinatieregistratiesysteem van RIVM. Het betreft een gevirtualiseerde Linux server (RHEL 7.8) waarop een secure shell daemon (verder: SSH daemon) draait. Deze SSH daemon verzorgt zowel de SFTP functionaliteit als beheertoegang tot de server. De configuratie van de server is op een aantal plaatsen aangepast aangezien de broncomponent van het oorspronkelijke vaccinatieregistratiesysteem meer functionaliteit bood dan benodigd voor CIMS.

---

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

2 DPV_161 Koppelingen CIMS t.b.v. covidvaccinatiegegevens d.d. 14 december 2020

In de configuratie zijn hier nog wel sporen van te zien. De server is geplaatst in een semi-vertrouwde zone (DMZ) aan de rand van het RIVM netwerk achter een load-balancer/firewall. Aanlevering van vaccinatiegegevens via SFTP vindt plaats middels CSV-bestanden conform door RIVM aangeleverde specificaties, welke uitgaat van een bestaand berichttype van de Jeuggezondheidszorg (JGZ).

Gebruik van de server is op hoofdlijnen als volgt:

1. Een externe gebruiker (b.v. IT-leverancier van verpleegtehuis) komt met behulp van een SFTP client programma binnen op de firewall/loadbalancer op poort 22 en wordt doorgezet naar poort 22 op de SFTP server. Hiervoor moet het IP adres van de externe gebruiker gewhitelist zijn op de firewall.
2. De gebruiker authenticeert zich middels een public/private keypair. Wachtwoord authenticatie is bij uitzondering ook mogelijk, maar het is de bedoeling dat dit alleen gebeurt als de SFTP server via een besloten netwerk wordt benaderd.
3. De gebruiker plaatst een CSV bestand in een gedeelde directory.
4. Een 'smartmove' script verplaatst het geüploade bestand vervolgens naar een andere directory, van waaruit het wordt ingelezen door de vaccinatiedatabase.
5. Het bestand wordt gearchiveerd op de SFTP server.

1.2 Systeembeschrijving koppelvlak op hoofdlijnen – na aanpassing (februari 2021)

Op 3 februari 2021 heeft RIVM de wijzigingen toegelicht die zij heeft aangebracht naar aanleiding van onder meer de bevindingen van ADR van eind december 2020. RIVM geeft hierbij aan dat de continuïteit van CIMS momenteel erg belangrijk is. Introductie van nieuwe workflows of aangepaste werkwijzen, zou al teveel risico met zich mee brengen, gezien de leeftijd van (en de ervaring met) de bestaande verouderde scripts ten behoeve van het binnenhalen van de vaccinatiedata. Verbeteringen zijn daarom gerealiseerd met als randvoorwaarde dat workflows en werkwijzen niet kunnen worden aangepast.

De belangrijkste wijziging is de inrichting van een nieuwe front-end SFTP server die de ontvangst van vaccinatiedata afhandelt en vervolgens doorgeeft aan de oorspronkelijke SFTP server (nu back-end server). Op de front-end server zijn nu twee SSH daemons aanwezig. Een (op de reguliere poort 22) voor beheertoegang en een op poort 2222 voor het aanbieden van SFTP functionaliteit. Overdracht van front-end naar back-end server vindt plaats via een NFS share van een NAS die in beide servers beschikbaar is gemaakt. Front-end en back-end server bevinden zich in hetzelfde VLAN in de DMZ van het RIVM netwerk. Verder geeft RIVM aan dat:

- voor NFS gebruik wordt gemaakt van IP access lists;
- de NAS voor beheer alleen vanuit een beheer-lan is te benaderen.

Gebruik van de front-end en back-end server is nu op hoofdlijnen als volgt:

1. Een externe gebruiker (b.v. IT-leverancier van verpleegtehuis) komt met behulp van een SFTP client programma binnen op de firewall/loadbalancer op poort 22 en wordt doorgezet naar poort 2222 op de front-end server. Hiervoor moet het IP adres van de externe gebruiker gewhitelist zijn op de firewall.
2. De gebruiker authentiseert zich middels een public/private keypair op de front-end server op de SSH daemon op poort 2222. Wachtwoord

authenticatie is bij uitzondering ook mogelijk, maar het is de bedoeling dat dit alleen gebeurt als de SFTP server via een besloten netwerk wordt benaderd. Dit wordt niet technisch afgedwongen in de configuratie van de SSH daemon. In principe kan vanaf internet met gebruikersnaam en wachtwoord worden ingelogd.

3. De gebruiker plaatst een CSV bestand in zijn home directory die hoort bij zijn SFTP account op de front-end SFTP server.
4. Een script monitort continu (op basis van inotify) de home directories en verplaatst zo snel mogelijk het CSV bestand naar een directory op de met de back-end server gedeelde NFS share.
5. Op de back-end server verplaatst een 'smartmove' script het geüploade bestand vervolgens naar een andere directory, van waaruit het wordt ingelezen door de vaccinatiedatabase.
6. Het bestand wordt gearchiveerd op de back-end server.

2 Onderzoeksvraag 2: Diverse bevindingen en aanbevelingen SFTP koppelvlak geïdentificeerd; Beveiliging SFTP koppelvlak significant verbeterd na aanpassingen maar verdere verbetering met kracht aangeraden

In deze paragraaf wordt de tweede onderzoeksvraag beantwoord: '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?'. Deze vraag wordt beantwoordt voor twee momenten:

1. het initiële onderzoek dat ADR in de tweede helft van december 2020 heeft uitgevoerd;
2. het opvolgingsonderzoek (hertest) dat in de week van 8 februari 2021 is uitgevoerd gericht op de opvolging van de initiële bevindingen waarvan RIVM heeft aangegeven dat deze zijn aangepakt.

In de volgende paragrafen worden op technisch detailniveau de oorspronkelijke bevindingen en de eventuele bevindingen uit de follow-up weergegeven. Hierbij wordt een risicoschatting voor de bevinding gegeven (in termen van Hoog/Midden/Laag) en een inschatting van de benodigde inspanning om een aanbeveling uit te voeren (Hoog/Midden/Laag). Onder opvolging is de stand van zaken weergegeven ten tijde van het opvolgingsonderzoek. Hierbij is onder meer gebruik gemaakt van een interview met beheerders en ontwikkelaars van RIVM op 3 en 10 februari 2021. Door de beperkte resolutie van de gehanteerde risiconiveaus (H/M/L) is het mogelijk dat getroffen maatregelen beveiligingsrisico's wel in enige mate reduceren maar dat de inschatting van het risiconiveau daardoor niet wijzigt. De bevindingen zijn logisch geclusterd naar een vijftal onderwerpen.

2.1 Inrichting server

2.1.1 Configuratie SSH daemon minder overzichtelijk; verbetering gerealiseerd

De SSH daemon op de SFTP server wordt zowel gebruikt voor beheertoegang als voor SFTP toegang voor overdracht van vaccinatiedata. De SSHD configuratiebestanden zijn minder overzichtelijk door deze mix van functies. Dit kan ook leiden tot onbedoelde gevolgen als wijzigingen ten behoeve van SFTP impact hebben op de SSH-beheertoegang en vice versa.
Risico: M

Aanbeveling: Breng scheiding aan tussen de verschillende functies. Dit kan onder andere door meerdere SSH daemons te draaien met verschillende configuratie, met bijvoorbeeld de beheertoegang op een niet standaard en niet naar buiten toe ontsloten poort.
Inspanning: M

Februari 2021
RIVM heeft een front-end server ingericht (zie ook paragraaf 1.1.2) waarop twee SSH daemons aanwezig zijn, een voor SFTP en een voor beheertoegang. Hiermee is dit punt opgelost.

2.1.2 *Hardening operating system en SSH daemon behoeft versterking*

RIVM heeft medegedeeld dat zij onder meer gebruik heeft gemaakt van BIR en BIO als kader voor hardening van het operating system en de SSH daemon van de SFTP server. Voor onderzoek van de hardening van de SFTP server is gebruik gemaakt van de audittool 'Lynis'. Het resultaat van het toepassen van deze tool bevestigt dat hardening is toegepast maar geeft ook aan dat verbetering op onderdelen mogelijk is.
Risico: M

Aanbeveling: Onderzoek de voorstellen uit de Lynis rapportage voor verbetering en pas deze zo veel mogelijk toe.
Inspanning: M

Februari 2021
Over aanpassing van de huidige back-end server hebben we geen nadere informatie ontvangen. Op basis van de Lynis output voor de front-end server is het beeld dat hardening heeft plaatsgevonden maar dat verbetering mogelijk is.
Risico: M

Aanbeveling: Zie oorspronkelijk aanbeveling. Pas deze toe voor zowel de front-end als de back-end server.

2.1.3 *Oude configuratie in SFTP server; verbetering deels gerealiseerd*

De CIMS omgeving is een directe kopie van de Praeventis SFTP server. Hierbij is oude configuratie in de server aangetroffen, onder meer voor functionaliteit en gebruikers die binnen CIMS niet worden gebruikt. Oude configuratie verhoogt kans op bijvoorbeeld onbedoelde functionaliteit en menselijke fouten. Daarnaast verhoogt dit ook het potentiële aanvalsoppervlak.
Risico: M

Aanbeveling: Richt de SFTP server opnieuw in op basis van een standaard image met alleen de daadwerkelijk benodigde functionaliteiten, koppelingen en gebruikers.
Inspanning: M

Februari 2021
Zoals in paragraaf 1.2.1 ook is aangegeven is een nieuwe frond-end server is ingericht die voor de back-end (oude) server is geplaatst. Hierbij worden beveiligingsrisico's gereduceerd doordat de oude server (nu back-end server) niet meer benaderbaar is vanaf internet. Wel wordt NFS[3] in combinatie met een NAS[4] toegepast voor communicatie tussen front-end en back-end server. De toepassing van NFS als protocol zonder encryptie en gebruik van twee servers in plaats van een in de DMZ[5] verhogen beveiligingsrisico's weer in enige mate. Onze inschatting is dat het aanvalsoppervlak vanaf internet is verkleind maar dat het interne aanvalsoppervlak hiermee groter is geworden. Het netto beveiligingsrendement van de verschillende aanpassingen is daarom lastig in te schatten.
Risico: M

[3] Een ouder protocol voor delen van bestanden op een netwerk.

[4] Network Attached Storage: een gespecialiseerde server oplossing voor het delen van informatie binnen een netwerk.

[5] Demilitarized Zone (DMZ): een semi vertrouwde zone in het netwerk tussen het internet en het interne netwerk in.

Aanbeveling: Onderzoek op welke wijze het aantal servers in de DMZ weer terug kan worden gebracht naar één en op welke wijze alleen protocollen met encryptie voor dataoverdracht kunnen worden toegepast. Realiseer dit vervolgens.
Inspanning: M

RIVM heeft ons medegedeeld dat zij voornemens is om op korte termijn NFS te vervangen door een veiliger oplossing.

2.1.4 *Verbetering cryptografische en andere instellingen SSH daemon mogelijk; verbetering deels gerealiseerd*
Voor data in transit wordt het ssh protocol gebruikt voor communicatie met de SSH daemon. In de uitgevoerde pentest is ondermeer middels de audittools 'ssh-audit', 'nmap' en 'Lynis' onderzoek gedaan naar de SSH daemon. Een bevinding is dat de instellingen voor de gebruikte cryptografische algoritmen afwijken van de eigen baseline van RIVM (afwijking is bijvoorbeeld het gebruik van de cipher 'AES128-CBC'). Deze instellingen kunnen verder ook worden versterkt, zie de aanwijzingen hiervoor in de output van de verschillende audittools zoals ter beschikking gesteld aan RIVM.
Risico: M

Aanbeveling: Breng de configuratie van de SSH daemon in overeenstemming met de baseline van RIVM.
Inspanning: L

Aanbeveling: Breng de configuratie van de SSH daemon in overeenstemming met de aanbevelingen en verbetermogelijkheden zoals gesignaleerd door de audittools 'ssh-audit', 'nmap' en 'Lynis'.
Inspanning: M

Februari 2021
Een verbetering is dat de cipher 'AES128-CBC' niet meer wordt ondersteund op de front-end server. Nog niet alle aanbevelingen van de audittool 'ssh-audit' en 'Lynis' zijn doorgevoerd (of voorzien van een onderbouwing waarom niet noodzakelijk/mogelijk).
Risico: M

Aanbeveling: Onderzoek op welke wijze voor de front-end server de aanbevelingen uit de audittool 'ssh-audit' en 'Lynis' kunnen worden gerealiseerd en documenteer de uitkomsten. Houd hierbij rekening met de clients die eventueel verbinding maken met oudere encryptiealgoritmes. Realiseer vervolgens de mogelijke verbeteringen en laat eventuele risico's accepteren door het verantwoordelijk management.
Inspanning: M

2.2 Bescherming netwerk

2.2.1 *Op netwerkniveau meer informatie vrijgegeven dan strikt noodzakelijk; verbetering gerealiseerd*
Vanaf internet is het voor iedereen mogelijk om de SFTP server te benaderen via ICMP ('ping'). Hiermee wordt meer informatie vrijgegeven dan strikt noodzakelijk.
Risico: L

Aanbeveling: Sta ICMP vanaf internet niet toe. Indien noodzakelijk kan dit voor op de firewall gewhiteliste hosts wel worden toegestaan.
Inspanning: L

Februari 2021
ADR heeft vastgesteld dat de front-end en back-end server niet meer benaderbaar zijn middels ICMP ('ping'). Hiermee is de verbetering gerealiseerd.

2.2.2 *Mogelijk onnodige verkeersstromen toegestaan naar hoger beveiligde zones*
Er worden voor de SFTP server mogelijk onnodige verkeersstromen toegestaan naar hoger beveiligde zones (b.v. TCP port 1521 naar database).
Risico: H

Aanbeveling: Onderzoek of toegang op TCP port 1521 naar de database functioneel inderdaad niet nodig is en zet deze poort dicht op de firewall tussen de SFTP server en het interne netwerk. Onderzoek of dit ook geldt voor andere poorten.
Inspanning: L

Februari 2021
Deze bevinding betreft nu de back-end server die niet meer rechtstreeks toegankelijk is vanaf internet. Geen nieuwe informatie ontvangen.

2.2.3 *Apart netwerk voor beheertoegang niet ingericht*
Er is geen apart netwerk (bijvoorbeeld vlan) voor beheertoegang ingericht waardoor beheerverkeer en productieverkeer niet van elkaar zijn gescheiden.
Risico: L
Aanbeveling: Onderzoek het gebruik van een separaat netwerk (bijvoorbeeld vlan) voor beheer en realiseer dit.
Inspanning: H

Februari 2021
Geen wijzigingen

2.3 Data bescherming

2.3.1 *Data in rust niet versleuteld; risico beperkt aangezien niet meer rechtstreeks vanaf internet benaderbaar*
Doordat data in rust op de SFTP server niet is versleuteld, is deze bij een beveiligingsincident op de server mogelijk toegankelijk. Oneigenlijke toegang tot de server leidt dan direct tot compromittering van de aanwezige vertrouwelijke gegevens, voor zover benaderbaar.
Risico: H

Aanbeveling: Zorg voor encryptie van data in rust die is opgeslagen op een server die rechtstreeks vanaf internet bereikbaar is. Dit houdt feitelijk in dat leveranciers van data hun bestanden versleuteld aanleveren. Decryptie van bestanden vindt dan dieper in het netwerk plaats (niet op de SFTP server!).
Inspanning: H

Februari 2021
Door de nieuwe constructie waarbij de back-end (oude) server niet meer rechtstreeks kan worden benaderd vanaf internet, is het risico op dit punt gereduceerd.
Risico: M

Aanbeveling: Wel blijft de oorspronkelijke aanbeveling staan om aanbieders hun bestanden versleuteld aan te laten leveren en pas dieper in het netwerk decryptie te laten plaatsvinden.

2.3.2 *SFTP server als archief gebruikt; verbetering deels gerealiseerd*
De SFTP server wordt ook als archief gebruikt. Alle aangeleverde bestanden met vaccinatiedata worden na het inlezen in de database naar een lokaal archief op de SFTP server verplaatst en daar bewaard. Ook wordt op dezelfde server dagelijks een BRP (Basis Registratie Personen) update bestand binnengehaald en voor 7 dagen bewaard. Door bovengenoemde zaken treedt opeenstapeling van (gevoelige) data op.

Risico: H

Aanbeveling: Gebruik een server die rechtstreeks is verbonden met internet of die in de DMZ staat niet voor een archieffunctie. Bewaar zo min mogelijk data voor een zo kort mogelijke periode op deze server. Denk hierbij ook aan de 'doubles' directory. Plaats de archieffunctie in de kern van het RIVM netwerk. Door de SFTP server niet voor archiefdoeleinden te gebruiken wordt het risico van paragraaf 1.2.4 ook deels gemitigeerd.
Inspanning: L

Februari 2021
Door de nieuwe constructie waarbij de back-end (oude) server niet meer rechtstreeks kan worden benaderd vanaf internet is het risico enigszins gereduceerd. De back-end server staat echter nog steeds in de DMZ en in het algemeen is dit geen goede plek voor een archieffunctie.
Risico: M

Aanbeveling: zie oorspronkelijke aanbeveling.

2.4 Gebruikersmogelijkheden beperken

2.4.1 *SFTP commando's bieden meer functionaliteit dan noodzakelijk*

De SFTP commando's die in een SFTP sessie kunnen worden uitgevoerd zijn niet beperkt terwijl dit wel mogelijk is. Mede hierdoor was het tijdens de pentest mogelijk zelf nieuwe directories aan te maken en uitvoerbare bestanden te plaatsen op de server.
Risico: H

Aanbeveling: Maak gebruik van whitelisting van SFTP commando's. Waarschijnlijk zijn alleen put en eventueel ls en cd nodig, maar zeker geen mkdir, df, symlink, get, etc.)
Inspanning: L

Februari 2021
In de configuratiefile voor de SFTP service op de front-end server is een aanzet zichtbaar voor restrictie maar uit de pentest blijkt dat deze niet effectief is.
Risico: H

Aanbeveling: zie oorspronkelijke aanbeveling.

2.4.2 *Versterking bestandsrechten en controle bestanden SFTP gebruikers noodzakelijk; belangrijke verbeteringen gerealiseerd*

Gedurende de pentest zijn de volgende zaken met betrekking tot bestandsrechten van SFTP gebruikers op de SFTP server vastgesteld:

1. Gebruikers kunnen zelf directories aanmaken en daarbinnen bestanden uploaden. Deze directories en bestanden zijn voor alle SFTP gebruikers in te zien en de bestanden te downloaden.
2. Bestanden die op de SFTP server worden geplaatst, worden niet gecontroleerd op malware. Er is geen malware scanner aanwezig op de SFTP server. Het is bijvoorbeeld mogelijk om testvirussen te uploaden. Dit maakt het mogelijk om uitvoerbare en/of malafide bestanden op de server te zetten.
3. Zodra bestanden tweemaal worden geüpload, komen deze terecht in de 'doubles' directory. Hier kunnen ze ook door andere gebruikers worden benaderd en gedownload, omdat alle SFTP gebruikers toegang hebben tot de 'doubles' map.

4. Het is mogelijk om legitieme bestanden die worden geüpload door gebruiker een in de incoming map, door gebruiker twee te laten downloaden voordat het 'smartmove' script het bestand verplaatst naar een locatie op het filesystem waar het niet meer bereikbaar is voor SFTP gebruikers.

Risico: M

Aanbeveling: Zorg ervoor dat per gebruiker een aparte upload directory beschikbaar is waartoe andere gebruikers geen toegang hebben.
Inspanning: L

Aanbeveling: Zorg er voor dat uitvoerbare en malafide bestanden worden geweerd van de server door het gebruik van bijvoorbeeld een malware scanner en het valideren van aangeleverde bestanden/bestandstypen.
Inspanning: M

NB. Deze risico's kunnen al behoorlijk worden beperkt door de onder paragraaf 1.2.7 genoemde whitelisting van SFTP commando's.

Februari 2021
Wij hebben vastgesteld dat een aparte upload directory per SFTP gebruikers is gerealiseerd op de front-end server. Verder is ons medegedeeld dat op de NAS een malware scanner wordt toegepast (zie ook paragraaf 1.2.2). Door het toepassen van een eigen directory per gebruiker en het direct verplaatsen van het bestand na upload middels een script wordt voorkomen dat gebruikers bestanden nog kunnen downloaden. Een aandachtspunt is dat upload van uitvoerbare bestanden nog steeds mogelijk is.
Risico: M

Aanbeveling: Voorkom dat uitvoerbare bestanden kunnen worden geüpload. Hiervoor kan bijvoorbeeld worden onderzocht of het voldoende is om op de front-end server het UMASK voor upload door gebruikers naar '0177' aan te passen in de 'sshd_sftp_config'.
Inspanning: L

2.5 In te zetten periodieke acitviteiten voor beheer

2.5.1 *Vulnerability assessments niet ingericht voor SFTP server*

De mogelijkheden tot het uitvoeren van vulnerability assessments op de componenten van CIMS zijn aanwezig bij het Security Operations Center van RIVM, maar is nog niet ingericht voor (de SFTP server van) CIMS.
Risico: M

Aanbeveling: Richt het periodiek (b.v. dagelijks of wekelijks) uitvoeren van vulnerability assessments in en draag zorg voor analyse en opvolging van eventuele bevindingen.
Inspanning: L

Februari 2021
RIVM heeft medegedeeld dat dit is ingericht maar hiervoor is geen aanvullend materiaal ontvangen. Aanbeveling blijft vooralsnog staan.

2.5.2 *Nog geen penetratiestest uitgevoerd op CIMS als geheel*

Er is nog geen penetratietest (technisch beveiligingsonderzoek) uitgevoerd op CIMS als geheel. De werkzaamheden van ADR zijn beperkt tot de SFTP server.
Risico: M

Aanbeveling: Voer structureel penetratietesten op CIMS uit. Doe dit minimaal 1x per vastgestelde periode (bijvoorbeeld een jaar) en bij grote wijzigingen.
Inspanning: H

Februari 2021
Geen verandering

2.5.3 *Logging en monitoring niet ingericht voor CIMS*
Het RIVM heeft een SOC die ook gebruik maakt van een SIEM (Security Information en Event Management) systeem. CIMS is echter nog niet gekoppeld aan het SIEM. Aangezien koppeling nog niet heeft plaatsgevonden, kan nog geen effectieve signalering van mogelijk misbruik plaatsvinden. Er zijn dus ook nog geen use cases gedefinieerd voor (de SFTP server van) CIMS om middels het SIEM bij het SOC afwijkingen van reguliere verkeersstromen en opvallende events op de SFTP server te kunnen detecteren.
Risico: H

Aanbeveling: Stuur SSHD/SFTP logging en file access logging (bijvoorbeeld met 'auditd') naar het SIEM.
Inspanning: L

Aanbeveling: (voorgaande aanbeveling is randvoorwaardelijk) Definieer use cases en richt bijbehorende procedures in bij het SOC en in beheerprocessen en richt bijbehorende technische voorzieningen (bijvoorbeeld drempelwaardes) in het SIEM in.
Inspanning: M

Februari 2021
RIVM heeft medegedeeld dat logging inmiddels wordt doorgestuurd naar het SIEM (eerste aanbeveling) en dat beheerders van RIVM met de tweede aanbeveling bezig zijn. Dit is niet verder onderzocht.

2.5.4 *Geen standaard oplossing voor patch management ingezet*
Er wordt geen gebruik gemaakt van de standaard RIVM oplossing (Satellite) om de SFTP server te patchen. Aangegeven is dat dit te maken heeft met het feit dat de patches op een specifiek moment automatisch worden doorgevoerd middels Satellite, maar dat op dat moment CIMS bereikbaar dient te zijn. De beheerder geeft aan dat patching handmatig wordt uitgevoerd zodra dat mogelijk is. Risico is dat patching niet of niet tijdig plaatsvindt.
Risico: H

Aanbeveling: Draag zorg voor structurele borging van tijdige patching van de SFTP server.
Inspanning: M

Februari 2021
RIVM heeft medegedeeld dat patching nu 1x in de drie maanden plaatsvindt. Hiervoor is geen nadere evidence aangeleverd maar op het moment van onderzoek draaide de nieuwe front-end server in ieder geval de laatste release van het operating system. Drie maanden tussen patchrondes is naar de professionele inschatting van ADR te lang.
Risico: M

Aanbeveling: Voer patching voor een server die rechtstreeks benaderbaar is vanaf internet vaker uit. Maak hiervoor een risicoafweging. Wellicht kan in een uitwisselingsprotocol voor vaccinatiedata worden opgenomen dat de aanleverende partij het bestand bijvoorbeeld 24 uur moet blijven aanbieden. RIVM kan dan bijvoorbeeld het systeem onder kantoortijd patchen en een roll-back doen als patching onverhoopt tot een verstoring leidt.
Inspanning: M

2.5.5 Aandachtpunten rondom capaciteit geïdentificeerd

In principe valt het volgende buiten de grens van ons onderzoek maar het onderwerp is mogelijk wel relevant: Tijdens de pentest kwam naar voren dat de beschikbare opslagruimte op de SFTP server beperkt is (3,5 GB vrije ruimte). Tevens leek de beschikbare bandbreedte bij upload van een groot bestand relatief laag (circa 2,7 MB/s). Wij hebben niet onderzocht waar deze beperking optrad. Voor een server die van een fors aantal partijen data moet ontvangen lijken de beschikbare schijfruimte en bandbreedte laag. Ook lijken geen diskquota aanwezig te zijn waardoor de schijfruimte b.v. als gevolg van een menselijke fout zou kunnen vollopen.

Aanbeveling: Onderzoek of de beschikbare resources van de server (opslagruimte en netwerkbandbreedte) voldoende zijn voor de use cases. Ga ook na of inzet van diskquota noodzakelijk is.

Februari 2021
Buiten scope, niet onderzocht.

2.6 Samenvattend beeld

Het samenvattend beeld is dat het initiële onderzoek eind december 2020 in eerste instantie heeft geleid tot circa 15 bevindingen. Voor zover wij in de beperkte tijd die beschikbaar was hebben kunnen onderzoeken, leiden deze bevindingen niet direct tot toegang tot vaccinatiedata die wordt aangeleverd op de SFTP server. Wel brengen deze belangrijke beveiligingsrisico's met zich mee. Uit de hertest komt het beeld dat een aantal bevindingen inderdaad is verbeterd, al leveren sommige oplossingen in enige mate ook weer hun eigen beveiligingsproblemen op, met name de inzet van NFS (zie paragraaf 2.1.3).

De concept bevindingen van de hertest zijn besproken tussen RIVM en ADR. De bevindingen werden hierbij herkend door RIVM. Een gedeeld beeld is dat om alle bevindingen op te lossen een herontwerp van de hele keten van aanbieder van vaccinatiedata tot RIVM zou moeten worden onderzocht. Hierbij zou dan bijvoorbeeld end-to-end encryptie van vaccinatiedata kunnen worden toegepast.

3 Verantwoording onderzoek

3.1 Context

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[6] 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.

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.

---

6 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 is ADR verzocht om een quick scan uit te voeren op het SFTP koppelvlak van CIMS, gericht op het aspect vertrouwelijkheid. Opdrachtgever hierbij is DG RIVM. 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 CIMS die benaderbaar is vanaf het internet (beschermd door een firewall).

3.2 Doelstelling en afbakening

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 zijn beantwoord middels het uitvoeren van een quick scan: een onderzoek dat is beperkt doorlooptijd en diepgang. Op verzoek van opdrachtgever is ook een test van verbeteringen (verder: hertest) uitgevoerd die RIVM heeft gerealiseerd naar aanleiding van de initiële bevindingen op het gebied van de tweede onderzoeksvraag van eind december 2020.

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 hebben geen deel uitgemaakt van het onderzoek.

Voor de beantwoording van onderzoeksvraag twee is in het kader van deze quick scan een beperkt referentiekader gehanteerd: een relevante selectie uit het DigiD assessment kader (Norm ICT-beveiligingsassessments DigiD versie 2.0), zie bijlage I. Daar waar in dit kader wordt gesproken over webapplicatie of webserver wordt in deze context de SFTP server bedoeld. In het kader van werkzaamheden voor de quick scan zijn enkele interviews uitgevoerd met beheerders van het SFTP koppelvlak, zijn documentatie en configuratiebestanden onderzocht en zijn enkele penetratiestestwerkzaamheden uitgevoerd met tooling vanaf internet en op de SFTP server zelf.

3.3 Gehanteerde standaard

Deze opdracht is uitgevoerd in overeenstemming met de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing (Standaarden IIA 2200-2450 en 2600). Tevens wordt verwezen naar het Audit Charter van de ADR voor de uitgangspunten die voor de ADR van toepassing zijn. Het Audit Charter bevat de algemene uitgangspunten voor de uitoefening van de interne auditfunctie bij de rijksdienst en beschrijft het doel, de taken, de bevoegdheden en de verantwoordelijkheden van de ADR.
In dit rapport wordt geen zekerheid verschaft, omdat er geen assurance-opdracht is uitgevoerd.

3.4 Verspreiding rapport

De opdrachtgever, Directeur-Generaal RIVM, 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.

4 Ondertekening

Den Haag, 18 maart 2021

5.1.2e

5.1.2e

Bijlage I Referentiekader

#	Beveiligingsrichtlijn
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, 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 want buiten scope)
U/PW.03	De webserver (SFTP server) 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.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 ICTsystemen 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.