23 augustus 2022

Security bij VRI's

Front paper

Opdrachtgever SmartwayZ.NL
Opdrachtnemer DTV Consultants B.V.

Inhoudsopgave

Versiebeheer 3

Samenvatting 4

1. Inleiding 8

1.1 Aanleiding 8

1.2 Doel van het onderzoek 8

1.3 Leeswijzer 8

2. Het landschap 10

2.1 Wat speelt er 10

2.2 Architectuur en keten 11

3. Security issues (i)VRI keten 18

3.1 Risico inventarisatie en beheersmaatregelen 18

3.2 Fasering van beheersmaatregelen 28

4. Consequenties voor de wegbeheerder 31

4.1 Kosten 31

4.2 Organisatie 32

Bijlage 1: Gesprekken stakeholders 34

Bijlage 2: Beheersmaatregelen per type stakeholders 35

Bijlage 3: Checklist beheersmaatregelen 40

Versiebeheer

Versie	Status	Auteur	Datum	Opmerkingen
0.1	Concept	DTV Consultants – Tom Steijvers & Joost Hormann	17-03-2022	Initieel document
0.2	Concept	DTV Consultants – Tom Steijvers & Joost Hormann	04-05-2022	Aanpassingen na bespreken met VRI specialisten en CISO's, samenvatting toegevoegd
0.3	Concept	DTV Consultants – Tom Steijvers & Joost Hormann	17-06-2022	Aanpassingen na review VRI specialisten en externe stakeholders
1.0	Definitief	DTV Consultants – Tom Steijvers & Joost Hormann	23-08-2022	Definitief maken na toelichting in CIBO

Samenvatting

Aanleiding en doel
Met de komst van de intelligente verkeersregelinstallatie (iVRI) is het landschap waarin een verkeersregelinstallatie (VRI) zich bevindt aanzienlijk veranderd. Doordat de iVRI onderdeel is van een (data-)keten en daarmee ook nieuwe functionaliteiten bevat, is veel meer aandacht nodig voor security. Daarom is deze front-paper opgesteld. Hiermee kunnen wegbeheerders hun management informeren over de security risico's rondom (i)VRI's en kan de paper als startpunt fungeren voor de verdere uitwerking van de LVMB-actie om te komen tot een handreiking Security VRI's.

Het landschap
Verkeerslichten staan er voor de (verkeers)veiligheid en voor het regelen van de doorstroming van het verkeer. Door de toegenomen technologische ontwikkelingen wordt de VRI ook steeds complexer en meer digitaal. Naarmate de VRI steeds digitaler wordt, wordt de VRI meer verbonden met andere systemen en netwerken en gaat de VRI steeds meer informatie verzenden en ontvangen. Hiermee wordt het risico op inbreuk in de VRI op de datastromen in de VRI alsmaar groter. Tot een aantal jaar geleden bestond de intelligente verkeersregelinstallatie (iVRI) nog niet. De architectuur van de VRI en de bijbehorende keten was en is (voor de installaties die nog op straat staan) een stuk minder uitgebreid en complex dan die van de iVRI. De iVRI maakt onderdeel uit van een dataketen van en naar de weggebruiker. Dit alleen leidt al tot een hoger veiligheidsrisico, want de weggebruiker moet ervan uit kunnen gaan dat de informatie die hij ontvangt, betrouwbaar is.

Wegbeheerders dienen als overheidsorganisatie te voldoen aan de richtlijnen ten aanzien van informatiebeveiliging voor de gehele overheid zoals vastgelegd in de Baseline Informatiebeveiliging Overheid (BIO). De BIO beschrijft alle maatregelen en controls die ervoor moeten zorgen dat de omgang met informatie (data) in systemen en door eindgebruikers op correcte wijze plaatsvindt. De BIO is echter te breed voor eisen die gesteld moeten worden aan veilige producten van leveranciers, zoals (i)VRI's. Daarnaast ervaren veel VRI-beheerders de BIO en het thema informatiebeveiliging als specifieke en complexe materie en als een nieuw vakgebied om aan te voldoen.

Security bij (i)VRI's is momenteel nog niet op orde, mede doordat VRI's veelal 15 jaar (of langer) op straat staan en dat bij eerdere aanbestedingen bepaalde huidige security eisen niet uitgevraagd zijn door wegbeheerders. Daarnaast is een concretisering van de BIO-eisen en -maatregelen voor het thema (i)VRI is gewenst.

Security issues
Er heeft een risico inventarisatie van security issues plaatsgevonden op basis van interviews met diverse wegbeheerders, het Ministerie van I&W en een iVRI-leverancier en op basis van literatuurstudie van diverse openbaar beschikbare en aangeleverde documenten.

Om ordening aan te brengen binnen de risico's en de bijbehorende beheersmaatregelen zijn deze onder verdeeld naar de volgende onderwerpen:

- Toegangsbeheer
- Informatiebeveiliging
- Change Management
- Incident Management
- Personeel en organisatie
- Imago

Per risico is een bijbehorende beheersmaatregel benoemd en voor wie deze beheersmaatregel bestemd is (lokale/regionale wegbeheerder, landelijke overheid of leverancier). Omdat het naar verwachting niet mogelijk is om alle beheersmaatregelen in één keer te implementeren, is een voorstel gedaan voor een fasering van beheersmaatregelen naar logische onderwerpen:

- Fase 1: Wegbeheerders en leveranciers implementeren zoveel mogelijk 'quick win' beheersmaatregelen. Hiermee kan het security niveau op korte termijn op relatief eenvoudige wijze aanzienlijk verhoogd worden. Tevens wordt hiermee een eerste stap gezet om volledig BIO-compliant te worden (jaar 1).
- Fase 2: De landelijke overheid stelt de benodigde landelijke richtlijnen op (jaar 1 en 2).
- Fase 3: Wegbeheerders en leveranciers passen de landelijke richtlijnen uit Fase 2 toe en implementeren de resterende beheersmaatregelen om volledig BIO-compliant te worden (jaar 3).

Op basis van deze faseringen is een checklist opgesteld waarin alle in deze front paper opgenomen beheersmaatregelen naar de genoemde fases zijn opgesplitst. Deze checklist biedt een handvat voor wegbeheerders en leveranciers, maar elke wegbeheerder en leverancier bepaalt uiteindelijk zelf welke maatregelen hij in welke fase wil uitvoeren.

Consequenties voor de wegbeheerder
Op hoofdlijnen zijn de consequenties uit te splitsen naar de aspect kosten en organisatie.

De aspecten die effect hebben op zowel eenmalige kosten en jaarlijkse kosten om de security rondom (i)VRI op orde te brengen, zijn:

- Eenmalige kosten
    - Openbreken van de huidige contracten met leveranciers en bijdragen aan de ontwikkelkosten van iVRI-component leveranciers om up-to-date te worden met de BIO-eisen (mogelijk enkele miljoenen euro's).
    - Kosten voor het eenmalig up-to-date brengen van het eigen areaal aan (i)VRI's (mogelijk € 10.000,- tot € 30.000,- per VRI).
    - Kosten voor inrichten van alle benodigde procedures en het (anders of aanvullend) inrichten van de beheerorganisatie (extra FTE benodigd).
- Jaarlijkse kosten
    - Extra jaarlijkse kosten in de onderhoudscontracten met leveranciers voor werkzaamheden van leveranciers van iVRI-componenten in verband met aanvullende eisen om iVRI-componenten secure te houden conform de BIO-eisen (mogelijk € 500,- tot € 2.000,- per jaar per VRI).

De aspecten die effect hebben op de organisatie van de wegbeheerders om de security rondom (i)VRI op orde te brengen, zijn:

- Inrichten van nieuwe procedures, aanscherpen van bestaande procedures en het vervolgens hierop inrichten van de projecten- en beheerorganisatie (extra FTE benodigd).
- Inrichten van nieuwe procedures en het aanscherpen van bestaande procedures voor de controle van alle dienstenleveranciers conform eisen BIO en het vervolgens hierop inrichten van de projecten- en beheerorganisatie (extra FTE benodigd).

Belangrijke constatering en aanbeveling
De belangrijkste constatering is dat de huidige (i)VRI's op straat niet voldoen aan de BIO én dat met de eisen die nu worden gesteld bij de aanschaf en het onderhoud van nieuwe (i)VRI ook niet wordt voldaan aan de eisen uit de BIO. Wegbeheerders missen nu een praktische vertaling van de BIO voor het thema (i)VRI die zij kunnen gebruiken bij aanbestedingen. Dit dient door de wegbeheerders opgesteld te worden. Ook dient samen met de leveranciers een transitiepad besproken te worden hoe markt en overheid over een aantal jaar gezamenlijk wel BIO-compliant zijn.

Geadviseerd wordt om dit landelijk op te pakken, zodat direct alle wegbeheerders hier baat bij hebben. Bij het uitwerken van deze vertaling is het noodzakelijk dat wegbeheerders en leveranciers gezamenlijk op een constructieve wijze samenwerken zodat er consensus ontstaat over de uitwerking van de eisen en zodat gezamenlijk een reëel transitiepas wordt bepaald waarbij zowel de wegbeheerder als de leverancier over een aantal jaar volledig BIO compliant zijn.

De ervaring leert echter ook dat dergelijke landelijke uitvoeringsacties vaak veel tijd kosten, lang duren en moeilijk te organiseren zijn. De noodzaak om binnen enkele jaren adequate maatregelen te treffen is echter wel aanwezig. De vraag is daarom of de Brabantse wegbeheerders hierop willen wachten. Mogelijk kunnen de Brabantse wegbeheerders gezamenlijk initiatief starten om (in overleg en samenspraak met de markt) tot concrete BIO eisen en een bijbehorend implementatieplan te komen. Mogelijk dat dit daarna versneld tot een landelijke standaard kan leiden.

Inleiding

1. Inleiding

1.1 Aanleiding

Met de komst van de intelligente verkeersregelinstallatie (iVRI) is het landschap waarin een verkeersregelinstallatie (VRI) zich bevindt aanzienlijk veranderd. Doordat de iVRI onderdeel is van een (data-)keten en daarmee ook nieuwe functionaliteiten bevat, is veel meer aandacht nodig voor security.

Wegbeheerders[1] zijn eigenaar en beheerder van de (i)VRI's en daarmee ook verantwoordelijk voor een gedegen beveiliging van deze objecten. Aangezien security zich steeds meer op het gebied van ICT en informatiebeveiliging bevindt, is meer specialistische kennis noodzakelijk. Om die reden trekken de VRI-specialisten, ICT-architecten en CISO's (Chief Information Security Officers) nauw met elkaar op om de security risico's in kaart te brengen en maatregelen te implementeren.

Vanuit de regio Brabant (B5) is het item 'security rondom (i)VRI's' door de VRI-specialisten en de CISO's apart van elkaar besproken. Beide partijen zien de noodzaak om het item op te pakken en verder te brengen. Daarom is gezamenlijk besloten tot het opstellen van een zogenaamd 'front paper' met hierin een inventarisatie van de security risico's, een overzicht van mogelijke beheersmaatregelen en een globaal uitvoeringsprogramma. De provincie Noord-Brabant heeft hierin de lead genomen. Deze rapportage betreft deze front paper.

1.2 Doel van het onderzoek

Doel van het onderzoek is te komen tot een generieke front-paper, waarmee de betrokken wegbeheerders hun management kunnen informeren over de security risico's rondom (i)VRI's. Tevens kan deze als startpunt fungeren voor de verdere uitwerking van de LVMB actie om te komen tot een handreiking Security VRI's.

Deze front-paper richt zich op de gemeenschappelijke onderdelen die voor alle wegbeheerders gelden en niet op specifieke (architectuur)zaken van individuele wegbeheerders. Op basis van deze front-paper wordt het mogelijk om op beleids- en/of bestuurlijk niveau keuzes te maken voor de te nemen maatregelen en de bijbehorende consequenties op het gebied van financiën en personeel.

1.3 Leeswijzer

Hoofdstuk twee beschrijft het landschap waarin de (i)VRI zich bevindt. In hoofdstuk drie zijn de belangrijkste risico's op het gebied van security beschreven. Hoofdstuk vier bevat een beschrijving van de consequenties hiervan voor de wegbeheerder.

[1] *De wegbeheerder is de overheid, overheidsorganisatie of instantie die is belast met het feitelijke wegbeheer van een weg of wegvak. Een (i)VRI maakt onderdeel uit van de weg.*

Het landschap

2. Het landschap

2.1 Wat speelt er

Verkeerslichten staan er voor de (verkeers)veiligheid en voor het regelen van de doorstroming van het verkeer. Door de toegenomen technologische ontwikkelingen wordt de VRI ook steeds complexer en meer digitaal. In feite zijn het computers die het verkeer regelen, waarbij de computer de hardware aanstuurt. Naarmate de VRI steeds digitaler wordt, wordt de VRI meer verbonden met andere systemen en netwerken en gaat de VRI steeds meer informatie verzenden en ontvangen. Hiermee wordt het risico op inbreuk in de VRI op de datastromen in de VRI alsmaar groter.

Baseline Informatiebeveiliging Overheid (BIO)
Wegbeheerders dienen als overheidsorganisatie te voldoen aan de richtlijnen ten aanzien van informatiebeveiliging voor de gehele overheid. Deze zijn vastgelegd in de Baseline Informatiebeveiliging Overheid (BIO). De BIO beschrijft alle maatregelen en controls (ook wel thema's genoemd, uitgewerkt in hoofdstukken 5 t/m 18 in de BIO) die ervoor moeten zorgen dat de omgang met informatie (data) in systemen en door eindgebruikers op correcte wijze plaatsvindt. De beschikbaarheid, integriteit en vertrouwelijkheid moet gewaarborgd zijn. De gekozen vorm waarin het BIO-raamwerk is vastgelegd is voortgekomen vanuit een perspectief van kantoorautomatisering (gericht op overheidsorganisaties zelf) en de maatregelen hebben veelal een te hoog abstractieniveau. In deze vorm is de BIO te breed voor eisen die gesteld moeten worden aan veilige producten van leveranciers[2], zoals (i)VRI's. Daarnaast ervaren veel VRI-beheerders de BIO en het thema informatiebeveiliging als specifieke en complexe materie en als een nieuw vakgebied om aan te voldoen.

Wegbeheerders kopen veel producten en diensten in bij de markt. Door zaken uit te besteden/in te kopen legt de overheid deel van deze verantwoordelijkheid bij de markt neer: in termen van de BIO: de marktpartij/leverancier is een dienstenleverancier. De dienstenleverancier dient zijn dienst volgens het BasisBeveiligingsNiveau 2 (BBN2) van de BIO te leveren. De dienstenleverancier dient aan te geven en aan te tonen hoe hij hieraan voldoet en blijft voldoen.

Veel van de huidige VRI's zijn op straat gerealiseerd middels aanbestedingen voordat de BIO in werking is getreden. Daarom is in deze aanbestedingen en in de huidige contracten veelal geen rekening gehouden met (alle) eisen uit de BIO.

Security bij (i)VRI's is dus nog niet op orde, mede doordat VRI's veelal 15 jaar (of langer) op straat staan en dat bij eerdere aanbestedingen bepaalde huidige security eisen niet uitgevraagd zijn door wegbeheerders. Daarnaast is een concretisering van de BIO-eisen en -maatregelen voor het thema (i)VRI is gewenst. De BIO gaat over maatregelen op het gebied van techniek en op het gebied van processen, waarbij het zwaartepunt ligt bij de processen. Naast het voldoen aan de technische eisen is het dus ook belangrijk dat zowel de wegbeheerders als marktpartijen de processen goed ontwerpen, aanpassen en implementeren.

[2] Bron: https://www.bio-overheid.nl/media/1480/digi-workshop-presentatie.pdf

Nationale Cybersecurity Certificerings Autoriteit (NCCA)
Om ervoor te zorgen dat apparatuur en diensten digitaal veilig zijn worden er vanuit Europa nieuwe veiligheidseisen gesteld, die zijn vastgelegd in de Europese Cybersecurity Verordening, ook wel Cybersecurity Act genoemd (CSA). De CSA creëert op een framework voor een Europees certificeringstelsel voor producten, diensten en processen op het gebied van cybersecurity. Elke lidstaat wijst een nationale autoriteit aan die toetst of producten en diensten aan de afgesproken eisen voldoen. Het Agentschap Telecom is sinds april 2022 officieel de Nationale Cybersecurity Certificerings Autoriteit (NCCA) die zich bezighoudt met de certificering van IT-producten, diensten en processen, zoals IoT-apparatuur. Dit nieuwe stelsel maakt voor iedereen inzichtelijk hoe veilig en weerbaar producten en diensten zijn. Gecertificeerde producten zijn veiliger in gebruik en weerbaarder tegen cybercriminaliteit. Zeker omdat de verwachting is dat de veiligheidseisen nu nog vrijwillig zijn, maar in de toekomst waarschijnlijk verplicht worden voor fabrikanten en aanbieders in Europa. Gecertificeerde producten zijn in de toekomst te herkennen aan een Europees cybersecurity logo.

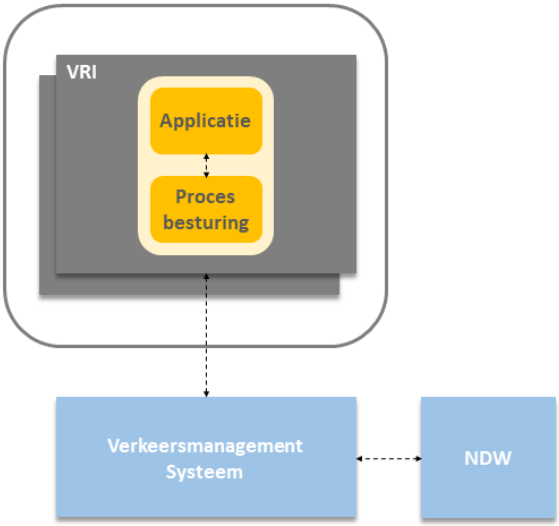
2.2 Architectuur en keten

Tot een aantal jaar geleden bestond de intelligente verkeersregelinstallatie (iVRI) nog niet. De architectuur van de VRI en de bijbehorende keten was en is (voor de installaties die nog op straat staan) een stuk minder uitgebreid en complex dan die van de iVRI. Omdat het huidige areaal in Noord-Brabant in grote mate uit zowel uit VRI's als iVRI's bestaat, is de architectuur en keten voor beide varianten in de navolgende paragrafen toegelicht. Hierbij geldt dat voor de VRI een 'sterfhuisconstructie' bestaat: bij het vervangen van de huidige VRI wordt deze vervangen door een iVRI. De verwachting is dat het aantal iVRI's daarmee alleen maar toe zal nemen de komende jaren. De huidige VRI blijft wel nog heel wat jaren in het areaal bestaan (verwachting tot rondom 2033), aangezien een VRI een gemiddelde vervangingstermijn van 15 jaar heeft en de implementatie van de iVRI in 2018 begonnen is.

2.2.1 VRI-architectuur en functionele keten

De VRI kent een regelautomaat in een kast op straat, voorzien van aantal deuren met sloten. Lokale bediening van de VRI is mogelijk vanuit deze kast. Belangrijke onderdelen van de VRI vormen de procesbesturing en de regelapplicatie. De procesbesturing zorgt voor de aansturing en bewaking van de lampen, het ontvangen van detectie informatie en het bewaken van de detectoren en voor het bewaken op diverse garantietijden. De regelapplicatie is het 'brein' van de VRI. De regelapplicatie bepaalt wanneer welke richting naar groen, geel of rood gestuurd moet worden. De procesbesturing en de regelapplicatie worden gecompileerd tot één stuk software dat als één geheel in de VRI wordt geladen.

De VRI is veelal verbonden met een verkeersmanagementsysteem voor het uitvoeren van technisch en verkeerskundig beheer. Het verkeersmanagementsysteem kent de actuele status en storingen van de VRI. De wegbeheerder kan parameterwijzigingen doorvoeren vanuit het verkeersmanagementsysteem. Het verkeersmanagementsysteem kan gevoed worden met huidige beschikbare (real-time) verkeersinformatie vanuit de VRI (bijv. VLOG) en vanuit NDW.



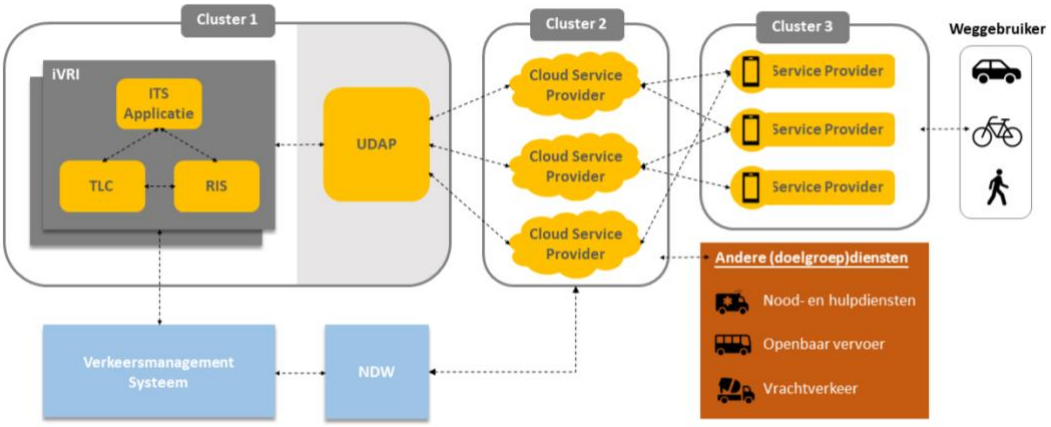
Figuur 1: VRI-architectuur en keten

2.2.2 iVRI-architectuur en functionele keten

Met de komst van de iVRI maakt deze onderdeel uit van een dataketen van en naar de weggebruiker. Met weggebruiker wordt in dit kader zowel een connected persoon (met gebruik van bijvoorbeeld apps op de telefoon) en een connected voertuig bedoeld (waarbij de connectiviteit in-car is gebracht). Er wordt hierbij veel informatie van en naar de iVRI verstuurd. Vanuit de weggebruiker wordt richting de iVRI informatie verstuurd over zijn positie en richting, identificatie en eventueel over een prioriteitsaanvraag en additionele informatie. Vanuit de iVRI wordt richting de weggebruiker informatie verstuurd over onder andere de status van het licht, de tijd tot groen en de vormgeving van het kruispunt. Dit alleen leidt al tot een hoger veiligheidsrisico, want de weggebruiker moet ervan uit kunnen gaan dat de informatie die hij ontvangt, betrouwbaar is. Hierbij speelt de privacy wetgeving (AVG) ook een belangrijke rol.

De architectuur van de iVRI zelf lijkt op de architectuur van de VRI, maar toch bestaan hierin belangrijke verschillen. Het belangrijkste is dat alle componenten altijd van elkaar gescheiden zijn en communiceren via landelijk vastgestelde koppelvlakken. De procesbesturing is in basis nog hetzelfde als in de VRI, alleen heet deze nu TLC (traffic Light Controller). De regelapplicatie heeft nu ITS-applicatie en is nog steeds het ‘brein’ van de iVRI. Er is een derde component bijgekomen, namelijk de RIS. Dit component maakt tweerichting communicatie tussen iVRI en weggebruiker mogelijk.

De architectuur van de iVRI-keten is opgebouwd uit drie clusters. Tussen deze drie clusters stromen verkeersgegevens: van cluster 1 via cluster 2 naar cluster 3 én andersom. De keten betreft een samenwerking tussen het Ministerie van I&W, diverse regionale en lokale overheden en diverse (inter)nationale bedrijven. Deze partners werken samen aan het versnellen van de ontwikkeling en ontsluiting en inzet van verkeerslichtgegevens (cluster 1). Een tweede gezamenlijk doel is het verwerken, verrijken en verspreiden van een grote verscheidenheid aan data en deze omzetten in op maat gemaakte, real-time beschikbare datasets en informatie (cluster 2). Het derde doel is het via service providers beschikbaar maken van deze informatie voor een breed scala aan weggebruikers via hun smartphones, persoonlijke en ingebouwde navigatiesystemen, boordcomputers etc. (cluster 3). Daarnaast bestaan nog specifieke doelgroepen die van de keten gebruik maken voor het aanvragen van prioriteit bij iVRI’s. figuur 2 toont de functionele uitwerking van deze architectuur en de keten.



Figuur 2: iVRI-architectuur en keten

Kenmerken cluster 1
Cluster 1 bestaat uit de iVRI en UDAP (Urban Data Access Platform). In dit cluster wordt gewerkt aan de beschikbaarheid van data door de ontsluiting en inzet van gegevens uit verkeerslichten. Met deze informatie kan de weggebruiker beter worden geïnformeerd én kan tegelijkertijd het verkeerslicht slimmer regelen door gegevens vanuit de weggebruiker.

Kenmerken cluster 2
Cluster 2 bestaat uit Cloud Service Providers. Dit cluster heeft als gezamenlijk doel het verwerken, verrijken en verspreiden van verschillende data en deze omzetten in op maat gemaakte, real-time beschikbare datasets en informatie. De data- en clouddiensten binnen dit cluster voegen de data ook samen en combineren deze met additionele data uit zowel publieke als private bronnen.

Kenmerken cluster 3
Cluster 3 bestaat uit Service providers. De informatie wordt beschikbaar gemaakt voor een breed scala aan weggebruikers, via bijvoorbeeld smartphones, navigatiesystemen en on-board computers. Hiermee wordt bereikt dat zo veel mogelijk eindgebruikers voorzien worden van informatiediensten, ongeacht het merk, type of leeftijd van hun vervoermiddel. Tegelijkertijd zorgen de cluster 3-partijen ervoor dat informatie (zoals locatie, snelheid, rijrichting) van de eindgebruikers, via cluster 2 naar cluster 1, terechtkomt bij de iVRI, zodat de verkeerslichten met deze informatie efficiënter kunnen regelen.

Functioneel doel iVRI-keten
Functioneel heeft de keten en de datastromen door deze keten als doel het realiseren van een drietal use cases:

Use case Prioriteren
Deze use case betreft het prioriteren van doelgroepen bij verkeerslichten. Dit zijn niet alleen de nood- en hulpdiensten en het openbaar vervoer, maar ook andere doelgroepen zoals vrachtverkeer, fietsers of pelotons van voertuigen. De keuze voor welke doelgroep wordt geprioriteerd dient uit gemeentelijk beleid te volgen.

Use case Informeren
Deze use case betreft het in-car kunnen verstrekken van actuele informatie en/of adviezen vanuit de iVRI's of berekende informatie van het in-car systeem dat (deels) is gebaseerd op informatie uit de VRI's. Hierbij gaat het bijvoorbeeld om het informeren van weggebruikers over de status van de

signaalgroepen en de tijd-tot-rood en tijd-tot-groen per signaalgroep. De iVRI stuurt gegevens over vormgeving van het kruispunt (MAP-data) en gegevens over de status van de signaalgroepen en de tijd-tot-rood en tijd-tot-groen informatie per signaalgroep (SPAT-data) de wereld in. Deze informatie kan door service providers gebruikt worden om de (individuele) weggebruiker beter te informeren en adviseren, bijvoorbeeld via apps op telefoons of 'in-car' rechtsreeks via de boordcomputer in de auto. Deze informatie is ook nodig om voertuigen (meer) autonoom te kunnen laten rijden.

Use case Optimaliseren
Deze use case gaat over het optimaliseren van de afwikkeling op een of meerdere kruispunten door het beschikbaar stellen van geanonimiseerde verplaatsingsdata van weggebruikers aan de verkeersregelingen. Door de implementatie van nieuwe technieken komt informatie beschikbaar per individuele weggebruiker en ook nog eens meer gedetailleerde informatie over exacte locatie, richting en snelheid van die specifieke weggebruiker, waardoor de verkeerslichtenregeling de groentijden veel optimaler op het werkelijke verkeersaanbod kan afstemmen. Dit moet leiden tot een hogere verwerkingscapaciteit van het kruispunt, maar ook voor minder verlies-/wachttijd bij de weggebruikers.

2.2.3 iVRI ICT keten

De VRI is veelal opgenomen in een beveiligd communicatienetwerk. De opbouw van het VRI-communicatienetwerk is veelal een eigen netwerk dat via VPN-tunnels (of corporate network verbindingen of eigen privaat afgeschermd netwerk) en firewalls is afgeschermd van het internet en de buitenwereld. Via het beveiligde communicatienetwerk kan de VRI via het internet bereikbaar worden gemaakt voor derde systemen en partijen.

De (i)VRI's zijn verbonden met een verkeersmanagementsysteem ten behoeve van technisch en verkeerskundig beheer. Communicatie met de (i)VRI's met dit systeem verloopt via het IVERA-protocol. Het verkeersmanagementsysteem zorgt over het algemeen ook voor de inwinning en opslag van (streaming) V-Log data.

Soms is het VRI-communicatienetwerk ook gekoppeld met de kantooromgeving van de wegbeheerder, waardoor de VRI ook vanuit de kantooromgeving te benaderen is. Steeds vaker krijgen externe partijen (zoals onderhoudspartijen) op afstand toegang tot de VRI's waar zij onderhoud op dienen te plegen.

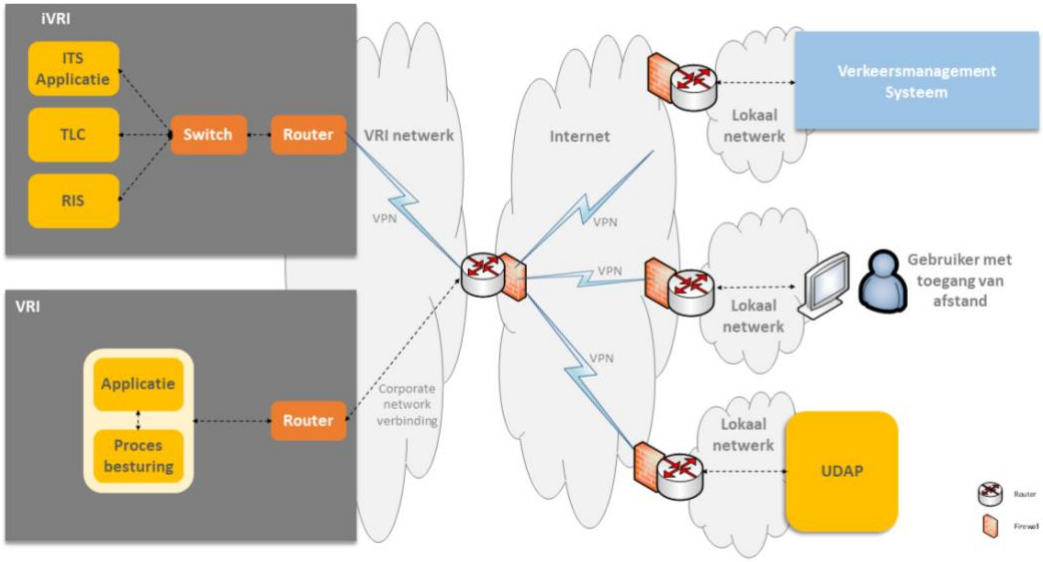
Een iVRI is daarnaast ook verbonden met UDAP in verband met de uitwisseling van iVRI-data tussen iVRI en weggebruiker (SPAT-MAP, CAM, SRM/SSM, DENM berichten. Dit betreffen Europees gestandaardiseerde berichten, de zogenaamde ETSI standaard).

De specificaties van de iVRI architectuur zijn hybride, dat wil zeggen dat deze geschikt zijn voor zowel cellulaire (4G/5G) communicatie als Wifi-P (G5) communicatie. Binnen Talking Traffic is gekozen om alleen cellulaire communicatie toe te passen. Dit houdt in dat de data de route volgt vanaf de weggebruiker (de app) via cluster 3 (de service providers), cluster 2 (de cloud service provider) naar cluster 1 (UDAP) en vervolgens naar de iVRI. Internationaal en door enkele wegbeheerders in Nederland wordt de Wifi-P route echter wel al als standaard toegepast. De Wifi-P communicatie kan worden toegepast voor rechtstreekse data uitwisseling tussen iVRI en een voertuig op basis van dezelfde gestandaardiseerde berichten.

Binnen de iVRI ICT-keten is het mogelijk om een Public Key Infratructure (PKI) met TLS certificaten toe te passen waarmee een extra laag van beveiliging ontstaat. Dit wordt in de praktijk nu in sommige gevallen toegepast bij gebruik van cloud ITS-applicaties (tussen de ITS applicatie en de TLC) en bij

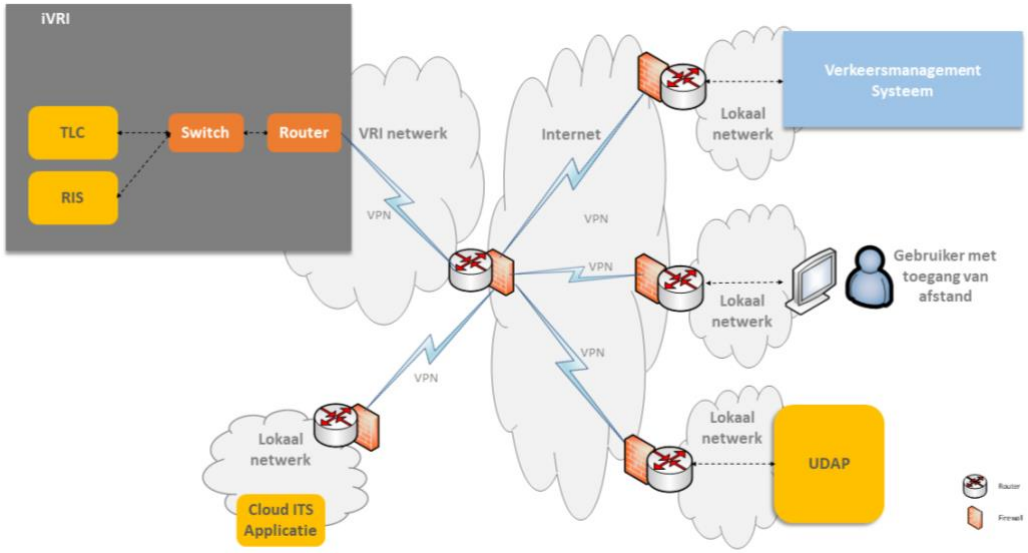
gebruik van een RIS (tussen de RIS en UDAP). Vanuit security oogpunt is het wenselijk om dit op de verbindingen tussen alle onderdelen van een iVRI toe te passen. Hiervoor dient de uitgifte en het beheer van de TLS beveiligingscertificaten landelijk nog ingeregeld te worden.

Een mogelijke (en veel voorkomende) uitwerking van de ICT-keten van een (i)VRI is in figuur 3 geschetst. Hierin is te zien dat de (i)VRI's deel uitmaken van een beveiligd VRI-netwerk waarin de verbinding naar elke (i)VRI met een VPN-verbinding of ander soort beveiligde verbinding is uitgevoerd. Het (i)VRI netwerk is gekoppeld aan andere netwerken waarin de systemen gehuisvest zijn waarmee de (i)VRI's verbonden dienen te zijn, zoals een verkeersmanagementsysteem of UDAP. Maar dit kan bijvoorbeeld ook de toegang van afstand tot de (i)VRI zijn voor de leverancier. Deze verbindingen tussen de netwerken worden over het algemeen ook met een beveiligde VPN-verbinding gerealiseerd.



Figuur 3: (i)VRI CT keten

Met de iVRI komt hier potentieel de ITS-applicatie in de cloud nog bij, zie figuur 4. Dit betekent nog een extra verbinding/schakel in de ICT keten. Deze variant is op diverse plaatsen in Nederland al operationeel. Optioneel kan ook de RIS nog in de cloud draaien, al dan niet op dezelfde locatie als de cloud ITS-applicatie. Deze variant is op dit moment in Nederland nog niet operationeel.



Figuur 4: iVRI ICT-keten me cloud ITS-applicatie

Security issues

3. Security issues (i)VRI keten

De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) heeft ‘vervoer over (hoofd)wegennet’ als een Categorie B vitaal proces binnen de vitale infrastructuur geïdentificeerd. Aangezien een (i)VRI onderdeel uitmaakt van het wegennet, is het hoogst onwenselijk dat een (i)VRI uitvalt of anders reageert als gevolg van een veiligheidslek. Door het combineren van werelden ontstaat op grote schaal (draadloze) real time communicatie tussen weggebruiker en verkeerslicht. Het uitwisselen van real time informatie vereist een koppeling tussen de systemen van de deelnemers in de keten. In zijn algemeenheid brengt het koppelen van systemen (cyber)security risico’s met zich mee. Denk bijvoorbeeld aan het bewerken van data door onbevoegden, het doven of op knipperen zetten van VRI’s of voertuigen die zich onjuist voordoen als bijvoorbeeld hulpdienst, vrachtwagen etc.

Dit hoofdstuk beschrijft de security risico’s die benoemd zijn in de gesprekken die DTV Consultants gevoerd heeft met de landelijke, regionale en lokale stakeholders en die herleid zijn uit overige aangeleverde documenten aangaande dit onderwerp. Op basis van de geïnventariseerde risico’s worden ook diverse beheersmaatregelen aangedragen, onderverdeeld naar de landelijke overheid, regionale/lokale wegbeheerders en leveranciers.

3.1 Risico inventarisatie en beheersmaatregelen

De risico inventarisatie heeft plaatsgevonden op basis van interviews met diverse wegbeheerders, het Ministerie van I&W en een iVRI-leverancier en op basis van literatuurstudie van diverse openbaar beschikbare en aangeleverde documenten. In **Error! Reference source not found.**is een overzicht opgenomen welke gesprekken met welke partijen en personen hebben plaatsgevonden.

Om ordening aan te brengen binnen de risico’s en de bijbehorende beheersmaatregelen zijn deze onder verdeeld naar de volgende onderwerpen:

- Toegangsbeheer
- Informatiebeveiliging
- Change Management
- Incident Management
- Personeel en organisatie
- Imago

Per risico is meteen een bijbehorende beheersmaatregel benoemd en voor wie deze beheersmaatregel bestemd is (lokale/regionale wegbeheerder, landelijke overheid of leverancier). In **Error! Reference source not found.**zijn de beheersmaatregelen samengevat per type stakeholder.

3.1.1 Toegangsbeheer

Onder toegangsbeheer verstaan we onder andere fysieke en digitale toegang, wachtwoordbeleid én mandaatbeheer. Overheden hebben hier veelal wel beleid op binnen de eigen organisatie, maar dit wordt ten aanzien van de (i)VRI lang niet altijd gevolgd of toegepast.

Fysieke toegang
Fysiek sleutelbeheer is niet overal goed ingeregeld en sleutelplannen ontbreken. Uit de gesprekken blijkt dat niet alle wegbeheerders weten hoeveel sleutels er zijn, wie de sleutels in bezit hebben en wie er gebruikt van maakt. Ook wordt niet altijd onderscheid gemaakt wie toegang hebben tot

verschillende compartimenten van de regelautomaat. Ook worden vaak dezelfde sloten gebruikt voor verschillende compartimenten, voor verschillende VRI's en zelfs voor verschillende wegbeheerders. Het risico bestaat hierbij dat onbevoegden in de VRI's kunnen en dat er onvoldoende zicht is wanneer bevoegde personen in de automaat kunnen. Het risico is dat lokaal geregeld (gefixeerd) kan worden, dat de VRI op knipperen of gedoofd gezet kan worden (beiden met de kans op grote verstoringen van de verkeersafwikkeling), dat onbevoegden op het data netwerk kunnen komen en het netwerk kunnen hacken (beiden met de kans op data lekken of security issues).

Verder blijkt er onvoldoende aandacht voor fysieke toegang tot ruimtes (zoals locatie met VRI-servers) en apparatuur (bijvoorbeeld computer/laptops zonder automatische vergrendeling).

Beheersmaatregelen:

- Wegbeheerder: Maak beleid op het gebied van fysiek toegangsbeheer van de VRI, ruimtes gerelateerd aan de VRI-toegang en apparatuur en laat dit bestuurlijk vaststellen.
  - Gebruik de BIO hoofdstuk 11 als leidraad.
  - Wie mag in (welk deel van welke) automaat? Wie beheert de sleutels en met welke voorwaarden worden sleutels gedeeld (denk hierbij ook de mogelijkheden van digitale sloten). Unieke sloten per wegbeheerder of per VRI?
- Wegbeheerder: Implementeer het beleid op gebied van fysiek toegangsbeheer en in de processen in de organisatie.

Digitale toegang

Net als fysieke toegang is de digitale toegang niet altijd goed geregeld. Wie heeft tot welk onderdeel toegang en onder welke voorwaarden? Soms komt het voort uit een gebrek aan beleid, soms komt het voort uit het niet naleven van beleid. Het risico is dat onbevoegde personen toegang hebben de VRI-omgeving – zoals een netwerkmanagementsysteem – en hier ongewenste wijzigingen kan aanbrengen. Hiermee kan bijvoorbeeld parameterwijzigingen doorgevoerd worden of een VRI op knipperen of gedoofd gezet worden (met de kans op grote verstoringen van de verkeersafwikkeling).

Beheersmaatregelen:

- Wegbeheerder: Maak beleid op het gebied van digitaal toegangsbeheer om inloggen op de VRI door ongewenste personen of systemen te voorkomen. Denk daarbij aan het inloggen in de automaat op straat, maar ook digitaal inloggen op afstand. Laat dit beleid bestuurlijk vaststellen.
  - Gebruik de BIO hoofdstuk 9 als leidraad.
  - Maak toegang persoonsgebonden, tijdelijk en op basis van need to have én gebruik two-factor authenticatie.
- Wegbeheerder: Implementeer het beleid op gebied van digitaal toegangsbeheer en in de processen in de organisatie.

Wachtwoordbeleid

Verder blijkt uit de gesprekken dat er niet altijd een wachtwoordbeleid is of deze niet wordt nageleefd. Ook hier gaat het om toegang tot de instellingen in de automaat (via het bedieningspaneel) zowel in de automaat op straat als via digitale toegang vanaf afstand. Zwakke wachtwoorden zijn makkelijk te kraken, waardoor ongewenste personen toegang kunnen krijgen tot de VRI's. Daarnaast is bekend dat VRI's (wegbeheerder overstijgend) toegankelijk zijn met dezelfde standaard gebruikersnaam en

wachtwoord. Verschillende wachtwoorden voor verschillende apparatuur en software is vanuit security oogpunt gewenst.

Beheersmaatregelen:
- Wegbeheerder: Maak wachtwoordbeleid en implementeer deze in de organisatie.
  - Gebruik de BIO paragraaf 9.3 en 9.4 als leidraad.

Toegang tot centrale verkeersmanagementsystemen
Bij meerdere wegbeheerders is geconstateerd dat er geen overzicht is van welke accounts actief zijn in het systeem en welke bijbehorende rechten per account zijn ingesteld en of de juiste personen de juiste rechten hebben. Het risico hierbij bestaat dat onbevoegde personen toegang krijgen tot het verkeersmanagementsysteem en VRI's kunnen bedienen en wijzigen. Hiermee kan bijvoorbeeld parameterwijzigingen doorgevoerd worden of een VRI op knipperen of gedoofd gezet worden (met de kans op grote verstoringen van de verkeersafwikkeling).

Daarnaast wordt lang niet altijd met een two-factor authenticatie ingelogd, maar enkel met een gebruikersnaam en wachtwoord. Hiermee wordt het onbevoegd inloggen (als gevolg van hack of het afkijken van het wachtwoord) eenvoudiger gemaakt. Indien two-factor authenticatie niet mogelijk is, stelt de BIO hogere eisen aan het wachtwoord en moet het wachtwoord minimaal halfjaarlijks worden vernieuwd. Het risico is dat onbevoegde personen toegang krijgen tot het verkeersmanagementsysteem en VRI's kunnen bedienen en wijzigen.

Ook is geconstateerd dat veelal geen einddatum op accounts binnen verkeersmanagement systemen is ingesteld. Hierdoor kunnen bijvoorbeeld medewerkers die reeds uit dienst zijn nog steeds toegang krijgen. Of kunnen medewerkers van adviesbureaus die voor een tijdelijke opdracht toegang kregen, nog steeds toegang hebben. Het risico is dat onbevoegde personen toegang krijgen tot het verkeersmanagementsysteem en VRI's kunnen bedienen en wijzigen.

Beheersmaatregelen:
- Wegbeheerder: Besteedt in het beleid op het gebied van digitaal toegangsbeheer ook aandacht aan de systemen die direct of indirect invloed hebben op de VRI's. Denk aan bijvoorbeeld netwerkmanagementsystemen en opslag van VRI-data.
  - Maak toegang persoonsgebonden, tijdelijk en op basis van need to have én gebruik two-factor authenticatie.

Toegang tot UDAP
NDW is contractbeheerder van UDAP en heeft hiermee een verantwoordelijkheid voor het toegangsbeheer tot UDAP. NDW handhaaft de aansluitvoorwaarden om een iVRI op UDAP toe te voegen. Maar NDW beheert ook de accounts van organisaties en admin-gebruikers van wegbeheerders in UDAP en de bijbehorende rechten. Een wegbeheerder heeft daarnaast zelf de mogelijkheid om (als admin-gebruiker) extra personen als gebruiker in UDAP toe te voegen binnen zijn organisatie. Geconstateerd is dat niet elke wegbeheerder overzicht heeft van welke accounts actief zijn in het systeem en welke bijbehorende rechten per account zijn ingesteld en of de juiste personen de juiste rechten hebben. Ook worden toegangsrechten zelden voorzien van een einddatum. Vanuit UDAP worden ook gebruikers toegevoegd aan wegbeheerdersaccounts. Het risico is dat onbevoegde personen toegang krijgen tot UDAP en gegevens van iVRI's kunnen inzien, instellingen van iVRI's kunnen wijzigen en iVRI's hiermee (onterecht) van UDAP kunnen afsluiten. Hierdoor wordt de dataketen onderbroken en functioneren de use cases niet meer. Dit kan gevolgen

hebben voor de veiligheid en doorstroming op het kruispunt en kan potentieel commerciële gevolgen hebben.

Beheersmaatregelen:

- Wegbeheerder: Besteedt in het beleid op het gebied van digitaal toegangsbeheer ook aandacht aan de toegang(voorwaarden) voor UDAP.
  - Maak toegang tijdelijk en op basis van need to have.
  - Maak gebruik van de functie van UDAP voor persoonsgebonden toegang, two-factor authenticatie en toegang op basis van vertrouwde IP-adressen.

Credential management VRI

Het huidige systeem van autorisatie van inloggen in het bedieningspaneel van de VRI is niet schaalbaar. Er is behoefte aan verschillende niveaus van toegang en autorisatie voor verschillende rollen (toegang tot bepaalde delen van de applicatie, inlogniveaus met lees- of wijzingsrechten, eindtijden op accounts). Doordat dit huidige systeem van inloggen niet schaalbaar is worden vaak dezelfde wachtwoorden toegepast over meerdere VRI's en meerdere wegbeheerders heen. Dit heeft als risico dat onbevoegde personen in de VRI kunnen inloggen en de VRI ongeoorloofd kunnen bedienen en wijzigen.

Beheersmaatregelen:

- Leverancier: het credential management van VRI's (radicaal) anders inrichten. Dit moet minimaal landelijke schaalbaar worden. Mogelijk dat toegang centraal en niet meer lokaal geregeld moet worden. Er dient gewerkt te worden naar een leverancier onafhankelijke oplossing.
  - Gebruik de BIO hoofdstuk 09 als leidraad.

Netwerkscheiding VRI-communicatienetwerken

VRI-netwerken zijn niet altijd gescheiden. Het is belangrijk om te bepalen welke partij/persoon/systeem toegang heeft/mag hebben tot welk deel van het netwerk. Mogen zij toegang hebben tot alle VRI's of een subset van VRI's? Mogen zij toegang hebben tot alle onderdelen van de VRI, of alleen specifieke componenten? Daarnaast blijkt dat vanuit een VRI ook andere VRI's in het netwerk benaderd kunnen worden. Dit heeft als risico dat onbevoegde personen in de VRI kunnen inloggen en de VRI kunnen bedienen en wijzigen.

Beheersmaatregelen:

- Wegbeheerder:
  - Maak voor de VRI's een gescheiden communicatienetwerk waarvoor alleen bevoegde personen en geauthentiseerde apparatuur toegang heeft.
  - Maak het onmogelijk om default vanuit een VRI andere VRI's te benaderen. Deze toegang dient bewust toegekend te worden.
  - Zorg ervoor dat leveranciers alleen tot de VRI onderdelen toegang hebben, waar dit noodzakelijk is.
  - Zorg dat toegang voor gebruikers is gebonden aan bloktijden, om controle op de toegang tot het netwerk te kunnen behouden.
  - Gebruik de BIO hoofdstuk 9 en 13 als leidraad.

Mandaatbeheer
Het is niet altijd duidelijk wie binnen een organisatie gerechtigd is om toegang te geven tot systemen en/of objecten en met welke rechten. Bij wegbeheerders is dit in de praktijk veelal de VRI-beheerder. Maar het is niet altijd duidelijk of deze VRI-beheerder conform het mandaatbesluit binnen zijn organisatie hier wel toe gemachtigd is. Dit heeft als risico dat een medewerker een andere persoon onbevoegd toegang heeft tot systemen.

Beheersmaatregelen:
- Wegbeheerder: Besteedt in het beleid op het gebied van zowel fysiek als digitaal toegangsbeheer ook aandacht aan mandaatbeheer. Wie is de bevoegde functionaris om gebruikers en gebruikersrechten toe te kennen en heeft deze beschikking over beleidsregels over het wel/niet toekennen van rechten.
    - Gebruik de BIO hoofdstuk 9 als leidraad.

3.1.2 Informatiebeveiliging

Informatiebeveiliging is het proces van vaststellen van de vereiste beveiliging van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen. Binnen dit kader zijn verschillende risico's geconstateerd.

Verantwoordelijk over data in de keten
Er heerst bij veel wegbeheerders onduidelijkheid over wie verantwoordelijk is voor de data in de keten en/of wie eigenaar is van de data in de keten. Hierdoor is het onduidelijk welke partij (welke) maatregelen op welke plek in de keten dient te treffen. Het risico is dat de data en informatie in de keten niet voldoende beveiligd wordt. Daarnaast bestaat bij wegbeheerders onduidelijkheid over de aansprakelijkheid bij het tonen van verkeerde informatie in de apps van de service providers.

Beheersmaatregelen:

- Wegbeheerder: De wegbeheerder heeft een zorgplicht waardoor hij ervoor kan zorgen dat hij niet aansprakelijk gesteld kan worden als er bijvoorbeeld ongevallen ontstaan door (foutieve) informatie uit de iVRI. De wegbeheerder moet zijn best doen (zorgplicht) om ervoor te zorgen dat er geen onjuiste gegevens verstuurd worden. Dit kan hij doen door:
  - Het implementeren van de BIO op het (i)VRI systeem.
  - Gebruik te maken van enkel gecertificeerde producten die voldoen aan de CROW richtlijnen en door te voldoen aan de geldende NEN-normen.
  - Gebruik te maken van landelijke uniforme bestekteksten en onderhoudscontracten voor de iVRI bij de aanbesteding van iVRI's.
  - Door structureel te (laten) monitoren op de kwaliteit van de iVRI-data middels het controleren van de KPI's in UDAP en bovenal te acteren bij afwijkingen.
- Wegbeheerder: Verantwoordelijkheid wegbeheerder voor borgen verwerken data die (mogelijk) persoonsgegevens bevatten: afsluiten van verwerkersovereenkomsten met leverancier(s) van iVRI componenten
- Landelijke overheid: Met consolidatie iVRI-architectuur de volgende zaken aanpakken:
  - Nieuwe aansluitvoorwaarden Cloud Service providers (cluster 2 partijen) om op UDAP aan te mogen sluiten. Deze partijen worden gecertificeerd. Marktpartijen krijgen hiermee ook een zorgplicht voor het op een veilige manier leveren van correcte data. C2 partijen zijn verantwoordelijk voor afsluiten overeenkomsten van de op hun aangesloten partijen (Service Providers, cluster 3 partijen).
  - Eigendom van data duidelijk vastleggen in overeenkomsten met de aangesloten partijen en wat wel en niet toegestaan is om te doen met de data door andere partijen anders dan de eigenaar.
- Wegbeheerder: Gebruik de eisen in BIO hoofdstuk 05 en 06 als leidraad.

Toepassing van Public Key Infrastructure (PKI) / TLS

Binnen de iVRI-keten wordt nog maar in beperkte mate gebruik gemaakt van PKI/TLS-certificaten. De belangrijkste reden hiervoor is dat de uitgifte van de certificaten nog niet goed is geregeld over de hele keten. Slechts op onderdelen binnen de keten (bijvoorbeeld tussen UDAP en de RIS en in sommige gevallen tussen een cloud ITS-applicatie en de lokale TLC en RIS) wordt dit wel al toegepast. Dit heeft als risico dat de verbindingen tussen systemen minder goed beveiligd zijn, wat weer leidt tot een hoger risico van inbreuk op de verbindingen en daarmee een verslechterde informatiebeveiliging.

Beheersmaatregelen:

- Landelijke overheid: Landelijk inregelen van het aanstellen van de Root Certificate Authority voor uitgifte en beheer van TLS certificaten in de iVRI data keten en alle bijbehorende systemen.
  - Gebruik de BIO hoofdstuk 10 als leidraad.

Delen van IVERA-formulieren/iVRI koppelvlak configuratieformulieren

Geconstateerd wordt dat wegbeheerders en leveranciers de formulieren nog per e-mail versturen, waarbij in de formulieren gevoelige informatie als gebruikersnamen en wachtwoorden zijn ingevuld. Dit heeft als risico dat formulieren (al dan niet bewust) naar onbevoegde personen gestuurd kunnen worden en dat de gegevens in deze e-mails onderschept of gehackt kunnen worden. Dit kan ertoe leiden dat onbevoegde personen toegang krijgen tot de VRI en de VRI kunnen bedienen en wijzigen, met mogelijke negatieve gevolgen voor de verkeersveiligheid en doorstroming.

Beheersmaatregelen:

- Wegbeheerder: Verstuur nooit formulieren met gevoelige informatie per mail.
  - Alternatief is het gebruikmaken te maken van afgeschermde omgevingen zoals sharepoint waar alleen geautoriseerde personen toegang tot hebben.
- Landelijke overheid: Digitaliseren en online brengen iVRI koppelvlak configuratie formulieren. Met rechten toegang geven op VRI's en deelrechten op onderdelen binnen formulieren, waaronder wachtwoorden. Bij voorkeur in UDAP, hier wordt al veel van de informatie geconfigureerd/opgeslagen die in het formulier terecht dient te komen. Voorkomen van dubbel opslaan en minder foutgevoelig. Middels rechten toegang geven aan personen tot bepaalde onderdelen van de formulieren.
- Wegbeheerder: Gebruik de eisen in BIO hoofdstuk 05 en 06 en 10 als leidraad.

3.1.3 Change management

Change management, ofwel wijzigingsbeheer, betreft veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging. Deze behoren te worden beheerst. Change management draagt er zorg voor dat wijzigingen op de ICT-infrastructuur (ICT-middelen en -diensten) efficiënt en effectief worden doorgevoerd met zo min mogelijk verstoring van de kwaliteit van de dienstverlening, zodat deze dienstverlening blijft voldoen aan de eisen die hieraan zijn gesteld.

Software updates

Software updates worden, mede vanuit security oogpunt, steeds belangrijker. Software is gevoelig voor virussen en beveiligingslekken. Software updates gelden voor allerlei onderdelen binnen een (i)VRI, denk aan (niet uitputtend) operating systems, ITS applicaties, RIS applicaties, TLC applicaties, firmware van alle componenten, waaronder ook de router en de UPS. Bij eigen (prioritaire) software van leveranciers kan dit volgens de leveranciers over het algemeen goed ingeregeld worden, want dit heeft de leverancier namelijk zelf in de hand. Problematischer wordt dit bij door de leverancier toegepaste embedded systemen in de VRI. Veel technologie (denk aan operating systeem, processors etc.) wordt door leveranciers ingekocht. De leverancier is hierbij afhankelijk van deze leverende partijen voor het verzorgen van deze updates. De leveranciers geven aan dat het lastig is voor hun om hier doorheen te breken. Daarnaast zijn de eisen per type software applicatie anders.

Om software updates op grote schaal en hoogfrequent mogelijk te maken, geldt dat de technische infrastructuur hiervoor correct ingericht moet zijn (de leverancier moet toegang hebben tot alle onderdelen van de VRI waarvoor hij verantwoordelijk is voor de software updates) en dat de bijbehorende processen bij zowel de wegbeheerders als de leveranciers opgesteld en geïmplementeerd dienen te zijn en opgevolgd dienen te worden. Vanuit het oogpunt van verkeersveiligheid is het belangrijk om zekerheden in te bouwen voor het geval een software update niet correct verloopt. Het mag niet zo zijn dat een VRI niet meer regelt of foutieve data verstuurt vanwege een foutieve software update.

Op basis van de gesprekken met wegbeheerders en leveranciers lijkt het met de huidige stand van de techniek onmogelijk om alle onderdelen met (embedded) software van een VRI (zonder vervangen) 15 jaar up-to-date te houden. Dit heeft als risico dat bepaalde onderdelen niet voldoen aan de beveiligingseisen zoals deze door de BIO gesteld worden en daarmee gevoelig zijn voor beveiligingslekken en hacken.

Beheersmaatregelen:

- Leverancier en wegbeheerder: bepaal gezamenlijk de restrisico's van het beperkt kunnen updaten van de software op embedded systemen en bepaal de beheersmaatregelen die nodig zijn om deze restrisico's als geaccepteerd te beschouwen.
- Wegbeheerder: Maak beleid op het gebied van software updates voor (i)VRI's inclusief het beheer hierop.
    - Gebruik de eisen in BIO hoofdstuk 12 als leidraad.

3.1.4 Incident management

Incident management is een proces dat een belangrijk instrument is bij het indammen van schade en voorkomen van erger als er informatiebeveiligingsincidenten optreden. Het hebben van een goed lopend incidentmanagementproces is cruciaal om schade voor de bedrijfsprocessen te beperken. Het proces bestaat uit het tijdig identificeren en oplossen, en het achteraf leren van een incident, zodat de impact laag en kans op herhaling minimaal is.

Draaiboek incident management
Geconstateerd is dat veel wegbeheerders als organisatie geen draaiboeken ter beschikking hebben of niet weten of een dergelijk draaiboek beschikbaar is, waarin is vastgelegd hoe te handelen bij uitval van (delen) van de VRI-keten of bij cyber security incidenten (zoals een hack of datalek). Het risico is dat incidenten niet snel genoeg verholpen worden en het systeem langer aan bedreigingen bloot staat.

Beheersmaatregelen:

- Wegbeheerder: Gebruik de VNG 'Handreiking Incident- en response management' voor de implementatie van de betreffende eisen uit de BIO omtrent cyber security incident management.
    - Wegbeheerder: Gebruik de eisen in BIO hoofdstuk 16 als leidraad.

Aansluitvoorwaarden
De huidige contracten vanuit het Ministerie van I&W met Talking Traffic cluster 2 partijen (de cloud service providers) zijn formeel verlopen. Op dit moment zijn nog geen nieuwe contracten met bijbehorende aansluitvoorwaarden aanbesteed en afgesloten. Dit betekent dat er geen vigerende afspraken, contracten en overeenkomsten zijn tussen verschillende overheids- en marktpartijen in de iVRI-dataketen. Het risico is dat er geen (actief) toezicht meer wordt gehouden op de implementatie van de BIO-eisen bij deze dienstenleveranciers. Dit kan mogelijk leiden tot een verslechtering van de beveiliging van data en systemen en daarmee leiden tot inbreuk op privacy (data lek) en security issues.

Beheersmaatregelen:

- Landelijke overheid: Met consolidatie iVRI architectuur de volgende zaken meenemen:
  - Nieuwe aansluitvoorwaarden Cloud Service providers (cluster 2 partijen) om op UDAP aan te mogen sluiten. Deze partijen worden gecertificeerd. Marktpartijen krijgen hiermee ook een zorgplicht voor het op een veilige manier leveren van correcte data. C2-partijen zijn verantwoordelijk voor afsluiten overeenkomsten van de op hun aangesloten partijen (Service Providers, cluster 3 partijen).
  - Eigendom van data duidelijk vastleggen in overeenkomsten met de aangesloten partijen en wat wel en niet toegestaan is om te doen met de data door andere partijen anders dan de eigenaar.

3.1.5 Personeel en organisatie

Veilig personeel

Uit de inventarisatie blijkt dat het regelmatig voorkomt dat personeel geen kennis heeft van en/of niet werkt volgens de diverse procedures rondom informatiebeveiliging zoals vastgelegd in het kwaliteitsmanagement systeem van de betreffende organisatie (welke gebaseerd is om de eisen uit de ISO27001/27002 en/of BIO) en/of deze procedures niet of niet geheel volgt.

Beheersmaatregelen:

- Wegbeheerders en leveranciers: Bewustwording creëren bij medewerkers voor alle bestaande en aanwezige procedures rondom informatiebeveiliging.
- Wegbeheerder: Gebruik de eisen in BIO hoofdstuk 07 als leidraad.

3.1.6 Imago

Imagoschade

Uit de gesprekken met de wegbeheerders blijkt dat met name de politiek gevoelig is voor imagoschade. De imago schade bestaat uit het beeld dat een overheidsorganisatie zijn zaken niet op orde heeft en daarop aangekeken en/of aangesproken wordt. Deze (bestuurlijke) imagoschade kan opgelopen worden doordat door de betreffende overheid niet wordt voldaan aan bepaalde eisen op het gebied van (informatie)beveiliging of beveiliging van de netwerken, waardoor incidenten ontstaan die directe of indirecte gevolgen hebben voor bijvoorbeeld medewerkers, inwoners of weggebruikers. Denk aan het uitvallen van een VRI waardoor er congestie in de stad ontstaat of waardoor wellicht zelfs een ongeval ontstaat.

Beheersmaatregelen:

- Wegbeheerder: Zorg dat bij aanbestedingen altijd de BIO wordt voorgeschreven, maar zorg in samenspraak met de leverancier(s) dat de eisen concreet en van toepassing zijn op het gevraagde in de aanbesteding, zodat de leverancier ook de mogelijkheid heeft om hier op een goede wijze aan te voldoen.
- Wegbeheerder: Gebruik de eisen in BIO hoofdstuk 07 en 15 als leidraad.

3.1.7 Overall

Misschien wel de belangrijkste constatering uit de gesprekken met de wegbeheerders en de CISO's is dat de huidige (i)VRI's (inclusief het bijbehorende data netwerk) niet voldoen aan de BIO én dat met de eisen die nu worden gesteld bij de aanschaf en het onderhoud van nieuwe (i)VRI ook niet wordt voldaan aan de eisen uit de BIO. Wegbeheerders missen nu een praktische vertaling van de BIO voor het thema (i)VRI's die zij kunnen gebruiken bij aanbestedingen. Geadviseerd wordt om dit regionaal (of landelijk) op te pakken, zodat alle wegbeheerders in de regio hier baat bij hebben.

Daarnaast is – bijvoorbeeld door Provincie Noord-Brabant maar ook door gemeente Amsterdam – geconstateerd dat wegbeheerders niet zomaar de BIO-eisen 1-op-1 kunnen toepassen bij een uitvraag voor (i)VRI's. De BIO is vooral gericht op kantoorautomatisering en veelal te hoog over voor de (i)VRI. Dit pleit ook voor een landelijke vertaling van de BIO voor het thema (i)VRI's. Daarnaast wordt getwijfeld of VRI-leveranciers momenteel wel kunnen voldoen aan alle BIO-eisen (bijvoorbeeld mede door afhankelijkheden van leveranciers van subonderdelen). Het risico hierbij is dat een wegbeheerder geen inschrijvingen ontvangt bij aanbestedingen. Afgevraagd dient te worden of het niet constructiever is om samen met de leveranciers een transitiepad te bespreken hoe markt en overheid over een aantal jaar gezamenlijk wel BIO-compliant zijn. Dit geldt voor zowel nieuwe aanbestedingen en contracten als voor het aanpassen van lopende contracten. Het voorstel is om de dialoog aan te gaan met de leveranciers over hoe je op een praktische manier de BIO-eisen vertaald naar de VRI-wereld en bijvoorbeeld welke restrisico's worden geaccepteerd.

De ervaring leert echter ook dat dergelijke landelijke uitvoeringsacties vaak veel tijd kosten, lang duren en moeilijk te organiseren zijn. De noodzaak om binnen enkele jaren adequate maatregelen te treffen is echter wel aanwezig. De vraag is daarom of de Brabantse wegbeheerders hierop willen wachten. Mogelijk kunnen de Brabantse wegbeheerders gezamenlijk initiatief starten om (in overleg en samenspraak met de markt) tot concrete BIO eisen en een bijbehorend implementatieplan te komen. Mogelijk dat dit daarna versneld tot een landelijke standaard kan leiden.

Beheersmaatregelen:

- Wegbeheerder of landelijke overheid: Stel een landelijke handreiking BIO-eisen VRI's voor toepassing bij aanbestedingen door wegbeheerders op. Dit creëert eenduidigheid in eisen en voor het bepalen van geaccepteerde risico's. Voor leveranciers is dit een goede basis om hun producten en diensten (en processen) op in te richten. Voor wegbeheerders is het een vorm van 'garantie' dat hiermee security conform eisen BIO zijn gewaarborgd. In het kader van de BIO dient een (i)VRI gezien te worden als een 'Network endpoint device' aangesloten op een IT besturingsnetwerk dat geplaatst is in een straatkast.
  - Het is aan te bevelen nog wel ruimte te laten voor leveranciers/marktpartijen om zich te kunnen onderscheiden. Aandacht voor het monitoren en controleren van zowel techniek (is versie software up-to-date) en organisatorisch/proces. Voorbeeld uitwerking BIO-eisen voor (i)VRI van gemeente Amsterdam kan hiervoor als basis/vertrekpunt fungeren.
- Wegbeheerders en landelijke overheid: Bewustwording creëren bij zowel wegbeheerders als marktpartijen voor noodzaak aanpassingen aan producten, diensten en processen om secure te worden en om te voldoen aan huidige regelgeving.
- Regio/wegbeheerder en leveranciers: het in samenspraak met leveranciers uitvoeren van pen-testen om kwetsbaarheden bloot te leggen. Deze testen dienen op drie niveaus uitgevoerd te worden:
  - De fysieke VRI
  - Het netwerk
  - Overige applicaties

  Ieder rapport van de pen-test bespreken met de leveranciers. Wegbeheerders stellen samen met markt een Plan van Aanpak op hoe de aspecten op gebied van security, waar nu niet conform BIO aan wordt voldaan, aangepakt worden en op welke termijn. Hierbij wordt gezamenlijk bepaald wat de kosten zijn en hoe de verdeling van de kosten plaatsvindt tussen wegbeheerders en leveranciers. Zowel wegbeheerders als leveranciers dienen hierin in redelijkheid en billijkheid hun aandeel nemen. Dit betekent ook dat wegbeheerders in overleg met de leveranciers de huidige contracten open moeten breken en moeten aanpassen naar de huidige eisen.
- Leverancier: om ook BIO-gecertificeerd te worden is het de aanbeveling om de BIO-eisen mee te nemen in ISO27001-certificering. Dit kan door de 43 aanvullende artikelen uit BIO aan de ISO-certificering toe te voegen en hier jaarlijks op te laten auditen. Zo wordt het mogelijk om vanuit de marktpartij/leverancier elk jaar een 'BIO In control' verklaring aan de betrokken wegbeheerders af te geven.

3.2 Fasering van beheersmaatregelen

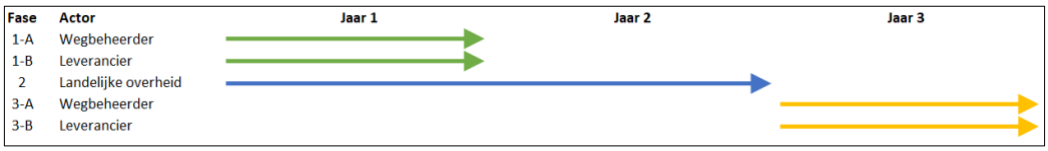
Zoals in hoofdstuk **Error! Reference source not found.** is beschreven dienen wegbeheerders als overheidsorganisatie te voldoen aan de richtlijnen ten aanzien van informatiebeveiliging voor de gehele overheid, vastgelegd in de BIO. Iedere wegbeheerder kan binnen deze kaders uiteindelijk zelf bepalen of, hoe en in welke mate aan alle eisen van de BIO voldaan gaat worden (binnen de eigen organisatie en voor de gecontracteerde dienstenleveranciers) om alle risico's te mitigeren. Daarom is het belangrijk om de risico's te prioriteren en te bepalen welke risico's wel of niet geaccepteerd zijn en voor hoe lang. De wegbeheerder dient dus de restrisico's in te schatten. Deze inschatting van geaccepteerder risico's kan per wegbeheerder anders zijn. En zijn dan dus ook andere beheersmaatregelen nodig. Hoe hoger de inzet op beveiliging, hoe lager het risico maar hoe hoger de kosten. Hier dient elke wegbeheerder de juiste balans in te vinden. Dit valt daarmee ook samen met de kosten-baten afweging voor het beheersen van de risico's.

Omdat het naar verwachting niet mogelijk is om alle beheersmaatregelen in één keer te implementeren, is het wenselijk een fasering aan te brengen. In deze paragraaf is een voorstel gedaan voor deze fasering van beheersmaatregelen naar logische onderwerpen, waarbij gestart wordt met de implementatie van maatregelen in fase 1 en geëindigd wordt met de maatregelen die behoren bij fase 3. Bij elke opvolgende fase geldt dat de maatregelen uit de voorgaande fase(s) onverminderd van kracht blijven.

Voorstel fasering beheersmaatregelen:

- Fase 1-A: Wegbeheerders implementeren zoveel mogelijk 'quick win' beheersmaatregelen (zie checklist in **Error! Reference source not found.**). Hiermee kan het security niveau op korte termijn op relatief eenvoudige wijze aanzienlijk verhoogd worden. Tevens wordt hiermee een eerste stap gezet om BIO compliant te worden.
- Fase 1-B: Leveranciers implementeren zoveel mogelijk 'quick win' beheersmaatregelen (zie checklist in **Error! Reference source not found.**). Hiermee kan het security niveau op korte termijn op relatief eenvoudige wijze aanzienlijk verhoogd worden. Tevens wordt hiermee een eerste stap gezet om BIO compliant te worden.
- Fase 2: De landelijke overheid stelt de benodigde landelijke richtlijnen op (zie checklist in **Error! Reference source not found.**).
- Fase 3-A: Wegbeheerders passen de landelijke richtlijnen uit Fase 2 toe en implementeren de resterende beheersmaatregelen om BIO compliant te worden (zie checklist in **Error! Reference source not found.**).
- Fase 3-B: Leveranciers passen de landelijke richtlijnen uit Fase 2 toe en implementeren de resterende beheersmaatregelen om volledig BIO compliant te worden (zie checklist in **Error! Reference source not found.**).

Hierbij geldt dat fases 1-A en 1-B in ieder geval parallel aan elkaar uitgevoerd kunnen worden. Fase 2 kan ook grotendeels gelijktijdig met fase 1 uitgevoegd worden. Fases 3-A en 3-B starten nadat fases 1 en 2 zijn afgerond (zie figuur 5). Tevens geldt dat sommige beheersmaatregelen in een meer eenvoudigere uitvoering in fase 1 op korte termijn kunnen worden uitgevoerd en in een uitgebreidere, definitieve wijze in fase 2 en/of 3.



Figuur 5: Visualisatie fasering

Checklist beheersmaatregelen

Op basis van deze faseringen is een checklist opgesteld waarin alle in deze front paper opgenomen beheersmaatregelen naar de genoemde fases zijn opgesplitst. De checklist is in **Error! Reference source not found.**opgenomen. Deze checklist biedt een handvat voor wegbeheerders en leveranciers, maar elke wegbeheerder en leverancier bepaalt uiteindelijk zelf welke maatregelen hij in welke fase wil uitvoeren. Aan elke beheersmaatregel hangen kosten en/of consequenties voor personele inzet. De beschikbaarheid van deze financiële en personele middelen zal in de praktijk waarschijnlijk ook mede leidend zijn voor de fasering van de implementatie van de beheersmaatregelen.

Consequenties voor de wegbeheerder

4. Consequenties voor de wegbeheerder

De consequenties voor de wegbeheerder op basis van alle risico's en bijbehorende beheersmaatregelen zijn niet eenvoudig op te sommen. Op hoofdlijnen zijn de consequenties uit te splitsen naar de aspect kosten en organisatie. Maar omdat niet elke wegbeheerder op hetzelfde niveau van beveiliging en implementatie van de BIO-eisen en -controls zit, is hierop dit moment geen eenduidig antwoord op te geven. Tevens is op dit moment nog onduidelijk welk kosten gemoeid zijn met de ontwikkelingen die noodzakelijk zijn om de dienstenleveranciers BIO compliant te maken en of de overheden gaan bijdragen in de (ontwikkel)kosten hiervan. Wel brengen we in dit hoofdstuk de onderdelen in kaart die een effect kunnen hebben op de kosten en de organisatie.

4.1 Kosten

In deze paragraaf zijn de verschillende aspecten benoemd die effect hebben op zowel eenmalige kosten en jaarlijkse kosten om de security rondom (i)VRI op orde te brengen.

Eenmalige kosten

- Openbreken van de huidige contracten met leveranciers en bijdragen aan de ontwikkelkosten van iVRI-component leveranciers om up-to-date te komen met de BIO eisen.
- Kosten voor het eenmalig up-to-date brengen van het eigen areaal aan (i)VRI's.
- Kosten voor het inrichten van alle benodigde procedures en het (anders of aanvullend) inrichten van de beheerorganisatie.

Aangezien de impact van de benodigde ontwikkelingen om BIO compliant te worden nog niet bekend is (en daarmee ook niet de impact en bijbehorende kosten van het vervolgens up-to-date brengen van de VRI's), is enkel een hele grove inschatting te maken van deze kosten.

De totale ontwikkelkosten van iVRI-component leveranciers om up-to-date te komen met de BIO eisen zullen naar verwachting enkele miljoenen euro's bedragen. Hiervoor zal een verdeling van het dragen van de kosten tussen de leveranciers en de overheden afgesproken moeten worden. Mogelijk dat het Ministerie van I&W landelijk aan deze ontwikkelkosten kan bijdragen (vergelijkbaar met de initiële ontwikkeling van de iVRI in het partnership Talking Traffic), zodat alle regionale en lokale overheden hier niet ieder apart een deel aan bij hoeven te dragen.

De kosten voor het up-to-date brengen van het eigen areaal aan iVRI's kunnen naar verwachting tussen de € 10.000,- en € 30.000,- per VRI liggen, afhankelijk van de noodzaak voor het vervangen en/of updaten van software en/of hardware. Dit betekent voor een gemiddelde wegbeheerder met een areaal van 80 VRI's een kostenpost van € 800.000,- tot € 2.400.000,-. Naar verwachting zijn deze kosten niet uit de reguliere eigen exploitatie te dekken.

De kosten voor het inrichten van alle benodigde procedures en het (anders of aanvullend) inrichten van de beheerorganisatie bestaan waarschijnlijk vooral uit de inzet en/of inhuur van personeel voor deze werkzaamheden.

Jaarlijkse kosten

- Extra jaarlijkse kosten in de onderhoudscontracten met leveranciers voor werkzaamheden van leveranciers van iVRI-componenten in verband met aanvullende eisen om iVRI-componenten secure te houden conform de BIO-eisen.

Net zoals bij de eenmalige kosten is enkel een hele grove inschatting te maken van deze jaarlijkse kosten, omdat de impact als gevolg van de BIO-eisen nog niet bekend is. Een eerste inschatting is dat de jaarlijkse kosten met € 500,- tot € 2.000,- per VRI per jaar zullen stijgen. Dit betekent voor een gemiddelde wegbeheerder met een areaal van 80 VRI's een jaarlijkse extra kostenpost van € 40.000,- tot € 160.000,-. Naar verwachting zijn deze kosten niet uit de reguliere eigen exploitatie te dekken.

4.2 Organisatie

In deze paragraaf zijn de aspecten benoemd die effect hebben op de organisatie van de wegbeheerders om de security rondom (i)VRI op orde te brengen.

- Inrichten van nieuwe procedures, aanscherpen van bestaande procedures en het vervolgens hierop inrichten van de projecten- en beheerorganisatie.
- Inrichten van nieuwe procedures en het aanscherpen van bestaande procedures voor de controle van alle dienstenleveranciers conform eisen BIO en het vervolgens hierop inrichten van de projecten- en beheerorganisatie.

De kosten voor het inrichten van de projecten- beheerorganisatie en de procedures voor de controle van de dienstenleveranciers bestaan waarschijnlijk vooral uit de inzet en/of inhuur van personeel voor deze werkzaamheden (extra benodigd aantal FTE). Het aantal benodigd extra FTE is op dit moment nog niet in te schatten.

Bijlagen

Bijlage 1: Gesprekken stakeholders

Namens DTV Consultants zijn alle gesprekken met de stakeholders gevoerd door de personen zoals opgenomen in **Error! Reference source not found.**.

Organisatie	Personen	Functie
DTV Consultants	Tom Steijvers	Adviseur Smart Mobility, projectleider opstellen front-paper security VRI's
	Joost Hormann	Adviseur Smart Mobility

Tabel 1: Deelnemers DTV Consultants gesprekken met stakeholders

Met de in **Error! Reference source not found.** opgenomen stakeholders zijn in het kader van deze front-paper gesprekken gevoerd.

Organisatie	Datum	Personen	Functie
Gemeente Breda	27 januari 2022	Erik van Holten	VRI specialist
		Paul Keverkamp	CISO
Gemeente Eindhoven	01 februari 2022	Leon van den Biggelaar	VRI specialist
		Paul Menting (niet aanwezig)	CISO
		Niels Wiersma	Data specialist
Provincie Noord-Brabant	17 februari 2022	Dennis Huijbers	VRI specialist
		Peter van den Boogaard	CISO
Ministerie van I&W	1 maart 2022	Marcel Westerman	Adviseur
Vialis	15 februari 2022	Maurice Rutten	Klantmanager
		Ronald Schrama	Klantmanager, commercieel aanspreekpunt cybersecurity
		Peter Goossens	Productmanager VRI

Tabel 2: Partijen en deelnemers gesprekken met stakeholders

Bijlage 2: Beheersmaatregelen per type stakeholders

In deze bijlage zijn alle in hoofdstuk 3 benoemde beheersmaatregelen samengevat per type stakeholder (wegbeheerder, landelijke overheid en leverancier).

Regionale en lokale wegbeheerders

Beheersmaatregelen:

- Wegbeheerder: Maak beleid op het gebied van fysiek toegangsbeheer van de VRI, ruimtes gerelateerd aan de VRI-toegang en apparatuur en laat dit bestuurlijk vaststellen.
  - Gebruik de BIO hoofdstuk 11 als leidraad.
  - Wie mag in (welk deel van welke) automaat? Wie beheert de sleutels en met welke voorwaarden worden sleutels gedeeld (denk hierbij ook de mogelijkheden van digitale sloten). Unieke sloten per wegbeheerder of per VRI?
- Wegbeheerder: Implementeer het beleid op gebied van fysiek toegangsbeheer en in de processen in de organisatie.
- Wegbeheerder: Maak beleid op het gebied van digitaal toegangsbeheer om inloggen op de VRI door ongewenste personen of systemen te voorkomen. Denk daarbij aan het inloggen in de automaat op straat, maar ook digitaal inloggen op afstand. Laat dit beleid bestuurlijk vaststellen.
  - Gebruik de BIO hoofdstuk 9 als leidraad.
  - Maak toegang persoonsgebonden, tijdelijk en op basis van need to have én gebruik two-factor authenticatie.
- Wegbeheerder: Implementeer het beleid op gebied van digitaal toegangsbeheer en in de processen in de organisatie.
- Wegbeheerder: Maak wachtwoordbeleid en implementeer deze in de organisatie.
  - Gebruik de BIO paragraaf 9.3 en 9.4 als leidraad.
- Wegbeheerder: Besteedt in het beleid op het gebied van digitaal toegangsbeheer ook aandacht aan de systemen die direct of indirect invloed hebben op de VRI's. Denk aan bijvoorbeeld netwerkmanagementsystemen en opslag van VRI-data.
- Maak toegang persoonsgebonden, tijdelijk en op basis van need to have én gebruik two-factor authenticatie.
- Wegbeheerder: Besteedt in het beleid op het gebied van digitaal toegangsbeheer ook aandacht aan de toegang(voorwaarden) voor UDAP.
  - Maak toegang tijdelijk en op basis van need to have.
  - Maak gebruik van de functie van UDAP voor persoonsgebonden toegang, two-factor authenticatie en toegang op basis van vertrouwde IP-adressen.
- Wegbeheerder:
  - Maak voor de VRI's een gescheiden communicatienetwerk waarvoor alleen bevoegde personen en geauthentiseerde apparatuur toegang heeft.
  - Maak het onmogelijk om default vanuit een VRI andere VRI's te benaderen. Deze toegang dient bewust toegekend te worden.
  - Zorg ervoor dat leveranciers alleen tot de VRI onderdelen toegang hebben, waar dit noodzakelijk is.
  - Zorg dat toegang voor gebruikers is gebonden aan bloktijden, om controle op de toegang tot het netwerk te kunnen behouden.
  - Gebruik de BIO hoofdstuk 9 en 13 als leidraad.
- Wegbeheerder: Besteedt in het beleid op het gebied van zowel fysiek als digitaal toegangsbeheer ook aandacht aan mandaatbeheer. Wie is de bevoegde functionaris om gebruikers en gebruikersrechten toe te kennen en heeft deze beschikking over beleidsregels over het wel/niet toekennen van rechten.
  - Gebruik de BIO hoofdstuk 9 als leidraad
- Wegbeheerder: De wegbeheerder heeft een zorgplicht waardoor hij ervoor kan zorgen dat hij niet aansprakelijk gesteld kan worden als er bijvoorbeeld ongevallen ontstaan door (foutieve) informatie uit de iVRI. De wegbeheerder moet zijn best doen (zorgplicht) om ervoor te zorgen dat er geen onjuiste gegevens verstuurd worden. Dit kan hij doen door:
  - Het implementeren van de BIO op het (i)VRI systeem.

    - Gebruik te maken van enkel gecertificeerde producten die voldoen aan de CROW richtlijnen en door te voldoen aan de geldende NEN-normen.
    - Gebruik te maken van landelijke uniforme bestekteksten en onderhoudscontracten voor de iVRI bij de aanbesteding van iVRI's.
    - Door structureel te (laten) monitoren op de kwaliteit van de iVRI-data middels het controleren van de KPI's in UDAP en bovenal te acteren bij afwijkingen.
- Wegbeheerder: Verantwoordelijkheid wegbeheerder voor borgen verwerken data die (mogelijk) persoonsgegevens bevatten: afsluiten van verwerkersovereenkomsten met leverancier(s) van iVRI componenten
- Wegbeheerder: Gebruik de eisen in BIO hoofdstuk 05 en 06 als leidraad
- Wegbeheerder: Verstuur nooit formulieren met gevoelige informatie per mail.
    - Alternatief is het gebruikmaken te maken van afgeschermde omgevingen zoals Sharepoint waar alleen geautoriseerde personen toegang tot hebben.
- Wegbeheerder: Gebruik de eisen in BIO hoofdstuk 05 en 06 en 10 als leidraad
- Wegbeheerder: Gebruik de VNG 'Handreiking Incident- en response management' voor de implementatie van de betreffende eisen uit de BIO omtrent cyber security incident management.
    - Wegbeheerder: Gebruik de eisen in BIO hoofdstuk 16 als leidraad
- Wegbeheerder: Maak beleid op het gebied van software updates voor (i)VRI's inclusief het beheer hierop.
    - Gebruik de eisen in BIO hoofdstuk 12 als leidraad
- Wegbeheerders en leveranciers: Bewustwording creëren bij medewerkers voor alle bestaande en aanwezige procedures rondom informatiebeveiliging.
- Wegbeheerder: zorg dat bij aanbestedingen altijd de BIO wordt voorgeschreven, maar zorg in samenspraak met de leverancier(s) dat de eisen concreet en van toepassing zijn op het gevraagde in de aanbesteding, zodat de leverancier ook de mogelijkheid heeft om hier op een goede wijze aan te voldoen.
- Regio/wegbeheerder en leveranciers: het in samenspraak met leveranciers uitvoeren van pen-testen om kwetsbaarheden bloot te leggen. Deze testen dienen op drie niveaus uitgevoerd te worden:
    - De fysieke VRI
    - Het netwerk
    - Overige applicaties

  Ieder rapport van de pen-test bespreken met de leveranciers. Wegbeheerders stellen samen met markt een Plan van Aanpak op hoe de aspecten op gebied van security, waar nu niet conform BIO aan wordt voldaan, aangepakt worden en op welke termijn. Hierbij wordt gezamenlijk bepaald wat de kosten zijn en hoe de verdeling van de kosten plaatsvindt tussen wegbeheerders en leveranciers. Zowel wegbeheerders als leveranciers dienen hierin in redelijkheid en billijkheid hun aandeel nemen. Dit betekent ook dat wegbeheerders in overleg met de leveranciers de huidige contracten open moeten breken en moeten aanpassen naar de huidige eisen.

Landelijke overheid

Beheersmaatregelen:

- Landelijke overheid: Met consolidatie iVRI-architectuur de volgende zaken meenemen:
  - Nieuwe aansluitvoorwaarden Cloud Service providers (cluster 2 partijen) om op UDAP aan te mogen sluiten. Deze partijen worden gecertificeerd. Marktpartijen krijgen hiermee ook een zorgplicht voor het op een veilige manier leveren van correcte data. C2 partijen zijn verantwoordelijk voor afsluiten overeenkomsten van de op hun aangesloten partijen (Service Providers, cluster 3 partijen).
  - Eigendom van data duidelijk vastleggen in overeenkomsten met de aangesloten partijen en wat wel en niet toegestaan is om te doen met de data door andere partijen anders dan de eigenaar.
- Landelijke overheid: Landelijk inregelen van het aanstellen van de Root Certificate Authority voor uitgifte en beheer van TLS certificaten in de iVRI data keten en alle bijbehorende systemen.
  - Gebruik de BIO hoofdstuk 10 als leidraad.
- Landelijke overheid: Digitaliseren en online brengen iVRI koppelvlak configuratie formulieren. Met rechten toegang geven op VRI's en deelrechten op onderdelen binnen formulieren, waaronder wachtwoorden. Bij voorkeur in UDAP, hier wordt al veel van de informatie geconfigureerd/opgeslagen die in het formulier terecht dient te komen. Voorkomen van dubbel opslaan en minder foutgevoelig. Middels rechten toegang geven aan personen tot bepaalde onderdelen van de formulieren.
- Landelijke overheid: Opstellen landelijke handreiking BIO-eisen VRI's voor toepassing bij aanbestedingen door wegbeheerders. Hierdoor eenduidigheid in eisen en bepalen van geaccepteerde risico's. Voor leveranciers goede basis om hun producten en diensten (en processen) op in te richten. Voor wegbeheerders ook vorm van 'garantie' dat hiermee security conform eisen BIO is gewaarborgd. Hiermee vaststellen van de baseline waaraan iedereen moet voldoen. In het kader van de BIO dient een (i)VRI gezien te worden als een 'Network endpoint device' aangesloten op een IT besturingsnetwerk dat geplaatst is in een straatkast. Wel nog ruimte laten voor leveranciers/marktpartijen om zich te kunnen onderscheiden. Aandacht voor het monitoren en controleren van zowel techniek (is versie software up-to-date) en organisatorisch/proces. Voorbeeld uitwerking BIO-eisen voor (i)VRI van gemeente Amsterdam kan hiervoor als basis/vertrekpunt fungeren.
- Landelijke overheid: Bewustwording creëren bij zowel wegbeheerders als marktpartijen voor noodzaak aanpassingen aan producten, diensten en processen om secure te worden en om te voldoen aan huidige regelgeving.

Leveranciers

Beheersmaatregelen:

- Leverancier: het credential management van VRI's (radicaal) anders inrichten. Dit moet minimaal landelijke schaalbaar worden. Mogelijk dat toegang centraal en niet meer lokaal geregeld moet worden.
- Gebruik de BIO hoofdstuk 09 als leidraad.
- Leverancier en wegbeheerder: bepaal gezamenlijk de restrisico's van het beperkt kunnen updaten van de software op embedded systemen en bepaal de beheersmaatregelen die nodig zijn om deze restrisico's als geaccepteerd te beschouwen.
- Regio/wegbeheerder en leveranciers: het in samenspraak met leveranciers uitvoeren van pen-testen om kwetsbaarheden bloot te leggen. Deze testen dienen op drie niveaus uitgevoerd te worden:
  - De fysieke VRI
  - Het netwerk
  - Overige applicaties

  Ieder rapport van de pen-test bespreken met de leveranciers. Wegbeheerders stellen samen met markt een Plan van Aanpak op hoe de aspecten op gebied van security, waar nu niet conform BIO aan wordt voldaan, aangepakt worden en op welke termijn. Hierbij wordt gezamenlijk bepaald wat de kosten zijn en hoe de verdeling van de kosten plaatsvindt tussen wegbeheerders en leveranciers. Zowel wegbeheerders als leveranciers dienen hierin in redelijkheid en billijkheid hun aandeel nemen. Dit betekent ook dat wegbeheerders in overleg met de leveranciers de huidige contracten open moeten breken en moeten aanpassen naar de huidige eisen.
- Leverancier: om ook BIO gecertificeerd te worden is het de aanbeveling om de BIO eisen mee te nemen in ISO27001 certificering. Dit kan door de 43 aanvullende artikelen uit BIO aan de ISO certificering toe te voegen en hier jaarlijks op te laten auditen. Zo wordt het mogelijk om vanuit de marktpartij/leverancier elk jaar een 'BIO In control' verklaring aan de betrokken wegbeheerders af te geven.

Bijlage 3: Checklist beheersmaatregelen

Beheersmaatregelen wegbeheerder				
Beheersmaatregel	**§**	**Onderwerp**	**Fase**	**√**
Toegangsbeheer				
Fysiek toegangsbeheer	3.1.1	Fysiek sleutelbeheer/sleutelplan	1A	
		Compartimentenbeheer	1A	
		Fysieke toegang ruimtes	1A	
		Apparatuur	3A	
		Mandaatbeheer	1A	
Digitale toegang/ wachtwoordbeleid	3.1.1	Beleid digitale toegang	1A	
		Toegang tot centrale verkeersmanagementsystemen	1A	
		Toegang VRI-data	1A	
		Toegang UDAP	1A	
		Mandaatbeheer	1A	
Wachtwoordbeleid	3.1.1	Wachtwoordbeleid	1A	
Netwerkscheiding VRI-communicatienetwerken	3.1.1.	Inrichten gescheiden VRI-netwerk	3A	
		Onmogelijk maken vanuit een VRI andere VRI's te benaderen	3A	
Informatiebeveiliging				
Verantwoordelijk over data in de keten	3.1.2	Voldoen aan zorgplicht ten aanzien van aansprakelijkheid	2 / 3A	
		Afsluiten verwerkersovereenkomsten	1A	
Delen van iVRI koppelvlak configuratieformulieren	3.1.2	Inrichten alternatief voor delen Security-gevoelige informatie	1A	
Change management				
Software updates	3.1.3	bepaal met leverancier restrisico's van het beperkt kunnen updaten van de software op embedded systemen	3A	
		bepaal beheersmaatregelen die nodig zijn deze restrisico's als geaccepteerd te beschouwen.	3A	
Incident management				
Draaiboek incident management	3.1.4	Implementeer a.d.h.v. VNG 'Handreiking Incident- en response management'	1A	
Personeel en organisatie				
Veilig personeel	3.1.5	Bewustwording creëren bij medewerkers voor alle bestaande en aanwezige procedures rondom informatiebeveiliging.	1A 3A	
Imago				

Imagoschade	3.1.6	Zorg dat bij aanbestedingen altijd de BIO wordt voorgeschreven.	3A	
Overall				
BIO-eisen vertalen naar (i)VRI BIO eisen	3.1.7	Opstellen handreiking BIO-eisen VRI's voor toepassing bij aanbestedingen door wegbeheerders.	1A	
Bewustwording creëren		Bewustwording creëren bij zowel wegbeheerders als marktpartijen voor noodzaak aanpassingen aan producten, diensten en processen om secure te worden en om te voldoen aan huidige regelgeving.	1A 3A	
Pen-testen		Pentesten uitvoeren voor de fysieke VRI, het netwerk en de overige applicaties	1A	

Beheersmaatregelen leverancier				
Beheersmaatregel	**§**	**Onderwerp**	**Fase**	**√**
Toegangsbeheer				
Credential management VRI	3.1.1	Credential management - landelijk schaalbaar - opzetten	1B	
Change management				
Software updates	3.1.3	bepaal met wegbeheerder restrisico's van het beperkt kunnen updaten van de software op embedded systemen	1B / 3B	
		bepaal beheersmaatregelen die nodig zijn deze restrisico's als geaccepteerd te beschouwen.	1B / 3B	
Personeel en organisatie				
Veilig personeel	3.1.5	Bewustwording creëren bij medewerkers voor alle bestaande en aanwezige procedures rondom informatiebeveiliging.	1B	
Overall				
BIO-certificering	3.1.7	BIO-eisen mee te nemen in ISO27001 certificering t.b.v. 'BIO In control' verklaring	3B	
Pen-testen	3.1.7	Pentesten uitvoeren voor de fysieke VRI, het netwerk en de overige applicaties	1B	

Beheersmaatregelen Landelijke overheid				
Beheersmaatregel	**§**	**Onderwerp**	**Fase**	**√**
Informatiebeveiliging				
Verantwoordelijk over data in de keten + Aansluitvoorwaarden	3.1.2 + 3.1.4	Aansluitvoorwaarden Cloud service providers (C2) toepassen	2	
		Aansluitvoorwaarden service providers (C3) toepassen	2	
		Eigendom data vastleggen	2	
Toepassing van Public Key Infrastructure (PKI) / TLS	3.1.2	Landelijk inregelen gebruik PKI/TLS certificaten	2	
		Aanstellen van de Root Certificate Authority voor uitgifte en beheer van TLS- certificaten	2	
Delen van iVRI koppelvlak configuratieformulieren	3.1.2	Digitaliseren iVRI koppelvlak configuratie formulieren, bij voorkeur in UDAP	2	
Overall				
BIO-eisen vertalen naar (i)VRI BIO eisen	3.1.7	Opstellen handreiking BIO-eisen VRI's voor toepassing bij aanbestedingen door wegbeheerders.	2	
Bewustwording creëren	3.1.7	Bewustwording creëren bij zowel wegbeheerders als marktpartijen voor noodzaak aanpassingen aan producten, diensten en processen om secure te worden en om te voldoen aan huidige regelgeving.	2	

Datum: 23 augustus 2022
Auteur: DTV Consultants B.V.
Opdrachtgever: SmartwayZ.NL
Contact: Etienne Wieme
ewieme@brabant.nl
www.smartwayz.nl