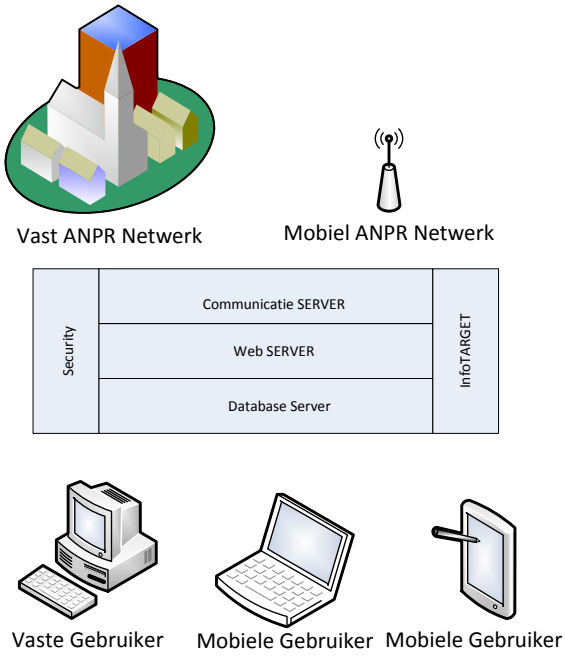
Fiche N° 14:

InfoTARGET - Keeping our roads safer

Voorwerp

SAMENGEVAT: de creatie van [zie onderstaande figuur]:

- ✓ Eén operationeel netwerk van ***vaste*** en ***mobiele*** ANPR-camera's
- ✓ Met het oog op **proactieve aansturing inzake verkeershandhaving** en reactieve verkeersdata analyse
- ✓ Van en voor de ***geïntegreerde verkeersdiensten***.



- Eind 2012 heeft de Vlaamse regering de uitbouw van een **vast ANPR-netwerk** in Vlaanderen goedgekeurd. Deze vaste ANPR-camera's registreren en herkennen de kentekens van voertuigen en worden hierbij gebruikt in het kader van de verkeersveiligheid: voor verkeersanalyse en verkeershandhaving. Vlaanderen biedt geïnteresseerde overheden de kans om via een opdrachtencentrale van het Agentschap Wegen en Verkeer dergelijke ANPR-apparatuur aan te kopen. De bedoeling is om de systemen compatibel te houden.
- Tegen het einde van de zomer 2013 is voorzien dat een proefproject met een aantal installaties in de regio Brasschaat, Sint-Job-in-'t-Goor en Brecht (met o.a. de op- en afrittencomplexen 3 en 4 van de E19) zal worden opgeleverd. Het proefproject betreft een eerste concepttest voor een geïntegreerd vast ANPR-systeem.
- Mogelijke volgende projecten zijn: een vrachtwagensluis in de Waaslandtunnel, handhaving van het vrachtroutenetwerk in de provincie Antwerpen en de uitbouw van trajectcontrole op het onderliggend wegennet.

- InfoTARGET is in hoofdzaak een dynamisch, interactief en snel hanteerbare tool om op structurele, transparante wijze gegevens inzake potentiële 'targets' te kunnen voeden en te kunnen raadplegen.
- Het gaat met name over een digitale tool voor het operationaliseren van het gebruik van "slimme" **mobiele ANPR camera's** tussen de verschillende politionele diensten belast met verkeerstoezicht (verkeersdiensten politiezones, federale wegpolitie,…). De erin opgenomen informatie inzake potentiële 'targets' betreft in hoofdzaak informatie omtrent nummerplaten van vervoermiddelen die gekoppeld zijn aan (potentiële) overtreders, wanbetalers, …,

- Bijvoorbeeld:
    - Onmiddellijke inningen: in bijzonder onbetaalde OI's (bv. Spaanse nummerplaat);
    - Verzekering: niet verzekerde voertuigen (VERIDASS - Assuralia);
    - Inschrijving: niet ingeschreven voertuigen bij de dienst inschrijving voertuigen (DIV);
    - Technische keuring: voertuigen waarvan de technische keuring is vervallen;
    - Ontzetting van het recht tot sturen: waarbij de mogelijkheid bestaat dat de bestuurder toch zijn voertuig zal besturen;
    - Misbruik: een garagehouder zou te pas en te onpas zijn 'garageplaten' uitlenen;
    - …
- Het opzet is om via een **'proof of concept'** (POC) te voorzien in een koppeling (via interfaces) tussen het vast ANPR-netwerk en de verschillende mobiele ANPR camera's. Hierbij zal InfoTARGET zijn vaste ANPR Info via een interface ophalen bij de politiezones die voorzien zijn van een ANPR server AWV (via hogervermelde aankoopcentrale AWV) en zijn mobiele ANPR Info over een 3G verbinding rechtstreeks in de van mobiele ANPR voorziene voertuigen (daarbij de functie van BOSS server overnemende).

Motivatie

- Het betreft het concreet voorstel voor het uitrollen van een **supralokaal** tweetalig (Nl/Fr) InfoTARGET **platform** binnen de geïntegreerde politie. In een eerste fase zal een POC worden opgezet in het Arr Antwerpen (binnen de POC betreft het 11 politiezones, waaronder de PZ Antwerpen en de federale entiteiten: WPR, CICANT, CSD, AIK, …). Nadien kan dit platform gefaseerd uitgerold worden in de verschillende entiteiten van de geïntegreerde politie.
- Om dit platform op te zetten, bestaat de module InfoTARGET die toelaat aan iedere verkeersentiteit van de geïntegreerde politie om op autonome basis 'verkeersitems' in te voeren waarop operationeel aangestuurd en gewerkt kan worden door iedere participerende (aangesloten) entiteit; de applicatie garandeert de aanbiedende eenheid communicatie omtrent resultaten via een forum en laat dus opvolging en (her)aansturing toe.
- Als bijlage gaat een fiche die de 'eenvoudige' en haalbare integratie van de actueel bestaande systemen, die een combinatie zijn van lokale (mobiele) en gewestelijke (vaste) ANPR camera's, toelaat.
- Zowel voor mobiele als vast ANPR is het op deze manier mogelijk om data in te voeren die toelaten om:
    - Vooraf verkeers TARGETS te identificeren - gericht op onmiddellijke detectie;
    - Via bv. CIC of in de politiezone/WPR online een nummerplaat in te voeren die toelaat om operationeel te reageren op een 'hit' via de vaste en mobiele ANPR camera's;

- In het **gemeenschappelijk actieplan** tot naleving van de **verzekerings- en keuringsplicht** van motorvoertuigen van de Ministers van Financiën, Economie, Binnenlandse Zaken, Justitie en de Staatssecretaris voor Mobiliteit (bijlage aan de COL 15/2013 van 20.06.2013), wordt onder andere de rol beklemtoond van het Belgisch Gemeenschappelijk Motorwaarborgfonds m.b.t. de opsporing en de melding van niet-verzekerde motorvoertuigen en GOCA voor de niet-gekeurde motorvoertuigen. In het bijzonder dient een geautomatiseerde procedure te worden uitgewerkt door de geïntegreerde politie (cfr. Pt 2.1, 6de lid, 6° van het actieplan). Een cruciaal hulpmiddel in het opsporen van de niet-verzekerde/gekeurde voertuigen, is het gebruik van camera's uitgerust met automatische nummerplaatherkenning (ANPR) (Cfr. Pt 2.2 van het actieplan).

Raming uitgaven - PM

- **FASE 1:** POC Arr Antwerpen
- **Roll-out FASE:** Geïntegreerde politie (GPI)

Opmerkingen

Onderstaande opmerkingen worden geformuleerd in antwoord op de gestelde vragen in het DirCom+ van 31.05.2013:

- Inzake de toepassing **wetgeving overheidsopdrachten**

  De wet van 24.12.1993 betreffende overheidsopdrachten en sommige opdrachten voor aanneming van werken, leveringen en diensten (B.S., 22.01.1994) en latere wijzigingen, voorziet inzonderheid in Art. 17, § 2, 1° f ('technische specificiteit') de mogelijkheid tot het voeren van een onderhandelingsprocedure zonder bekendmaking voor de verwerving van een product dat dermate specifiek is, dat enkel bij één welbepaalde leverancier kan worden betrokken.

  Er werd in het verleden voor de verwerving van bestaande (specifieke) software reeds veelvuldig gebruik gemaakt van deze gunningsprocedure.

- Inzake de **privacycommissie** (CBPL) en het **Controleorgaan** van het **politioneel informatiebeheer** (COC)

  InfoTARGET werd op 25.04.2013 aangegeven aan de Privacycommissie (CBPL) onder de referentiesleutel VT005012813 en bekwam, door tussenkomst van het parket Kortrijk en met de steun van de Federale Procureur, op 07.03.2013 de status "akkoord" als bijzondere databank (met referentienummer 99999808) bij het "Controleorgaan van het Politioneel Informatiebeheer" (COC).

  Tevens dient in het kader van de privacywetgeving te worden verwezen naar de aanbeveling van de CBPL uit eigen beweging (nr 04/2012 van 29.02.2012) inzake de diverse toepassingsmogelijkheden van camerabewaking. Hieruit blijkt: "*Het gebruik van mobiele bewakingscamera's met nummerplaatherkenning met het oog op onder meer de opsporing van gestolen voertuigen enzovoort, is met andere woorden de lege lata problematisch gelet op deze recente aanpassing van de camerawet. Het gebruik van* ***vaste bewakingscamera's*** *met nummerplaatherkenning is volgens de camerawet daarentegen wel mogelijk (bv. aan sommige op- en afrittencomplexen of bij binnenkomst van een stad of gemeente) en juridisch sluitend (randnummer 53). In de huidige stand van de wetgeving is echter geen sluitend juridisch positief antwoord te geven op de vele vragen en zorgen alvast de* ***mobiele ANPR's*** *(ten dele) voor wettelijke problemen afhankelijk van de concrete toepassingen (randnummer 54)."* Het is echter perfect mogelijk om een "mobiele ANPR" bv. in een controle dispositief statisch te gebruiken, waardoor deze als vaste ANPR wordt ingezet, wat in de huidige stand van de wetgeving perfect mogelijk is.

  In deze dient tot slot te worden meegegeven dat de minister van Binnenlandse Zaken in antwoord op de mondelinge vraag (Nr 5-1021) van G. De Padt op 30.05.2013 het volgende heeft geantwoord: *"Om deze en andere redenen bereid ik een* ***wetsontwerp*** *voor tot wijziging van de camerawet van 2007. Ik hoop dit ontwerp nog vóór de zomer bij de Ministerraad in te dienen, zodat het in het najaar in het parlement kan worden besproken."*

- Inzake de **veiligheid** van het **platform**, ISLP en Hilde vs. **CertiPOL**

  Actueel zijn er twee soorten netwerken in voege bij de politiezones, namelijk:
  - ISLP op het beveiligde Hilde netwerk waar GEEN gateway mogelijk is naar burgerlijke netwerken zoals LAN/WAN internet of het 3G datanetwerk en
  - PolADMIN, of het lokaal administratief netwerk van de zones waar middels een lokale router en een terminal of Citrix server een administratieve omgeving wordt opgezet die kan worden opgestart door het runnen van een ICA-client op de ISLP omgeving.

  Het veiligheidsmodel dat door DST-DTTD-IID vooropgesteld werd bij het opmaken van de standaard voor de toegang tot de IT middelen van het ISLP netwerk vanuit het administratief netwerk van een politiezone richt er zich op zich te wapenen tegen directe of indirecte schade aan de digitale informatie of de applicaties van de geïntegreerde politie.

  Een uitbreiding die zich sedert 2012 opdringt in dit model is het bijvoegen van een derde netwerk, het zogenaamde 'VDI' netwerk. Het VDI netwerk omvat alle actieve elementen, de werkposten en servers nodig om alle IT middelen in het ISLP-netwerk te benaderen van uit het administratief netwerk.

  Op heden is het draaien van de InfoTARGET web toepassing mogelijk op een webserver binnen het ISLP netwerk, echter de kracht van de mobiele beschikbaarheid van deze toepassing, maken net het verschil in de dagtaken van de politieagent bij het streven naar EPZ!

  Basis van het Hilde netwerk (2 fasen beveiliging) is dat:
  - Het netwerk afgeschermd is en enkel bevoegden zich fysiek toegang kunnen verschaffen tot de resources op het netwerk (binnen de zone door middel van LAN toegang op de Hilde router, of via een VDI netwerk in de voertuigen). In wezen komt het dus neer op 'enkel bevoegden kunnen fysiek de resources aanspreken) – inbreuken of hacks op dit netwerk moeten derhalve van fysieke aard zijn en kunnen onmogelijk door middel van een 'man-in-the-middle' principe worden uitgevoerd.
  - Eenmaal men gecertificeerd is op een netwerk en de fysiek plaats, moet men zich als gebruiker nog aanmelden. Dit is de fase 2, dit kan door middel van een login en paswoord, of door middel van een token, eID kaart of andere. Inbreuken hier zijn van sociale hacking aard, m.a.w.. een individu geeft zijn credentials willens of nillens door aan een potentiële hacker.

  Het creëren van een 'vertrouwde' *ergo* 'gekende' omgeving waar geen 'sniffing' of kaping van gegevens mogelijk is op de datastroom tussen de 'server' en de 'gebruiker' kan technisch perfect door middel van een encryptie, de zogenaamde **SSL encryptie**. Deze encryptie methodiek maakt gebruik van veiligheidscertificaten die aan beide kanten aanwezig moeten zijn en zorgen voor een beveiligde lijn of 'pijp' waar de actuele data in getransporteerd wordt. Het verstrekken van een **veiligheidscertificaat** is steeds middels een internationaal erkende instantie (Thawte bvb.) die als derde partij toeziet op de waarheid en echtheid van de twee partijen binnen de uitwisseling van gegevens.

  Bij het Certipol principe is dit Fase 1, of de gecertificeerde en beveiligde connectie tussen de gebruiker, het toestel, en de server. CertiPOL gaat vervolgens zorgen voor zekerheid dat het toestel (vast of mobiel) gekend is bij de bron (zoals dit bij Hilde – ISLP- fysiek het geval is). Dit gebeurt door middel van een tweede certificaat. De InfoTARGET server omgeving heeft een CertiPOL Root certificaat server staan die op basis van MAC-adres informatie op automatische of manuele (te beheren door een IT manager of Functioneel beheerder) manier een certificaat uitgeeft aan het toestel. Deze PC, laptop of tablet moet dan vervolgens dit certificaat installeren. Op die manier weet CertiPOL met zekerheid via zijn Fase 1 en Fase 2 beveiligingsstap dat:

- De communicatie veilig is naar inhoud (er is geen kaping van de sessie mogelijk) en
- Het toestel dat straks de login informatie zal doorsturen 'fysiek betrouwbaar is'

Op die manier kan de beheerder van het CertiPOL platform – in voorkomend geval - steeds de gestolen toestellen blokkeren in de certificaatslijst en op die manier de toegang tot het netwerk ontzeggen.

Fase 3 van het CertiPOL beveiligingstraject is dan opnieuw een aanroepen van https://certipol.be waarbij nu de verbinding wordt geëncrypteerd door het officiële certificaat en de authoriteit die het uitgeeft (bvb Thawte) en daarna ook kijkt of het toestel 'bevriend' is door middel van het InfoTARGET eigen certificaat.

Eenmaal dat deze procedure OK is, wordt dan overgegaan naar Fase 4, de zogenaamde fase 2 bij ISLP, namelijk de gebruikers authentificatie. Hier zijn zowel op Hilde als op het CertiPOL netwerk mogelijkheden om dit te doen, met name:

- Eenvoudige login middels V-nummer en paswoord;
- Token authentificatie en
- eID authentificatie.

InfoTARGET werkt actueel met de eerste methode, waar mogelijkheid bestaat om via LDAP een synchronisatie uit te voeren met de PolADMIN actief directory (bij grote politiezones is dit wenselijk naar beheer toe). Op die manier biedt het **CertiPOL netwerk** – gebruik makende van internet en het mobiele 3G netwerk van een van de nationale operatoren – **dezelfde veiligheidsgaranties als Hilde**. Een uitgebreide logging op alle niveau's en bij alle fases is voorzien, en dit ten behoeve van reconstructies i.f.v. calamiteiten.

Binnen het 'gesloten LAN netwerk' van Hilde is het in principe onmogelijk een verbinding te maken naar het internet. Pogingen tot hacking, sessie kaping of sniffing zijn dus uitgesloten, tenzij de betrokkene zich fysiek de toegang verschaft op het netwerk, in de politie gebouwen, of in het data center FedPol. De CertiPOL omgeving steunt op het creëren van een gelijkwaardige omgeving, echter het transport medium is hier het publieke internet.

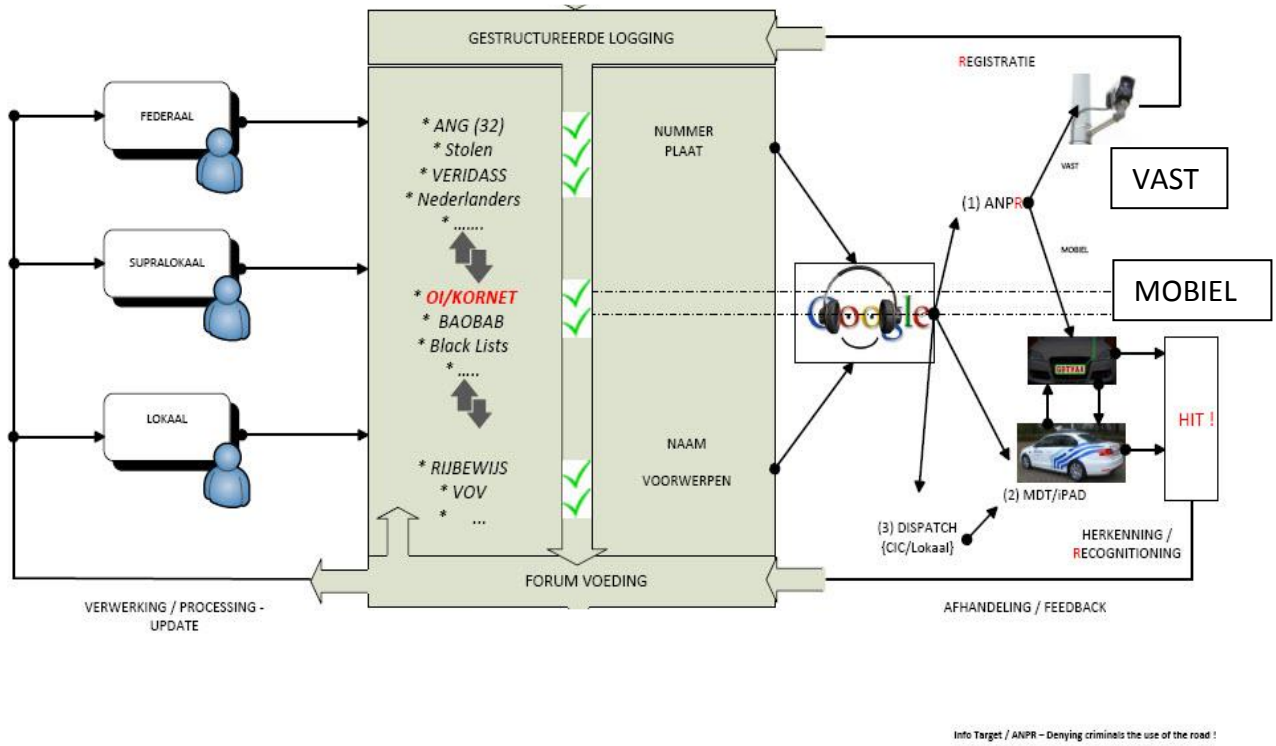
Onderstaande **besluiten** konden worden genoteerd n.a.v. het DirCom+ van 25.06.2013:

De integratie van Infotarget (of een vergelijkbare oplossing, aan te schaffen via overheidsopdracht, waarbij de reeds effectieve werking van de oplossing van fundamenteel belang is om snelle resultaten te boeken) wordt als operationeel noodzakelijk geacht.

Om de hoger vermelde reserves uit te klaren:

- zal CGO de oplossing Infotarget inkaderen in de huidige politie informatie. Dit dient oplossingsgericht te gebeuren of m.a.w. bekijken hoe de oplossing mogelijk wordt (regelgeving, procedures, eventueel te bekijken link met ANG) en niet een opsomming van redenen waarom het niet mogelijk zou zijn;
- ISIS zal samen met InfoSec CB in een overleg met de huidige firma van Infotarget de veiligheid van de oplossing nagaan.

Dircom+ is het eens dat indien er, vanuit politieke hoek of IF, teveel vragen zouden rijzen over de beoogde oplossing, dit dossier de andere projecten in het verkeersveiligheidsfonds niet in het gedrang mag brengen.



Info Target / ANPR – Denying criminals the use of the road !