Eerste ervaringen: werken met RRO’s

Indrukken vanuit een helicopterview

Smart Mobility Solutions

Introductie

- De DITCM security tafel faciliteert een aantal partijen bij het maken van een Risico Reductie Overzicht* (RRO)
- Het doel is om het resultaat van een risico analyse inzichtelijk te maken, door visueel de samenhang te laten zien tussen dreigingen, maatregelen en risico's.
- In 2015 is zowel door RWS als het PCP A58 project een RRO opgesteld
- Deze presentatie geeft de eerste ervaringen van het werken met een RRO

* http://rro.sourceforge.net/

Waarom een RRO?

- Verwachting is dat deze een uitstekende basis biedt voor risicocommunicatie binnen en tussen C-ITS projecten.
- Wat noodzakelijk is bij het vinden van synergie tussen (C-ITS) projecten

- Daarnaast:
  - op de RRO site (http://rro.sourceforge.net/) is goede documentatie beschikbaar
  - Daar is ook een visualisatie tool beschikbaar
  - Zowel de methode en tools zijn open source

- De RRO methodiek is ontwikkeld door het Ministerie van Defensie is daar net als bij Rijkswaterstaat standaard onderdeel in het risicomanagement systeem.

Status eind 2015:

- Ervaring opdoen met RRO's (loopt)
- Samen met projecten
  - 2 projecten -> RRO (RWS en PCP A58)
  - 2 projecten -> Intake gesprek
- High level bevindingen (zie volgende slides)

Bevinding 1: Scope bepaalt de focus restrisico's

- Met het opstellen van de RRO voor PCP A58 kwam naar voren dat de focus op de technische risico's en maatregelen lag.
  - Daardoor waren een aantal finale risico's die relevant waren voor de applicatie-eigenaren niet benoemd
  - Wanneer andere projecten een andere focus belemmert dit de mogelijkheid om resultaten van risico analyses en RRO's te vergelijken.
- Met behulp van de RRO heeft het PCP A58 project samen met applicatie-eigenaren bepaald dat aanvullende technische maatregelen nodig waren.

Aanbeveling 1.A: Maak bij uitvoeren van een risico analyse en visualisatie in een RRO expliciet voor wie finale risico's bepaald worden.

- Waar bij de analyse voor het A58 project de focus lag op de techniek heeft iVRI het zwaartepunt liggen bij de diensten.
- Naast deze voorbeelden kan de focus ook liggen op een businesscase (wat zijn bijvoorbeeld de risico's dat niet betaald wordt voor een dienst, waardoor een businesscase onderuit gaat).
- Daarbij is absoluut aandacht nodig voor safety aspecten, maar ook voor privacy.
- Om RRO's over projecten heen te kunnen vergelijken zal een vergelijkbare focus en zelfde type risico-eigenaar de basis moeten vormen

Aanbeveling 1.B: Start een risico analyse met de inventarisatie en classificatie van assets

- Ga uit van alle relevante assets. Dus niet alleen technische componenten, maar ook mensen, processen, huisvesting etc. Daarmee wordt voorkomen dat relevante risico's voor deze assets over het hoofd gezien worden.
- Ter illustratie:
  - Wat wordt gedaan om te voorkomen dat een belangrijke technische component gestolen kan worden?
  - Hoe wordt ervoor gezorgd dat alleen vertrouwd personeel wijzigingen aan kan brengen?

Bevinding 2: Onvoldoende inzicht (en daarmee betrokkenheid) van gevolgen voor risico eigenaren

- C-ITS projecten zijn per definitie projecten waar veel stakeholders bij betrokken zijn.
- Door de complexiteit is het niet vanzelfsprekend dat alle stakeholders beseffen dat ***hun risico's*** niet automatisch geadresseerd worden.
- Daardoor geven zij onvoldoende sturing op voor hun noodzakelijk maatregelen of onvoldoende betrokken bij het oplossen van problemen.
- Daarbij moet opgemerkt worden dat risico's vaak "subjectief" zijn. Dit doordat deze afhankelijk zijn van de "pijn" die een stakeholder ervaart als iets misgaat. Dat wordt versterkt doordat risico's vaak niet kwantitatief te maken zijn door gebrek aan harde cijfers.

Aanbeveling 2: Maak expliciet voor welke stakeholder een RRO bedoeld is en maak zijn “pijn” (in de vorm van finale risico’s) herkenbaar

- Ga voor het opstellen van een RRO na voor wie deze gemaakt wordt en wat het belang is van deze stakeholder bij het project.
- Dit kan betekenen dat er een aantal versies van een RRO nodig zijn om alle stakeholders voldoende te betrekken.
- Verschillen zullen dan hoofdzakelijk zitten in de formulering van het finale risico.
- Deze stakeholder centrische aanpak wordt ook benoemd in een recent ENISA rapport*.

* Cyber Security and Resilience of Intelligent Public Transport, ENISA, December 2015

Relatie RRO en Risicoanalyse

- De RRO is een visualisatiemiddel om de resultaten van een risicoanalyse makkelijker te kunnen communiceren met verschillende stakeholders.
- Een RRO is geen vervanging van een Risicoanalyse, maar een aanvulling daarop. Daarbij is het uit (laten) voeren van een risico analyse een best practice.

Wat is er nodig voor het maken van een RRO?

- De basis voor het maken van een RRO is een (goed gedocumenteerde risicoanalyse)
- Afhankelijk van de complexiteit kost het maken van een RRO 1 - 2 RRO experts een dag. Daarbij is het aan te bevelen om daar ook 1 – 2 projectleden met inhoudelijke kennis van het systeem of dienst voor een dagdeel beschikbaar te hebben.
- Het visualiseren zelf kan door gebruik te maken van de RRO Tool.

“Disclaimer” bij RRO’s

- Bij een kwalitatieve risicoanalyse zal de RRO ook kwalitatieve informatie bevatten. Om de mate van subjectiviteit hierin te beperken is aan te raden om ook de RRO ter review bij diverse experts uit te zetten.

Wanneer kan een RRO ingezet worden?

- Om communicatie met risico eigenaren op gang te brengen en op deze wijze awareness te creëren.
- Bij expliciet maken van welke risico’s binnen een project niet afgedekt worden / niet afgedekt kunnen worden.
- Om de samenhang tussen elementen (dreigingen, maatregelen en restrisico’s) van een risicoanalyse inzichtelijk te maken.

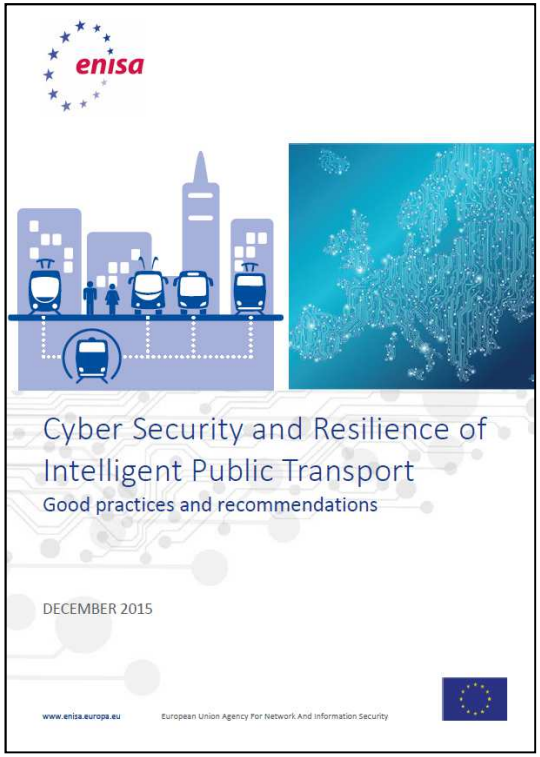
RRO’s helpen bij “dynamische” aanpassingen.

- Door de visualisatie is veel sneller duidelijk wat effecten zijn bij veranderingen in dreigingen en maatregelen.
- Het effect op restrisico’s en finale risico’s van het niet treffen van een maatregel kan snel inzichtelijk gemaakt worden voor de verschillende stakeholders.
- Vooral dit laatste is aan de hand van standaard Risico analyse rapportages een stuk lastiger.

Samenvatting van bevindingen

- De complexiteit van de C-ITS projecten en het aantal betrokken stakeholders vraagt om meer aandacht voor verschil in risico's en hoe zij ervaren worden.
- Voor alle stakeholders: Als iets niet op orde is en jij daar pijn van ervaart, betekent dat je een risico eigenaar bent. Ga na of jouw risico's (mogelijke pijnpunten) worden afgedekt door passende maatregelen.
- Een RRO maakt de samenhang tussen dreigingen, maatregelen en restrisico's inzichtelijk.
- Het helpt om over de projecten heen een zelfde focus te kiezen, om later de RRO's vergelijkbaar te maken. Dat is op dit moment nog niet mogelijk.
- Binnen C-ITS ligt de focus vaak op ICT security aspecten. Het is noodzakelijk om zaken als safety en privacy expliciet mee te nemen.

➜ Tenslotte: awareness voor security groeit.



Leading partners in Smart Mobility

DITCM Innovations

Smart Mobility Solutions