Over de security van ITS systemen

KORTE HANDREIKING VOOR BESTUURDERS, OPDRACHTGEVERS EN OPDRACHTNEMERS

Ronde Tafel Security

LANDELIJKE RONDE TAFELS VOOR SMART MOBILITY | RONDETAFELS.DITCM.EU

30-11-2015

Over de security van ITS systemen

Doelstelling van deze handreiking

Initiatiefnemers van ITS-projecten worden geconfronteerd met vragen wat ze gaan doen aan (information) security? Evenzo worden er aan bestuurders vragen gesteld over de mogelijkheden en de gevolgen van hacking.

Deze notitie is een *korte handreiking* aan bestuurders, opdrachtgevers en opdrachtnemers hoe om te gaan met (information) security van ITS-systemen. Hiermee kunnen bestuurders het onderwerp (information) security tijdig agenderen in de interne organisatie en in extern overleg en mobiliseren.

Aandachtspunten:

1. Wat is het belang van het ITS-systeem?

    a. Zonder security zijn ITS-systemen niet betrouwbaar. Dan zullen er, vroeg of laat, onverwachte gebeurtenissen met ongewenste effecten gaan optreden. Het ITS-systeem is dan niet beschikbaar en/of vertoont onvoorspelbaar gedrag. Dit kan gevolgen hebben voor de verkeersveiligheid, het milieu en/of de doorstroming van het verkeer.
    b. Aan een permanent operationeel ITS-systeem worden waarschijnlijk meer eisen van betrouwbaarheid gesteld dan aan een systeem voor een tijdelijk (verkeerskundig) onderzoek. De eisen aan betrouwbaarheid dienen altijd expliciet te worden gemaakt.
    c. Het is een illusie dat enig ITS-systeem ooit 100% betrouwbaar zal zijn onder alle omstandigheden. Een *risico-gebaseerde aanpak* is daarom aan te bevelen. Door de implementatie van een verzameling van risico-mitigerende maatregelen kan een ITS-systeem voldoende betrouwbaar worden gemaakt. Dat is het doel van security.
    d. Security van ITS-systemen is daarom altijd een maatpak.

2. Wie is verantwoordelijk voor security?

    a. Security is een organisatorische verantwoordelijkheid. De bestuurder van een organisatie is verantwoordelijk.
    b. De verantwoordelijkheid voor security kan niet worden gedelegeerd. Delegatie van deze verantwoordelijkheid kan noch in de eigen organisatie noch naar een externe opdrachtnemer of leverancier.

c. In de situaties van een opdrachtgever en een opdrachtnemer dienen beide in gezamenlijkheid te bespreken en te beoordelen welke risico's m.b.t. het ITS-systeem wel en niet acceptabel zijn. Op basis hiervan kunnen de gewenste en noodzakelijke maatregelen opgenomen worden in het *programma van eisen*.
d. In een zogenaamde toeleveringsketen van fabrikanten, leveranciers en/of (onder)aannemers is elke organisatie verantwoordelijk voor de security van de totale dienst/product die zij levert incl. die van de keten van diensten/producten van derden die zij direct/ indirect afneemt.
e. Periodieke evaluatie van de afgesproken security maatregelen is essentieel.

3. Wat zijn de wettelijke voorschriften?

a. Op dit moment gelden er weinig tot geen *specifieke* wettelijke verplichtingen t.a.v. information security van ITS-systemen.
b. Alle partijen zijn zelf onderhevig aan diverse wettelijke eisen voor information security waaraan zij dienen te voldoen. De kennis daarvan is aanwezig bij de verantwoordelijke voor information security in de eigen organisatie. De meeste organisaties, bijv. wegbeheerders, hebben eigen security baselines waaraan elk informatiesysteem moet voldoen, dus ook ITS.
c. Daarnaast is het zo dat als er persoonsgegevens en/of locatie-gegevens van voertuigen of mobiele devices worden verwerkt de *privacywetgeving* van toepassing is. In die wetgeving worden specifieke voorwaarden gesteld aan de verwerking en de opslag van gegevens alsook aan hoe de gegevens dienen te worden beveiligd.

Communicatie over information security

- Geen enkel ITS-project, hoe klein ook, kan helemaal zonder security.
- Het is aan te bevelen dat opdrachtgever en opdrachtnemer de bovenstaande drie aandachtspunten *vooraf* bespreken en hun uitgangspunten en afspraken vastleggen.
- Dat is de basis voor partijen om eenduidig intern en extern over security te communiceren.
- Het is belangrijk om goed voorbereid te zijn op eventuele security-vragen en ook op security-incidenten.

- Omdat de reputatie en het imago van zowel het ITS-systeem als van de betrokken partijen op het spel staan, is een goede voorbereiding en regie over de communicatie noodzakelijk.

Vragen en informatie

Voor vragen of een verkennend gesprek over ITS en information security kunt u altijd contact opnemen met de Ronde Tafel Security.

Contact ir. Gilles Ampt CISM CIPP/E, tel. 0654-252007, amptgj@xs4all.nl

Handreiking voor bestuurders in overheidsorganisaties

Een uitgebreidere handreiking voor bestuurders in overheidsorganisaties is te vinden op:

http://www.taskforcebid.nl/producten/instrumenten-informatieveiligheid/