Welkom

Bijeenkomst Platform Tunnels en veiligheid

10-12-2020

COB
Nederlands kenniscentrum voor ondergronds bouwen en ondergronds ruimtegebruik

Agenda

1. Welkom
2. Introductie thema’s 2021
3. Van object-naar systeemveiligheid
4. Cybersecurity-lancering groeiboek
   - Terugblik
   - Toelichting nieuwste versie
   - Volwassenheidsscan
   - In gesprek met de beheerder
5. Terugkoppeling thema’s 2021

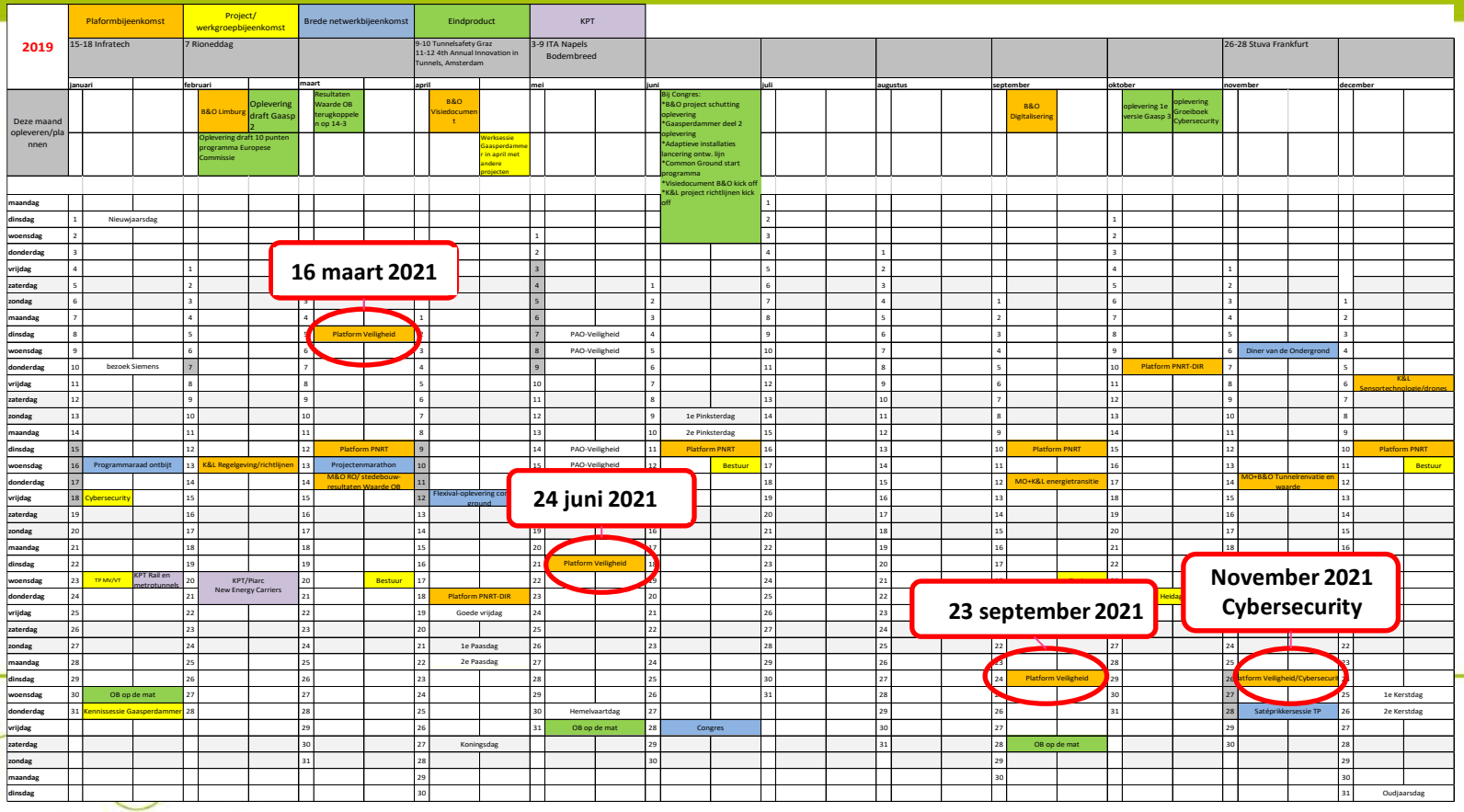
Korte terugblik 2020

- **Platformbijeenkomsten**
  - Afgelast 17-03-2020
  - Smart mobility 12-06-2020
  - Bediening en besturing 15-09-2020
  - Cybersecurity en systeemveiligheid 10-12-2020
- **Cybersecurity – Presentatie groeiboek versie 3**
- **Faciliteren ISAC tunnels**
- **Systeemveiligheid – Workshops Haaglanden, Rotterdam en Amsterdam**

Jaarplan 2021

- **Vervolg project Cybersecurity – Doorontwikkeling groeiboek**
- **Faciliteren ISAC tunnels,** voorzitter Tom van Tintelen
- **Doorstart groeiboek ‘Tunnelrenovatie’,** vanuit de samenvoeging van de groeiboeken ‘renoveren kun je leren’ en ‘hinderarm renoveren’
- **Aanhaken bij structural health analyse voor opzetten TTI expertteam**
- **4 platformbijeenkomsten**
  - Tom van Tintelen co-coördinator voor bijeenkomsten en linking pin met KPT

Data bijeenkomsten platform Tunnels en veiligheid 2021



Intro thema's 2021 voor bijeenkomsten

Hoofdthema in 2021 is **Renovatie**

Ideeën voor bijeenkomsten tot nu toe:

- Ervaringen VIT2, 'renoveren met de winkel open'
- Gebruik van digital twin bij renovatie
- Tunnelrenovaties in relatie tot 'aantoonbaar veilig' (weg en spoor)
- V&V bij gedeeltelijke renovatie
- Ontwikkelingen in standaardisering; LTS/HTS/ATS/IA bouwblokken
- Uitkomst evaluatie LTS/vluchtconcepten (onder van vrijgave)
- Cybersecurity, terugkoppeling projectresultaten
- Ontwikkelingen en innovaties bij TTI
- … en andere ontwerpen, graag uw inbreng!

Wordt vervolgd na de laatste presentatie

Platform Tunnels en veiligheid

Van object- naar systeemveiligheid

Ron Beij

COB
Nederlands kenniscentrum voor ondergronds bouwen en ondergronds ruimtegebruik

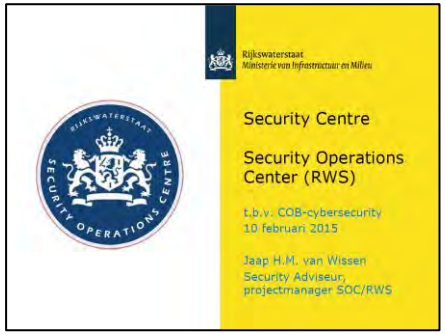
Platform Tunnels en veiligheid

Cybersecurity
Lancering groeiboek 3.0

Nederlands kennis centrum voor ondergronds bouwen en ondergronds ruimtegebruik

Terugblik: de aanleiding

Bijeenkomst veilige software en cybersecurity op 10 februari 2015



Oproep aan de deelnemers:
Wie heeft er interesse om deel te nemen aan een werkgroep (ISAC) om kennis en ervaringen aangaande cyber security in infrastructuur te delen, en gezamenlijk na te denken over hoe dit bij andere projecten en objecten ingezet kan worden.

Terugblik: de werkgroep

Eerste overleg 9 september 2015 (voorzitter André Stehouwer)
Het initiatief van deze werkgroep is ontstaan vanuit een bijeenkomst van het Platform Veiligheid. In deze bijeenkomst heeft Jaap van Wissen van RWS een toelichting gegeven op de ISAC's die al zijn opgericht voor o.a. havens en luchthavens, maar niet voor tunnels.

Lidmaatschapsrichtlijnen Tunnel-ISAC

Versie 1.3 – januari 2016

Inhoud

1 Taakstelling

1.1. De Tunnel-ISAC[1] is bedoeld om **een veilige en vertrouwde omgeving te bieden waarbinnen private partijen, die een onderdeel zijn van de vitale infrastructuur in de tunnel-community en de, met (cyber)security belastte overheidspartijen, gevoelige en vertrouwelijke informatie over cyberdreigingen en best practices kunnen uitwisselen.**

1.2. Doelstellingen

1.2.1. **De Tunnel-ISAC is een gremium waar het delen van kennis, informatie en ervaringen ten aanzien van cybersecurity tussen leden binnen de tunnel-community centraal staat.**

1.2.2. **De ISAC draagt bij aan het versterken van de (keten)beveiliging in de sector door een permanent netwerk te vormen waardoor partijen elkaar ook buiten het overleg om makkelijker weten te vinden.**

1.2.3. **Toegevoegde waarde en onderling vertrouwen staan aan de basis van de Tunnel-ISAC.**

1.3. Het lidmaatschap is beperkt tot organisaties die aan de in **Hoofdstuk 2** genoemde criteria voldoen.

1.4. Vertegenwoordigers van deze organisaties moeten aan de in **Hoofdstuk 3** genoemde criteria voldoen.

1.5. Alle deelnemers zijn gehouden de in **Hoofdstuk 4** genoemde procedures en voorschriften ten aanzien van het uitwisselen van informatie, na te leven.

1.6. De ISAC staat onder voorzitterschap van een vertegenwoordiger van de tunnelsector.

1.7. Waar nodig stelt de ISAC subgroepen en werkgroepen in om de door de ISAC overeengekomen werkprojecten te trekken. Het lidmaatschap van subgroepen en werkgroepen is niet noodzakelijkerwijs beperkt tot ISAC-vertegenwoordigers, maar staat ook open voor externe benoemingen als het project daartoe aanleiding geeft.

1.8. Externe communicatie over de werkzaamheden van de ISAC wordt uitsluitend gedaan door de voorzitter van de ISAC of door iemand die daartoe door de voorzitter is aangewezen.

Terugblik: ontstaan groeiboek

In 4 werkgroep-bijeenkomsten in 2016 is verder gewerkt aan deze doelstellingen en zijn op 21 juni de voorstellen voor een inhoudsopgave besproken.

Voorzet inhoudsopgave boekje ISAC Tunnels, cyber security opgesteld door:
Tom Versluijs en RitaPuggioni

1. Inleiding /cybersecurity bij tunnels/(bruggen en sluizen)(*evt. klein stukje geschiedenis er bij*)
2. Doelstelling
3. Doelgroep en scope
4. (Bestuurlijke) afweging/probleemanalyse(*Kan ook in risicoanalyse*).
   Toelichting: wil je als organisatie verder om jouw objecten cyber secure te maken?
   Wanneer wordt het voor jouw organisatie belangrijk om je objecten cyber secure te maken?
   Welke afwegingen kun je maken om dit te bepalen?
   1.1 welke problemen kun je ondervinden als je object(en) niet cyber secure zijn (voorbeeld)
   1.2 waarom is het een probleem voor 'ons'? (voorbeeld)
5. Inventarisatie objecten en prioritering
   Toelichting: als je besloten hebt dat jouw objecten cyber secure moeten worden, hoe weet je welke objecten secure moeten worden?
   Hoe bepaal ik de onderlinge prioriteiten? Waar kan ik vinden hoe ik verder moet hiermee?)(verwijzingen)
6. Risico's per object
   Toelichting:als je besloten hebt welke objecten je cyber secure wilt maken en welke prioriteiten je daarin hebt, dan dien je te bepalen welke risico's er mogelijk zijn per (soort) object (en hoe je die herkent).
7. Mogelijke maatregelen
   Toelichting: *Hier zou je kunnen beschrijven hoe je uniforme problematiek beheersbaar kunt maken?*
   Dit stuk tekst kan als begeleidend schrijven worden gezien waarin diverse bijlagen, zoals bijvoorbeeld: een systematiek met diverse bijlagen, kan worden toegelicht.
8. Implementatie voorbeelden goed en fout?
9. Links naar informatie.
   Toelichting: kennisvergaring, links naar rapporten ISAC tunnels, Bron opgave.
10. Bijlagen in de vorm van eisen pakketten / richtlijnen, systematieken of formats ed.

Voorstellen voor inhoudsopgave ISAC tunnels, cyber security

Voorstel Jasper Kimstra:

1. We gaan beveiligen
Onze object heeft een onderhoudsbeurt nodig omdat we dat voor dit jaar hadden gepland, of ons object moet aangepast worden omdat het niet meer voldoet. Nu we toch gaan timmeren / onderhouden, gaan we gelijk de beveiliging op orde brengen. Maar het kan ook zijn dat de bedreigingen zo veranderen dat we de beveiliging moeten aanpassen.

2. Wat gaan we beveiligen
Welk object, waar ligt je systeemgrens voor dit beveiligingsproject.

3. Waartegen gaan we beveiligen
Wie zijn onze belagers, bedoeld en onbedoeld, en waarom zijn ze onze belagers.

4. Voor wie gaan we beveiligen
Wie lopen er risico. Welk risico lopen zij. Levert ons beveiligingsproject een verlaging van hun risico op?

5. Wie hebben we nodig om dit beveiligingsproject te realiseren?
Welke rollen en wie doet wat

6. Wat zijn de risico's
Wat proberen we door te beveiligen te voorkomen? We moeten het wel met elkaar eens zijn over deze lijst van risico's. Alleen dan wil de opdrachtgever betalen en wil de autoriteit de beveiligingsgraad goedkeuren.

7. Wat zijn de maatregelen
Hoe gaan we de risico's mitigeren?

8. Wat zijn onze restrisico's en wat doen we daar mee?
Wat blijft er over, wat kun je niet beveiligen, en welk risico blijft er over. Kunnen we daar nog iets anders mee? Moeten we iemand waarschuwen? Gaat de autoriteit het restrisico accepteren?

Terugblik: vervolg werkgroep

Na afstemming mei 2017 tussen RWS en het COB over de relatie tussen RWS en de COB/KPT-projecten is afgesproken de cybersecurity-activiteiten weer op te starten.

Eerste overleg in de nieuwe samenstelling
20 september 2017 (voorzitter Leen van Gelder)

Terugblik: groeiboek cybersecurity

Groeiboek versie 1 (30-5-2018)
Tunnelbeheerders

Organisatie
En rollen

Update

Projectfases

Groeiboek versie 2 (26-11-2019)
Alle stakeholders en projectfases

Werkgroep cybersecurity en ISAC-tunnels 2020

Werkgroep cybersecurity

Master class

Business case

Update groei-boek

Werkgroep Cybersecurity
Voorzitter
Jasper Kimstra

Inter-nationaal

ISAC-tunnels

Havens
Luchthavens
Zorg
Energie
Water
Nucleair
Telecom

Keren en Beheren
Rijks
Verzekeringen
Financiële instellingen
Pensioenen
Multinationals
Beheerders ICT

+ Tunnels (infrastructurele objecten)

Voorzitter Leen van Gelder

Groeiboek Cybersecurity

Overhandiging en presentatie 1e versie aan Burgemeester van Belzen-Barendrecht

Overhandiging 3e versie aan Leen van Gelder!

Platform Tunnels en veiligheid

De onthulling

Groeiboek Cybersecurity

1. Toelichting nieuwe versie groeiboek- Johannes Braams

2. Volwassenheidsscan-Erik Versteegt

3. In gesprek met de beheerder- Jasper Kimstra

www.cob.nl/groeiboek/cybersecurity

Thema’s 2021

Uw inbreng is van belang!

Mentimeter

Platform Tunnels en veiligheid

Vragen?

Heel graag tot de volgende keer!!!!

Bedankt voor uw aanwezigheid