Tunnels & Cybersecurity

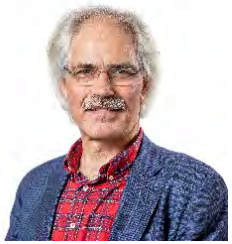
Johannes Braams

Royal HaskoningDHV

7 oktober 2020

Nederlands kenniscentrum voor ondergronds bouwen en ondergronds ruimtegebruik

Even voorstellen



Johannes Braams

- Senior adviseur Cyber Security Industriële Automatisering Royal HaskoningDHV
- Lid werkgroep Groeiboek Cybersecurity COB
- Lid Industrieel Platform Cyber Security NEN

- ✓ GICSP: Global Industrial Cybersecurity Professional
- ✓ CISSP: Certified Information Systems Security Professional
- ✓ IEC 62443 gecertificeerd

Wat is Cybersecurity?

Cybersecurity is het geheel aan technische, organisatorische en fysieke maatregelen om schade door verstoring, uitval of misbruik van ICT systemen (en van IA-systemen) te **voorkomen**.

Die schade kan bestaan uit de aantasting

- de **V**eiligheid,
- **B**eschikbaarheid,
- **I**ntegriteit of
- **V**ertrouwelijkheid

van systemen en de daarin opgeslagen informatie dan wel (IA) de door die systemen bestuurde processen.

Proactief

Wat is Cyberweerbaarheid?

Cyber weerbaarheid is het geheel aan technische, organisatorische en fysieke maatregelen die er op zijn gericht om, in geval van een verstoring van de ICT/IA-systemen (b.v. t.g.v. een aanval), de gevolgen van de verstoring tot een minimum te beperken.

- Duur van de verstoring
- Impact van de verstoring
- Forensisch bewijs (!)

Reactief

Waarom Cybersecurity en Cyberweerbaarheid?

- Cybersecurity in de infrastructuur is belangrijk om de *kans* op verstoring van het functioneren van het object, met als mogelijk gevolg verkeersopstoppingen, ongevallen en economische schade onder een acceptabele grens te brengen en houden.
- Cyberweerbaarheid in de infrastructuur is belangrijk om de gevolgen van een verstoring van het functioneren van het object te beperken tot een maximaal geaccepteerde duur en omvang.

Balans

Organisatie

Processen

Techniek

Balans

Geld

Gebruiksgemak

Risiconiveau

Stellingen

1. Ik weet als beheerder c.q. onderhouder precies wie in mijn complex aanwezig is.
   1: Altijd, 2: Meestal, 3: Soms, 4: Nooit
2. Ik weet als beheerder c.q. onderhouder precies wat de aanwezigen doen in mijn complex.
   1: Altijd, 2: Meestal, 3: Soms, 4: Nooit
3. Als een monteur voor zijn werk een laptop moet aansluiten dan gebruikt hij
   1: Zijn eigen laptop
   2: Zijn eigen laptop nadat hij heeft aangetoond dat deze virusvrij is
   3: Een op het complex aanwezige laptop die nooit aan een ander netwerk wordt gekoppeld

Stellingen (2)

4. Als iemand een apparaat op het netwerk in mijn complex aansluit dan
    1. *Krijg ik een alarm bericht en kan het apparaat geen verkeer versturen/ontvangen*
    2. *Krijg ik een alarm bericht maar het apparaat krijgt toegang tot het netwerk*
    3. *Het apparaat krijgt toegang tot het netwerk, dit staat in de logging*
    4. *Het apparaat krijgt toegang tot het netwerk.*

Stellingen (3)

5. Ik weet als beheerder c.q. onderhouder welke apparatuur en software in mijn tunnel aanwezig is.
   1. *Nee, ik heb geen idee*
   2. *Alleen op basis van de As-Built documentatie*
   3. *Op basis van de As-Built documentatie en de beschrijving van de uitgevoerde wijzigingen*
   4. *Op basis van mijn Configuration Management Database (CMDB) die bij elke wijziging wordt bijgewerkt*

Stellingen (4)

6. Ik weet als beheerder c.q. onderhouder welke risico's ik loop
   1. *Nee, geen idee*
   2. *Ja, ik denk het wel*
   3. *Ja, op basis van een risicoanalyse*
   4. *Ja, op basis van een risicoanalyse met door het management geaccepteerde rest-risico's*
7. Ik weet als beheerder c.q. onderhouder wat ik moet doen als een risico zich voordoet
   1. *Nee, er kan toch niks gebeuren*
   2. *Nee, dat ga ik dan uitzoeken*
   3. *Ik ga dan eerst het Incident Response Plan opzoeken en doornemen*
   4. *Ja, we oefenen jaarlijks met een Incident Response Plan*

Bedreigingen en Risico's tunnel

- **Bedreiging**:
  Een niet geautoriseerd persoon heeft fysiek toegang tot bedien- en technische ruimten van een tunnel.

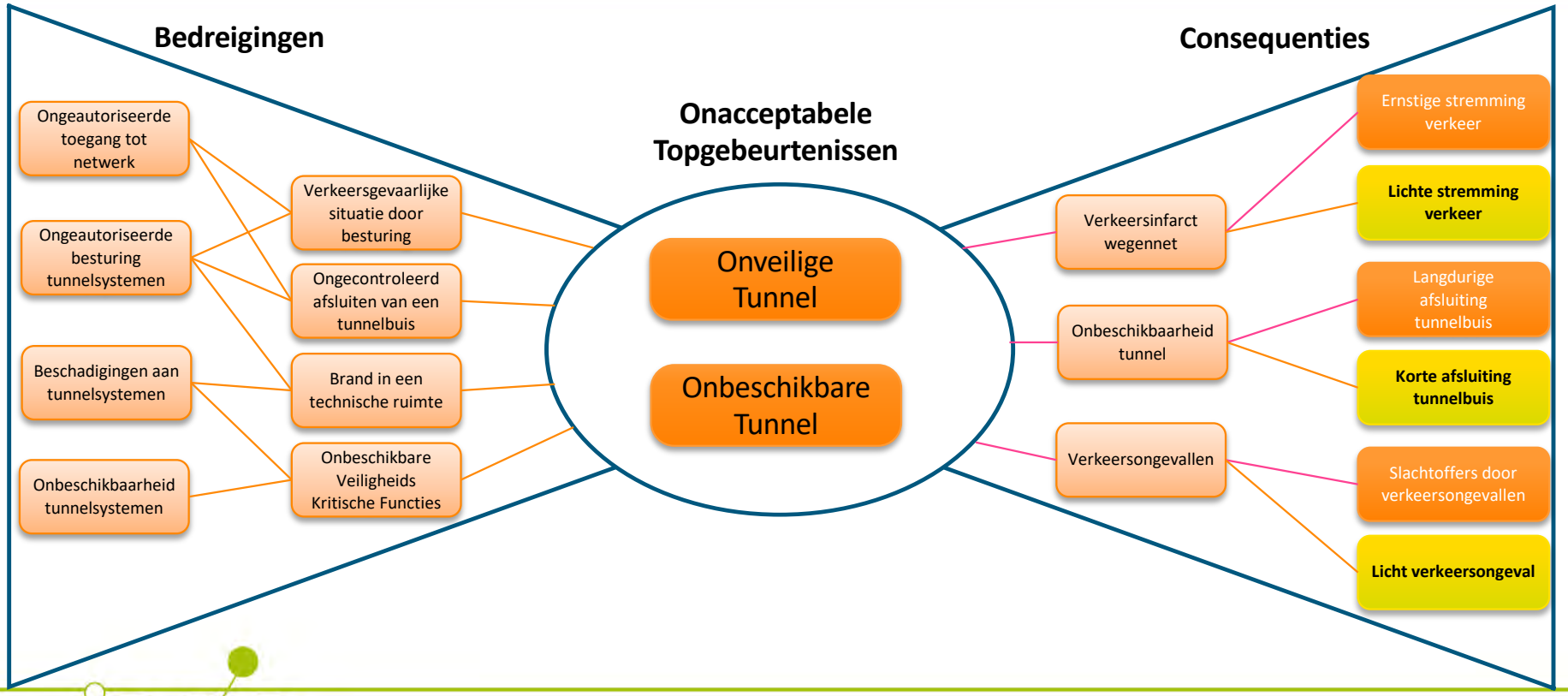
- Risico:
  Als een niet geautoriseerd persoon toegang heeft tot de technische ruimte van een tunnel *dan* kan hij de IA-systemen uitschakelen met als gevolg dat de tunnel niet beschikbaar wordt.

Zwakheden en Risico's tunnel

- **Zwakte**:
  Gebeurtenissen in de apparatuur worden door het Operating Systeem niet in de logging vastgelegd.

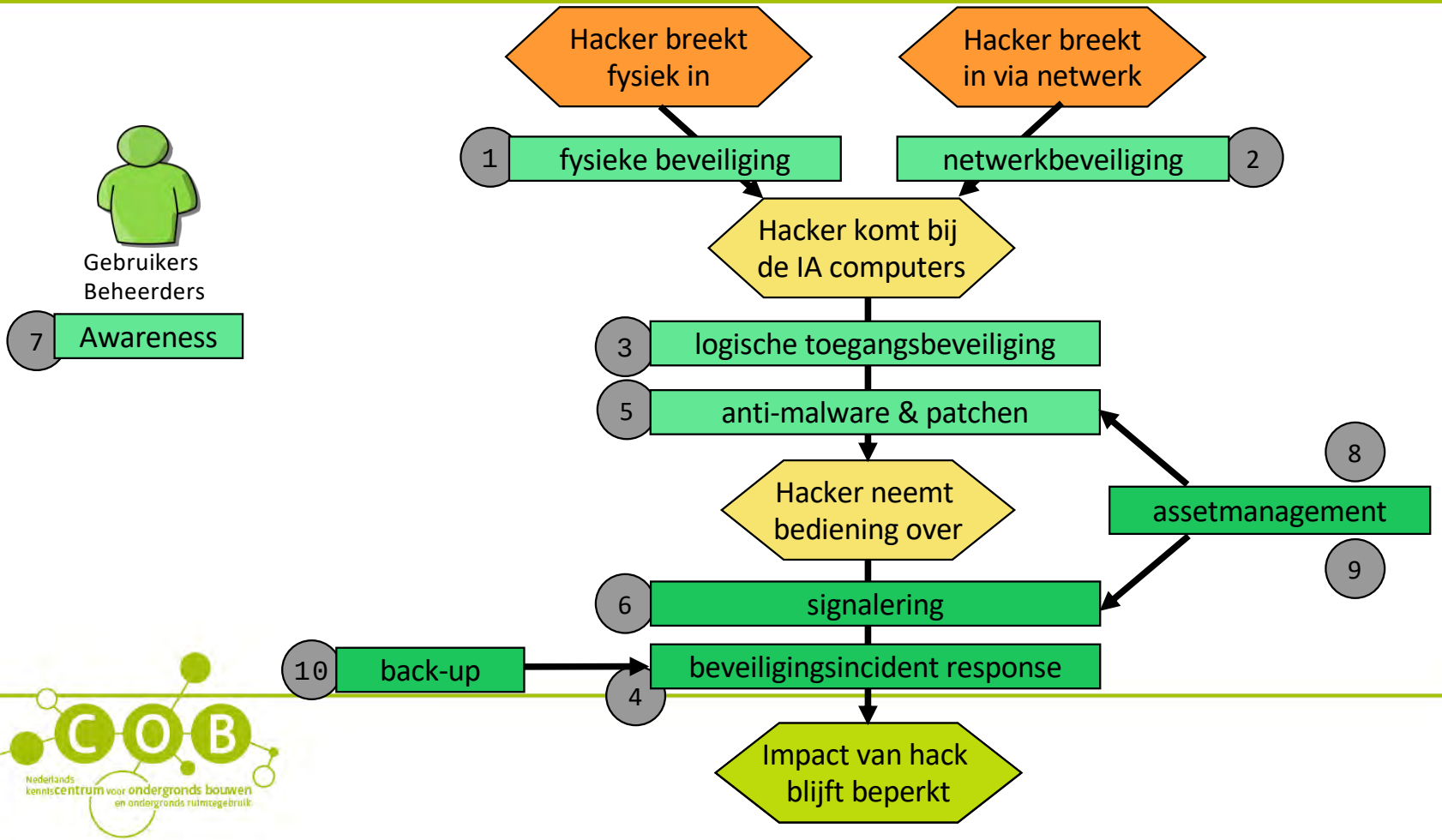
- Risico:
  Als een onbekend proces wordt gestart op een besturingscomputer en dat wordt niet gelogd *dan* is dat feit achteraf niet zichtbaar in de logging met als gevolg dat als zich onverwachte gebeurtenissen voordoen niet is vast te stellen wat daarvan de oorzaak was.

Vlinderdas model



COB Nederlands kenniscentrum voor ondergronds bouwen en ondergronds ruimtegebruik

Risico Reductie Diagram



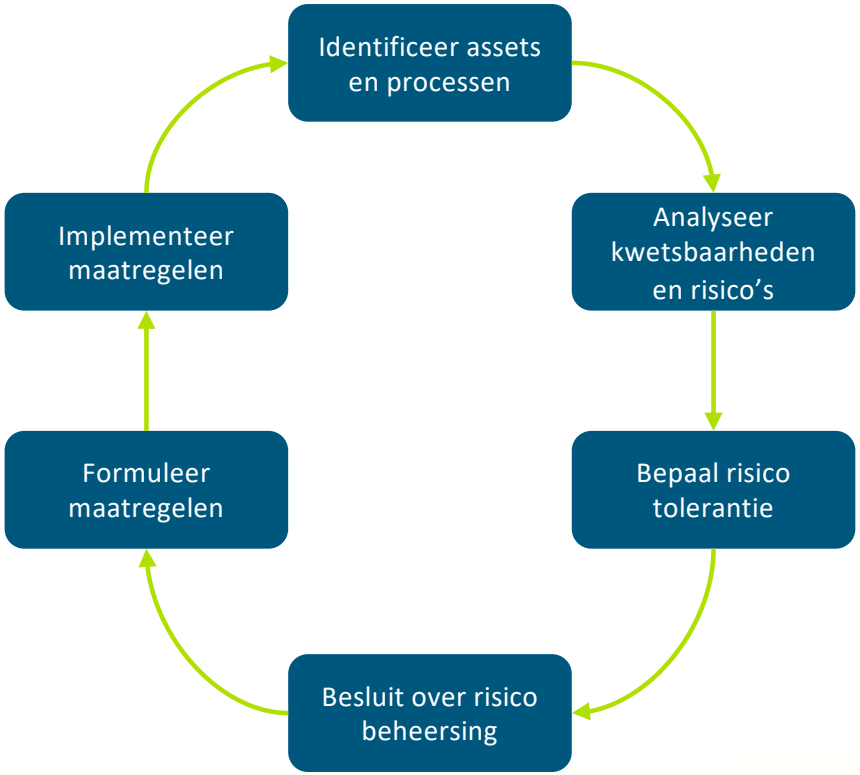
Weerbaarheid in de levenscyclus

- Ontwerp
  - Security by design
  - Cybersecurity in het eisenpakket van de opdrachtgever
  - Vanaf het eerste voorlopige ontwerp via alle ontwerp- en realisatiestappen tot en met sloop
- Verificatie & Validatie
- **Continue bewaken tijdens de levensloop**
- Asset management
  - Identificeren van alle componenten
  - Netwerk analyse
  - **Terugkerende risico analyse (model based)**
  - Scenario's en simulaties

COB
Nederlands kenniscentrum voor ondergronds bouwen en ondergronds ruimtegebruik

Dreigingen en risico’s beheersen

1. Identificeer het systeem
   - Identificeer en specificeer alle (sub)systemen en processen
   - Voor risico analyses uit
2. Kies de vereiste acties
   - Besluit de risico tolerantie
   - Besluit welke risico’s beheerst moeten worden
3. Ontwerp en implementeer oplossingen
   - Formuleer maatregelen
   - Implementeer de maatregelen
   - Analyseer de nieuwe situatie



Nederlands kenniscentrum voor ondergronds bouwen en ondergronds ruimtegebruik

Groeiboek Cybersecurity V1.0

Versie 1.0 gepubliceerd november 2018

- Deze versie was primair gericht op de beheerders van tunnelobjecten
- Inhoud:
  - Wet- en regelgeving
  - Risico gestuurde aanpak
  - Maatregelen
  - Borging
  - Ervaringen uit de praktijk

Groeiboek Cybersecurity V2.0

Versie 2.0 gepubliceerd november 2019

- Uitbreiding van de inhoud gericht op nieuwbouw en renovatie projecten, inclusief de sloop activiteiten:
  - Update van de bestaande hoofdstukken
  - Contractvormen
  - Initialisatie en aanbestedingsfase
  - Ontwerpfase
  - Realisatiefase (Nieuwbouw én renovatie)
  - Exploitatiefase
  - Sloop
  - Verificatie en validatie
  - Incident en herstel
  - Voorlichting, opleiding, training en oefenen

Groeiboek Cybersecurity V2.5

Versie 2.5 te publiceren december 2020

- Verbetering van de leesbaarheid, toevoegen van onderwerpen:
  - Cybersecurity Business Case
  - Volwassenheidscan van de organisatie
  - Cybersecurity en Safety

Cyber Security Implementatie Richtlijn

- Ontwikkeld in 2014/2015 door RWS
- Gebaseerd op:
  - Baseline Informatiebeveiliging Rijksdienst (**BIR**, **ISO 27001/2**)
  - NCSC Checklist ICS/SCADA
  - NIST SP800-82
  - **IEC 62443-2-1**
- Maatregelpakketten
  - Mens
  - Procedures & Organisatie
  - Techniek
- Geflankeerd met standaard contractbepalingen (Proces en Techniek)

Maatregelpakketten CSIR

1. Fysieke Toegang
2. Logische Toegang
3. Beveiligingsincidenten en Incident Response
4. Netwerkkoppelingen
5. Bescherming tegen malware, hardening en patching
6. Logging en Monitoring
7. Bewustwording en training
8. Gecontroleerd wijzigen
9. Beheer en Onderhoud
10. Back-ups

Ontwikkeling nieuwe versie CSIR

- Algemene Ontwikkelingen
  - Baseline Informatiebeveiliging Overheid (**BIO**) vervangt BIR, IBI, BIG en BIWA
  - Van IEC 62443 zijn de afgelopen jaren meer delen gepubliceerd
  - Ervaringen opgedaan met gebruik CSIR v1.4
  - CSIR wordt ook gebruikt buiten RWS
- Nieuwe versie ontwikkeld op basis van ontwikkelingen
- Status: concept wordt nu gereviewed.

Bedankt voor uw aandacht