Hoewel het groeiboek geschreven is voor tunnels, is de inhoud breed toepasbaar op alle **infrastructurele werken met industriële automatisering**, zoals bruggen, sluizen en stuwen. Het groeiboek biedt informatie voor alle betrokken partijen en in alle projectfasen.

Cybersecurity tunnels

COB
Nederlands kenniscentrum voor ondergronds bouwen en ondergronds ruimtegebruik

Over cybersecurity is weliswaar veel informatie beschikbaar, maar vaak is het moeilijk hierin de juiste weg te vinden en goede afwegingen te maken. Het COB-netwerk heeft daarom speciaal voor infra-objecten een openbaar toegankelijk groeiboek over cybersecurity opgesteld. Het digitale document beschrijft de gehele levenscyclus van een infra-object, van planfase tot sloop, en beschrijft voor alle betrokken stakeholders de taken en verantwoordelijkheden op het gebied van cybersecurity. Het is belangrijk dat men zich ervan bewust wordt hoeveel en welk werk er verzet moet worden en dat je cybersecurity er 'niet zomaar even bij doet'.

Het groeiboek is opgesteld door een COB-werkgroep met ca. veertig deelnemers vanuit overheden en marktpartijen zoals ingenieursbureaus, systemintegrators, leveranciers en cyberbeveiligingsbedrijven. Het boek is globaal op te delen in:

- Theoretische beginselen (bewustwording, wet- en regelgeving, organisatie, risicogestuurde aanpak, verificatie en validatie, monitoring, en incident en herstel)
- Aandachtspunten per projectfase: planfase en aanbesteding, realisatie (nieuwbouw), exploitatie (dagelijks beheer en renovatie) en sloop. Per fase worden de taken, bevoegdheden en verantwoordelijkheden, fase-specifieke risico's, maatregelen en borging beschreven.
- Ervaringen uit de praktijk.

Het groeiboek is gratis online te raadplegen op
www.cob.nl/groeiboek/cybersecurity

Cybersecurity tunnels

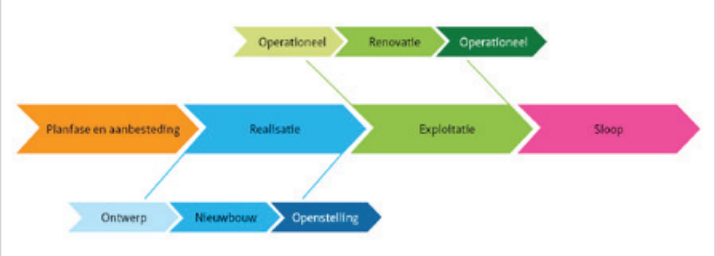
Alert en kundig
Bewustwording is de goedkoopste en meest effectieve methode om een basis te leggen voor cybersecurity binnen een organisatie. Je maakt mensen alert en kundig. Naast deze bewustwording van alle bij de tunnel betrokken personen, moeten er specifieke functionarissen benoemd zijn én gelden er enkele specifieke eisen met betrekking tot medewerkers die operationeel zijn bij het beheer van de tunnel (eigen en ingehuurd personeel).

Wet- en regelgeving
Operationele veiligheidregimes zijn primair de kaders voor cybersecurity: tunnelveiligheid (tunnelwet, TSI-SRT – *technical specifications for interoperability safety in railway tunnels*), spoorveiligheid (Spoorwegwet, Wet lokaal spoor), de publieks-, arbo-, milieu- en sociale veiligheid, etc. In deze regelgeving wordt cybersecurity (nog) niet specifiek benoemd, maar stakeholders bij de realisatie en het beheer van een infra-object kunnen de cybersecurityrisico's – anno 2019 – niet negeren bij het beheersen van de veiligheidsrisico's.

Organisatie van cybersecurity
Door taken, verantwoordelijkheden en bevoegdheden op het gebied van cybersecurity in de organisatie in te bedden, zal cybersecurity onderdeel uitmaken van de standaard processen van de organisatie. Doel van deze aanpak is te bewerkstelligen dat:

1. Cybersecurityrisico's worden onderkend en geprioriteerd.
2. Maatregelen worden geformuleerd en belegd bij personen met vakkennis, zodat deze maatregelen op een juiste wijze worden geïmplementeerd.
3. Instandhouding en evaluatie van maatregelen wordt getoetst aan wet- regelgeving en veranderende dreigingen.

+ Specifieke aspecten in projectfases
In elke projectfase kent cybersecurity een aantal specifieke aspecten. De taken, bevoegdheden en verantwoordelijkheden kunnen bijvoorbeeld per fase verschillen. Daarnaast zijn de risico's niet altijd hetzelfde, waardoor er ook andere maatregelen nodig zijn.



+ Ervaringen uit de praktijk
Het groeiboek wordt gecompleteerd met een aantal bevindingen uit de praktijk, bijvoorbeeld geconstateerd bij inspecties en na evaluaties van incidenten. Hierbij worden voorbeelden van beheersmaatregelen genoemd die getroffen kunnen worden om weerbaar te zijn tegen cyberrisico's. De voorbeelden laten wederom zien dat je cybersecurity er 'niet zomaar even bij doet'.

Het groeiboek is te vinden op
www.cob.nl/groeiboek/cybersecurity

Risicogestuurde aanpak
In het groeiboek wordt een risicogestuurde aanpak beschreven die de stakeholders in staat stelt de weerbaarheid van hun object/project te beoordelen en processen zodanig te optimaliseren dat tijdig de juiste maatregelen kunnen worden genomen om cyberincidenten te voorkomen of te beheersen. De handreiking helpt partijen ook om eventueel opgetreden effecten bij incidenten te kunnen mitigeren. De aanpak bestaat uit zes stappen die telkens herhaald worden:

1. Inventariseren van de situatie/het ontwerp.
2. Opstellen van de risicoanalyse.
3. Keuze van de te nemen maatregelen.
4. Evalueren van de restrisico's en acceptatie restrisico's.
5. Uitvoeren van de maatregelen.
6. Borgen maatregelen (inclusief verificatie en validatie).

Verificatie en validatie
Veiligheidsvoorzieningen moeten niet alleen aanwezig zijn, maar ook aantoonbaar correct werken. Dat geldt eveneens voor cybersecuritymaatregelen: ook voor dit type veiligheid is verificatie en validatie vereist.

Met verificatie wordt objectief en expliciet aangetoond dat een oplossing voldoet aan de gestelde eisen. Validatie toont aan dat een oplossing geschikt is voor het beoogd gebruik. Voor cybersecurity geldt bovendien dat bij de verificatie en validatie nadrukkelijk moet worden gekeken naar afwijkende situaties. Met andere woorden: niet alleen het '*sunny day*'-scenario testen, maar juist ook (meerdere) '*rainy days*'.

Monitoring
Ondanks alle maatregelen is het onmogelijk om cyberincidenten geheel te voorkomen. Bovendien wordt er meestal een zeker restrisico geaccepteerd. Met de inrichting van cybersecuritymonitoring van de technische systemen wordt continu de status van de digitale veiligheid in de gaten gehouden. Zo kunnen nieuwe kwetsbaarheden gesignaleerd worden en cyberincidenten beter gedetecteerd en afgehandeld worden. Het doel van monitoring is het herkennen van afwijkend gedrag (voor het detecteren van een incidentdreiging), het vastleggen van relevante gebeurtenissen en het verzamelen van bewijs. De Baseline informatiebeveiliging overheid (BIO) vraagt maatregelen om aan deze doelstelling te kunnen voldoen. De verantwoordelijkheid voor het voldoen aan de BIO ligt bij de beherende partij.

Incident en herstel
Een cyberincident is een gebeurtenis of actie waarbij de beveiliging van hardware, software, informatie, een proces of organisatie mogelijk in gevaar is gebracht of geheel of gedeeltelijk is doorbroken. Een dergelijk incident is niet altijd zichtbaar en wordt niet altijd als zodanig herkend. Daarom is bewustwording en training in het herkennen en melden van incidenten een belangrijke eerste stap. Na een melding is het zaak het incident te classificeren (hoe ernstig is het?) en te prioriteren (niveau van opschaling). Vervolgens wordt het incident toegekend aan een responsteam. Dat team bepaalt de corrigerende maatregelen, legt deze vast in een herstelplan en voert ze uit. Om van het incident te leren, vindt er een evaluatie plaats en wordt informatie gedeeld.