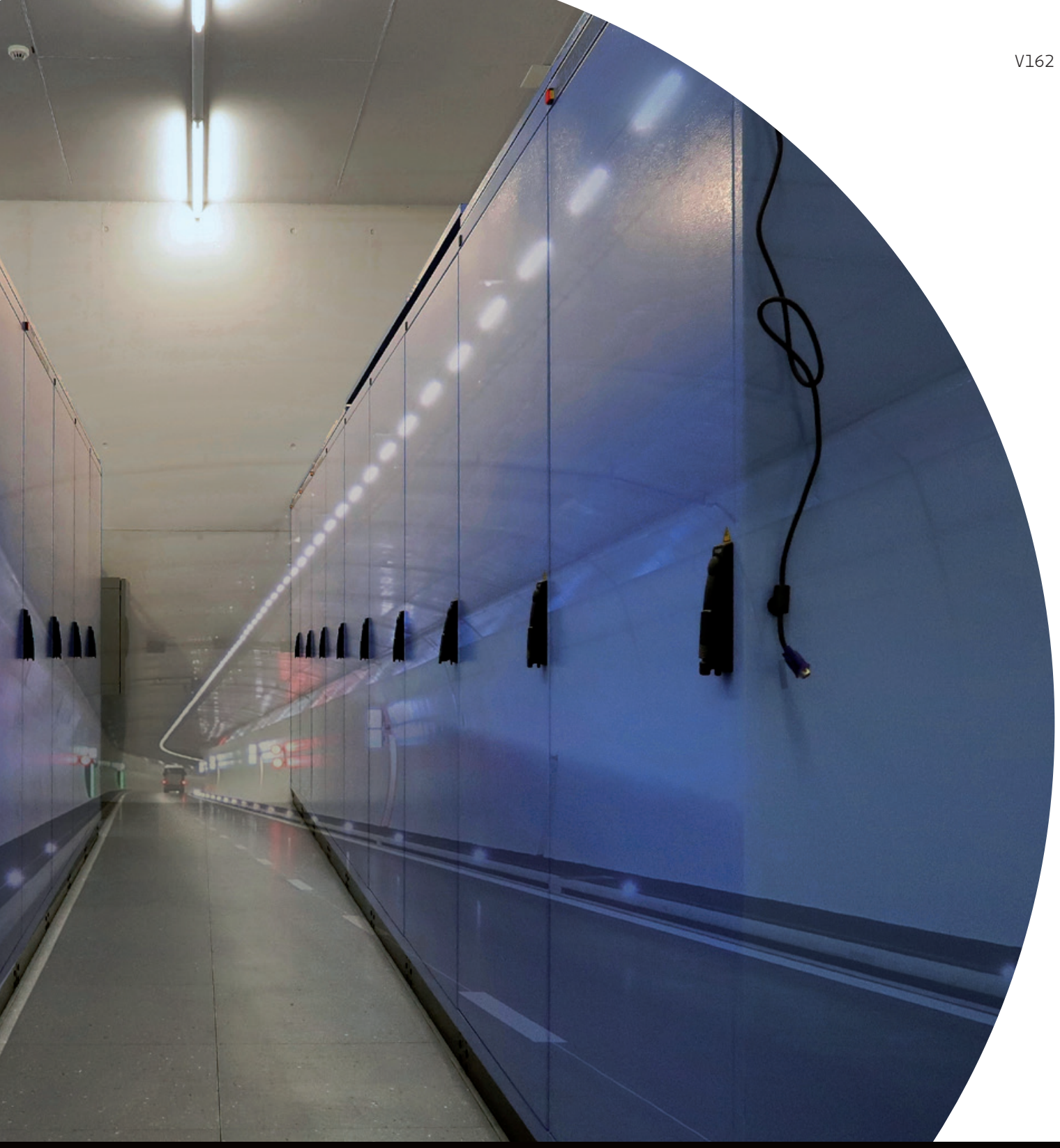


Cybersecurity en tunnelveiligheid

Aanbevelingen voor cybersecurity als aspect in toetskader tunnelveiligheid

COB
Nederlands kenniscentrum voor ondergronds bouwen en ondergronds ruimtegebruik

Cybersecurity en tunnelveiligheid

Aanbevelingen voor cybersecurity als aspect in toetskader tunnelveiligheid

Inhoudsopgave

1 Inleiding

Een ogenschijnlijk (en op papier) veilige tunnel kan wel degelijk onveilig zijn zonder dat de verantwoordelijke tunnelbeheerder en zijn veiligheidsbeambte zich daarvan bewust zijn. Dat komt doordat cyberveiligheid (vanaf nu: cybersecurity) vooralsnog geen onderdeel is van het toetskader voor tunnelveiligheid zoals bedoeld in de tunnelwetgeving.

Dit memo beschrijft hoe inhoud kan worden gegeven aan cybersecurity in relatie tot veiligheid in het algemeen en tunnelveiligheid in het bijzonder. Hiermee kan dit aspect worden geïntegreerd in het toetskader voor tunnelveiligheid, waarmee het een integraal onderdeel wordt van het tunnelveiligheidsdossier van de veiligheidsbeambte.

HOOFDSTUK 5 toont een voorbeeld uit de praktijk. Hier staat beschreven hoe operationele procesbewaking van cybersecurity bij Rijkswaterstaat is geïntegreerd in de bestaande procesbewaking van de tunnel en hoe de informatiestroom zou kunnen verlopen.

2 Probleemstelling

In de Wet aanvullende regels veiligheid wegtunnels (Warvw) in artikel 5, lid 3 is aangegeven dat de veiligheidsbeambte, aangewezen door de tunnelbeheerder, alle preventieve en veiligheidsmaatregelen coördineert ter verzekering van de veiligheid van de tunnelgebruikers en het tunnelpersoneel. Het aspect cybersecurity is vooralsnog echter geen onderdeel van zijn toetskader. De wet regelt dat er wordt getoetst op een planologisch besluit bij de afgifte van een omgevingsvergunning voor de activiteit bouwen en bij de afgifte van een openstellingsvergunning. Doordat cybersecurity ontbreekt in het toetskader, is (of lijkt) cybersecurity geen onderdeel te zijn van het tunnelveiligheidsplan (TVP), veiligheidsbeheerplan (VBP)[1] en tunnelveiligheidsdossier (TVD)[2].

De veiligheidsbeambte baseert zijn advies aan de tunnelbeheerder op de zelfredzaamheid van de tunnelgebruikers en de aanwezigheid van afdoende veiligheidsvoorzieningen. De mate van cybersecurity en het weerstandsniveau worden niet meegewogen in het advies ten aanzien van de openstellingsvergunning, zowel bij bestaande als bij nieuw te bouwen tunnels.

Cyberincidenten
Het voorkomen of afhandelen van een cyberincident is, in tegenstelling tot welke vorm van fysiek incident ook, niet binnen de veiligheidsketen geregeld. Hierdoor zijn de verantwoordelijke tunnelbeheerder en veiligheidsbeambte zich niet bewust (of worden zij in elk geval onvoldoende bewust gemaakt) van de risico's en mogelijke consequenties van cyberincidenten. Zoals het zich momenteel laat aanzien, worden beide functionarissen niet geïnformeerd bij een cyberincident, omdat de IT-infrastructuur feitelijk niet actief wordt gemonitord en bewaakt. Hierdoor kan een fysiek incident wel degelijk het gevolg zijn van een cyberincident, maar wordt dat, omdat het cyberincident niet wordt gedetecteerd, niet meegenomen als mogelijke oorzaak. Dit komt pas veel later tot uiting nadat het fysieke incident is onderzocht en de besturingssystemen bij dat onderzoek betrokken worden.

Geslaagde hackpogingen
Een concreet voorbeeld van een geslaagde hackpoging is die bij de rioleringspompen en gemalen van de gemeente Veere (2012). Via internet waren deze bereikbaar met het eenvoudige wachtwoord 'Veere'. Er was geen materiële schade, maar wel vertrouwensschade. Een ander voorbeeld komt uit 2017. Toen werd de Maersk-terminal in Rotterdam door een cyberaanval voor aantal dagen platgelegd, met enkele miljoenen Euro's schade tot gevolg.

1 Zoals beschreven door IFV in Bestuurlijke handreiking openstellingsvergunning wegtunnels, 10 mei 2019

2 Zoals beschreven in RWS Richtlijn structuur en inhoud tunnelveiligheidsdossier, 25 juni 2014.

Verplicht
Met het in werking treden van de Wet beveiliging netwerk- en informatiesystemen (Wbni) per 9 november 2018, is de wettelijke verplichting ontstaan om systemen tegen de risico's van cyberincidenten te beveiligen. In vervolg hierop heeft de Minister van Infrastructuur en Waterstaat in een brief aan de Tweede Kamer (10 maart 2020, kenmerk IENW/BSK-2020/26291) aangegeven te starten met een nadere invulling van deze wet. Hierin heeft zij de bediening van bruggen en tunnels als onderdeel van het (hoofd) spoorwegennet en (hoofd)wegennet als vitaal B geclassificeerd. In dezelfde brief geeft de minister aan dat de aanbieders van essentiële diensten bij wet verplicht zijn om maatregelen te nemen voor de beveiliging van hun ICT (zorgplicht) en ernstige incidenten te melden (meldplicht). Er staat echter niet beschreven wat de relatie is met de wet- en regelgeving die van toepassing is op tunnels.

(On)voorspelbaarheid
Een groot verschil tussen cybersecurity en bijvoorbeeld constructieve veiligheid is de voorspelbaarheid. Voor constructieve veiligheid geldt dat op basis van kennis een redelijk goede voorspelling te maken is van de veroudering van een constructie en daarmee de degradatie in de tijd. Op basis daarvan kan vervolgens bepaald worden met welk interval er inspecties moeten plaatsvinden om met een bepaalde zekerheid uitspraken te kunnen doen over de veiligheid van de constructie.

Bij cybersecurity ontbreekt deze voorspelbaarheid. Een systeem dat nu malware-vrij is, kan door een geslaagde hack morgen besmet zijn. Waar op dit moment geen inloggegevens in onbevoegde handen zijn, kan morgen door social engineering een medewerker toch (veelal onbewust) zijn wachtwoord prijsgeven. In een besturingssysteem dat nu veilig wordt geacht, kan morgen een nieuwe kwetsbaarheid worden ontdekt, waardoor toegang door onbevoegden mogelijk wordt. Deze onvoorspelbaarheid vraagt om een ander perspectief bij het vaststellen van het maatregelenpakket om de cybersecurity te borgen. Om tijdens de hele levenscyclus van de tunnel de veiligheid te kunnen waarborgen, is er een reguliere bijstelling van de risicoanalyse nodig, evenals het permanent monitoren op nieuwe kwetsbaarheden en het bijstellen van maatregelen. Meer informatie hierover is te vinden in het groeiboek Cybersecurity tunnel op www.cob.nl/groeiboek/cybersecurity. Ook interessant is het artikel *Geen safety zonder cybersecurity*, door Marcel Jutte en William van der Veen (Hudson Cybertec), in Process Control, nummer 4, 2019. Dit artikel is online te vinden op www.hudsoncybertec.com/wp-content/uploads/2019/06/Process-Control-Geen-safety-zonder-cybersecurity.pdf

3 Aanbevelingen

Cybersecurity moet deel uitmaken van de veiligheidsanalyse van de tunnel en worden opgenomen in het toetsinstrumentarium, zodat elke veiligheidsbeambte (rijkstunnels en niet-rijkstunnels) een instrument heeft om zijn tunnelbeheerder te adviseren over het borgen van cybersecurity.

Om over het aspect cybersecurity en het weerstandsniveau een uitspraak te kunnen doen, zal de veiligheidsbeambte aanvullende expertise moeten inschakelen omdat hier specifieke kennis voor nodig is. De uitspraak kan hij vervolgens meenemen in zijn advies voor een uiteindelijke openstelling.

Daarnaast zal de tunnelbeheerorganisatie moeten voorzien in monitoring van de tunnelfunctionaliteit, zodat continu bewaking van de cybersecurity van de tunnel kan worden uitgevoerd en bij een cyberincident direct kan worden beoordeeld of (direct) ingrijpen noodzakelijk is.

4 Uitwerking en consequenties

4.1 KPI's en veiligheidsincidenten

Voor een object kunnen KPI-afspraken worden gemaakt ten aanzien van veiligheid. Deze KPI's worden mede bepaald door het geaccepteerde restrisico. In onderstaande tabel is een voorbeeld gegeven om de KPI's voor verschillende typen incidenten vast te leggen. De KPI wordt uitgedrukt in een acceptabel aantal incidenten van een bepaalde soort en impact per jaar.

Tabel 4.1 / Operationele KPI's, restrisico op incidenten

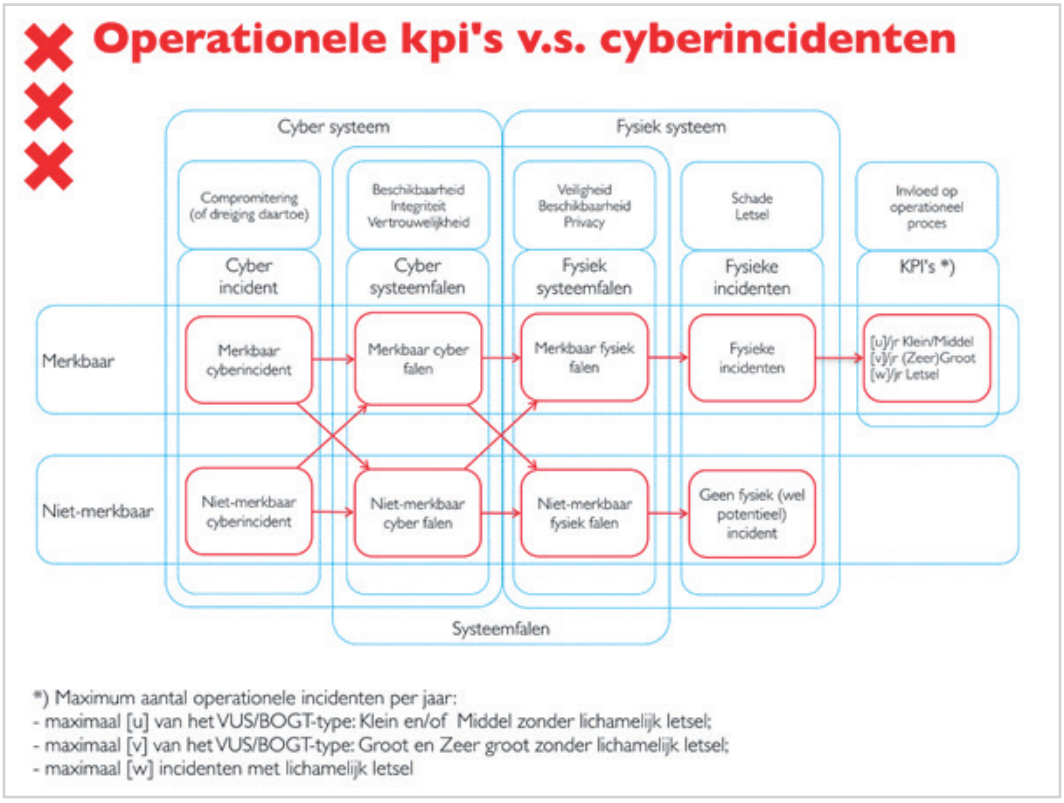
Incidententype	Acceptabel aantal incidenten per jaar	Ernst	Criteria
Veiligheid (letselincidenten)	...	Groot	Dodelijke slachtoffers
	...	Klein	Gewonden
Beschikbaarheid (storingen)	...	Groot	MTTR>
	...	Middel	MTTR> en <
	...	Klein	MTTR<
Privacy (incidenten)	...	Groot	Aantal personen>
	...	Klein	Aantal personen<

MTTR = *Mean time to repair*, gemiddelde tijd nodig voor reparatie.

Om de KPI's te bepalen, wordt meestal onderscheid gemaakt tussen letselincidenten en overige incidenten. Vanuit een arboveiligheidsbeleid staat een streven naar nul letselincidenten voorop. De KPI's voor de beschikbaarheid worden afgeleid uit de RAMS-analyse, waarbij de contractueel vereiste beschikbaarheid afgewogen wordt tegen de benodigde maatregelen hiervoor. Hierbij wordt een kosten-batenanalyse gemaakt voor de inspanning die nodig is om het incident te voorkomen vs. de kosten daarvoor. Voor de privacy geldt een wettelijke grondslag met een afweging van het type overtreding, de ernst, omvang en duur van de overtreding en of er sprake is van opzet of recidive. Dit wordt vertaald in boetebeleidsregels in verschillende categorieën. Een verantwoord bedrijfsbeleid streeft natuurlijk naar nul privacy-incidenten. De eerlijkheid gebiedt te zeggen dat ook hier ook een kosten-batenanalyse aan ten grondslag kan liggen.

Onderstaande afbeelding visualiseert de relatie tussen deze KPI's en cybersecurity. Om cyberincidenten te kunnen detecteren, is monitoring essentieel. Een cyberincident (merkbaar of niet-merkbaar) kan leiden tot een systeemfalen (merkbaar/niet-merkbaar) met een mogelijk fysiek incident tot gevolg. Voor een begrip van deze relatie is het essentieel om een duidelijk inzicht te hebben in de aard van de verschillende incidenten. Een cyberincident kan leiden tot een verhoogd risico op een

fysiek incident. Naast het beoordelen vanuit de fysieke veiligheid zal een cyberincident ook beoordeeld moeten worden vanuit veiligheidsaspecten zoals privacy en vanuit gevolgen voor de beschikbaarheid van het object.



Figuur 4.1 / Cyberincidenten leiden tot fysieke incidenten. (Bron: Wim van Asperen, gemeente Amsterdam)

4.2 Relatie cybersecurity en integrale veiligheid

Wettelijk gezien is de tunnelbeheerder volledig verantwoordelijk voor de integrale veiligheid van de wegtunnel. De uitvoering van de taken voor de operationele veiligheid zijn neergelegd bij de bedienaar.

Onderstaande afbeelding toont de verschillende aspecten van integrale veiligheid in hun samenhang, zoals deze bij Rijkswaterstaat wordt beschreven in het Kader integrale veiligheid in projecten.

Integrale Veiligheid	Interne Veiligheid	Algemeen	Constructieve veiligheid	
			Brandveiligheid	
			Arbeidsveiligheid	
			Sociale veiligheid	
			Security	
		Modaal/ Sectoraal/Object-gericht	Veilgheid Wegverkeer	Verkeersveiligheid
				Tunnelveiligheid
				Machineveiligheid
			Zee- en binnenvaart	
			Spoorwegveiligheid	
			Veiligheid tegen overstroming	
	Externe Veiligheid	Gevaarlijke stoffen	Inrichtingen	
			Transport	
	Hulpverlening	(Bereikbaarheid)		
		(Middelen)		
		(Organisatie)		

Figuur 4.2 / Aspecten uit RWS Leidraad integrale veiligheid. Constateer dat deze tabel niet alleen op de droge maar ook natte infra van toepassing is.

Voor het bepalen van de definities van en eisen aan integrale veiligheid wordt gebruikgemaakt van de (vigerende versie van de) volgende documenten:

- Leidraad integrale veiligheid
- Model integraal veiligheidsplan
- Veiligheidsplan
- Toetskader veiligheidsbeambte RWS
- Kader integrale veiligheid in projecten

Opvallend, maar feitelijk ook weer niet heel vreemd, is dat het relatief jonge aspect cybersecurity geen onderdeel uitmaakt van integrale veiligheid. Cybersecurity-maatregelen dragen wel degelijk bij aan de integrale veiligheid van het te beveiligen object. Door gebrekkige cybersecurity kunnen bijvoorbeeld andere genomen beveiligingsmaatregelen buiten werking worden gesteld.

In onderstaande tabel wordt de relatie gelegd tussen de aspecten van integrale veiligheid en cybersecurity. Hierbij wordt in twee richtingen gekeken. De ene kolom beschrijft de impact op veiligheidsrisico's als de cybersecurity niet op orde is; de andere kolom beschrijft welke cybersecurityrisico's er ontstaan door een gebrekkige veiligheid.

Tabel 4.2 / Relatie tussen de aspecten van integrale veiligheid en cybersecurity.

Onderwerp	Risico's bij gebrekkige cybersecurity	Risico's voor cybersecurity	Toelichting
Constructieve veiligheid	Nee	Kritische ruimten, en toegangen tot die ruimten, dienen voldoende inbraakwerend te zijn. Denk ook aan kabelwegen en toegang via kruipruimtes.	Mogelijk kan uit documenten informatie komen betreffende zwakste plekken in de constructie. Classificatie van informatie en veilig omgaan met informatie is van belang.
Brandveiligheid	Brandmeldingen worden niet doorgegeven door een hack, overbelast netwerk, of storing in de meldkamer.	Risico op ongeoorloofde toegang doordat bij brand er vaak automatisch openende deuren zijn. Verlies van gegevens (incl. back-ups) en systemen.	
Arbeidsveiligheid	Nee	Indirect	Goede arboveiligheid draagt bij aan gestructureerd en netjes werken. Dat is zeker ook goed voor cybersecurity.
Sociale veiligheid	Persoonsgegevens vallen in verkeerde handen, camerabeelden worden openbaar, monitoringcamera's werken niet en daarmee is geen sociale controle mogelijk.	Hack middels aansluitingen op camerasystemen.	
Security	Inbraak wordt niet opgemerkt doordat de bewakingsinstallatie het niet doet.	Toegang tot kritische ruimten en informatie.	Denk aan inbraakwerendheid.
Verkeersveiligheid (incl. vandalisme en betreding)	Verkeersregelinstallaties werken niet (goed), wegkantsystemen werken niet.	Verkeersinstallaties zijn ook onderling gekoppeld en hebben eigen netwerkverbindingen.	Cybersecurity is van groot belang voor de verkeerssystemen als product, alsmede voor de inzet van de verkeerssystemen in een object.

Machineveiligheid	Slecht beveiligde besturing kan leiden tot onvoorspelbaar gedrag van machine.	Machineveiligheid stelt eisen aan de cybersecurity van systemen en netwerken.	Er is een directe relatie tussen de normen voor machineveiligheid (61508 + 61511) en cybersecurity (62443).
Veiligheid scheepvaart (zee- en binnenvaart)	Scheepvaartinformatie klopt niet, wat kan leiden tot aanvaringen en verdrinking.	Nee	Betreft de systemen die invloed hebben op de begeleiding en monitoring van het scheepvaartverkeer, niet de systemen op het schip zelf.
Spoorwegveiligheid	Treininformatie klopt niet, wat kan leiden tot aanrijdingen en verdrinking.	Spoorwegen maken gebruik van eigen netwerken voor de kritische installaties. Deze netwerken dienen aan dezelfde beveiligingseisen te voldoen. Treinverkeer en elektromagnetische straling beïnvloeden de werking van systemen.	Zie ook tunnelveiligheid. Dit betreft de systemen die invloed hebben op de begeleiding en monitoring van het treinverkeer, niet de systemen in het rijdend materieel zelf.
Veiligheid tegen overstroming	Waterkering wordt geopend door cyberaanval of de kering kan niet gesloten worden als het nodig is. Denk ook aan intelligente meetopnemers: als een sensor een verkeerde waterstand doorgeeft, zal de waterkering niet waarschuwen, en ook niet reageren.	Nee	Kritische systemen zullen uitvallen als zij bij een overstroming onder water komen te staan. Dit leidt tot verlies van gegevens (incl. back-ups) en systemen.
Externe veiligheid inrichtingen en transport	Uitstoot van emissies door installaties.	Straling leidt tot uitval van systemen.	EMC-aspecten en gevaarlijke stoffen
Hulpverlening	Niet direct kunnen schakelen vanaf een brandweerbedienpaneel doordat deze niet beschikbaar is.	Niet-toegestane bediening doordat hulpverlening ongeautoriseerde toegang heeft tot alle ruimten.	Dit gaat om de directe hulpverlening door ambulance of brandweer.

4.3 Betrouwbaarheid, integriteit en beschikbaarheid

Cybersecurity is gericht op de R (*reliability*, betrouwbaarheid en integriteit) en heeft invloed op de A (*availability*, beschikbaarheid) en de S (*safety*, veiligheid) van een object.

Het probleem met veel cyberincidenten is dat de faalkansen en de impact niet direct getalsmatig zijn in te vullen. Daardoor is dit falen moeilijk in een *failure mode effect and criticality analysis* (FMECA) te verwerken. Er zullen andere methodes gevonden moeten worden om een reële inschatting te kunnen doen. Incidentresponsplannen, back-ups en continuïteitsplannen (*disaster recovery*) moeten een grotere rol spelen.

Betrouwbaarheid
Een object kan veilig functioneren als bedienings- en besturingssystemen de functies veilig en volledig uitvoeren. Een systeem is betrouwbaar als de uitkomst van een vereiste functie voldoet aan de verwachting binnen gegeven omstandigheden en tijdsinterval. Dreigingen worden weggenomen door alleen geautoriseerde gebruikers toegang te geven tot de systemen en de gegevens.

Integriteit
Het object kan veilig functioneren als de verwerkte gegevens in bedienings- en besturingssystemen volledig en juist zijn. Informatie is integer als deze ongewijzigd op de bestemming aankomt. Maatregelen kunnen dreigingen wegnemen:

- De systemen waarin gegevens worden verwerkt, zijn juist en controleerbaar.
- De opgeslagen loggegevens kloppen. Ze kunnen niet worden gewist of gewijzigd door een onbevoegde.
- Als de gegevens toch worden veranderd, wordt dit gelogd en kan een back-up deze gegevens vervangen.

Beschikbaarheid
Operationele techniek (OT) is beschikbaar en gebruikers hebben toegang tot het systeem. Maatregelen kunnen dreigingen wegnemen:

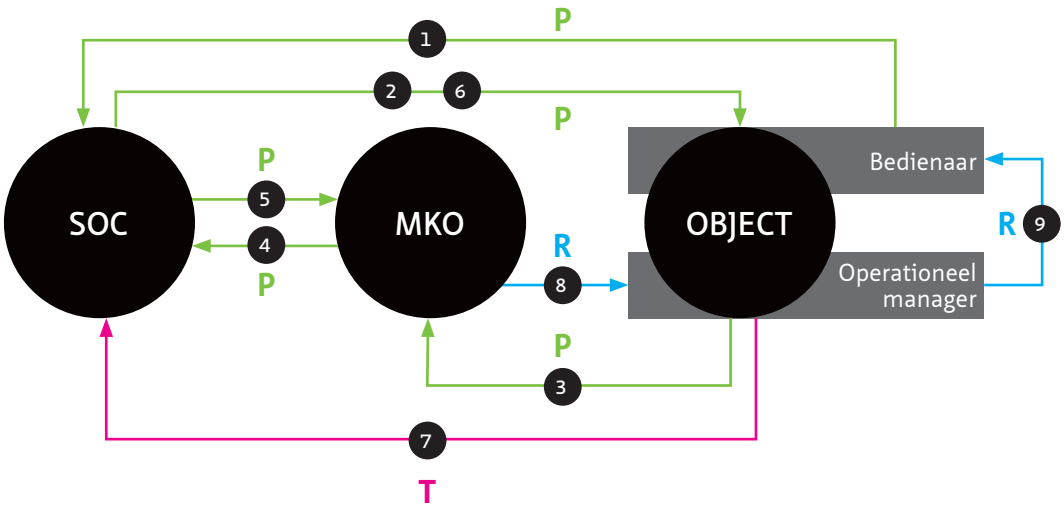
- OT kan niet buiten werking worden gesteld met een *distributed denial of service*-aanval (DDoS).
- Regelmatige back-ups zorgen ervoor dat de bedrijfscontinuïteit niet in gevaar komt bij een hack met malware, ransomware of cryptoware, waarbij informatie in systemen gewist, aangepast of versleuteld wordt.
- De beschikbaarheid van OT kan worden bedreigd door kwaadwillende software, virussen of malware. Neem maatregelen om besmetting door deze software te voorkomen.
- Een procedure voor incidentrespons met regelmatige oefening op basis van scenario's.

Aanbeveling:

Gebruikmaken van praktijkgegevens voor herstel van dienstverlening in de ICT-omgeving kan nuttig zijn, maar zijn niet een-op-een bruikbaar. Maak scenario’s samen met de verantwoordelijken voor de FMECA.

5 Voorbeeld Rijkswaterstaat

Om te laten zien hoe operationele procesbewaking van cybersecurity geïntegreerd kan worden in de bestaande procesbewaking van een tunnel, beschrijft dit hoofdstuk hoe de informatiestroom verloopt bij Rijkswaterstaat. In onderstaande afbeelding zijn de relaties bij Rijkswaterstaat weergegeven voor het melden van cyberincidenten tussen het security operation center (SOC), het controlcenter van de missiekritieke ondersteuning (MKO) en het object, in dit geval de tunnel. In de afbeelding zijn de uitvoerende maatregelen weergegeven als pijl en staat **T** voor techniek, **P** en **R** voor (regulier) proces. De nummering in de figuur correspondeert met de maatregelen aangegeven onder de figuur.



Figuur 5.1 / Workflow cybersecurity Rijkswaterstaat.

- SOC/Nationaal cybersecuritycentrum (NCSC) bewaakt het netwerk en heeft meldfunctie richting de operatie.
- Er is een technische monitoring door het SOC op de systemen en netwerken in het object (7).
- Indien er in de monitoring een (mogelijk) cyberincident wordt gevonden, zal dit worden doorgemeld naar het MKO (zijnde de tunnelbeheerder en de veiligheidsbeambte) en het object (5 en 6). Procesmatig kunnen meldingen op verschillende manieren worden gedaan:
  - Een bedienaar kan direct meldingen doen bij het SOC (1).
  - Vanuit het object kunnen procesmatig (incident)meldingen worden gegeven naar het MKO (3).
  - Het MKO zal een melding van een cyberincident doorzetten naar het SOC (4).
- Het SOC kan nieuw bekend geworden kwetsbaarheden of dreigingen bekendmaken bij het object (2).
- Het MKO zal bij een melding vanuit het SOC bepalen wat het veiligheidsrisico is, en het reguliere proces volgen door, indien noodzakelijk, de operationeel manager (8) opdracht te geven het object te sluiten. Deze zal de opdracht vervolgens doorzetten naar de bedienaar van het object (9).

Een melding vanuit het SOC zal altijd worden vergezeld van een handelingsadvies. In de respons op een cyberincident zal het SOC de noodzakelijke acties en aanbevelingen doorgeven aan het MKO en het object. SOC, MKO en object zullen, in het geval van cyberincidenten, nauw moeten samenwerken waarbij het SOC een coördinerende rol kan vervullen.

Colofon

Uitgever
Het Nederlands kenniscentrum voor ondergronds bouwen en ondergronds ruimtegebruik (COB).

Van der Burghweg 1, 2628 CS Delft • gebouw De Bouwcampus
Postbus 582, 2600 AN Delft
085 4862 410 • info@cob.nl • www.cob.nl

Auteurs
- Jack Blok (deelprojectleider), Arcadis
- Sip Schoonveld, Arcadis
- Erik Vinke, Vialis
- Jaap van Wissen, Rijkswaterstaat
- Gijs Withagen, Kienia

Eindredactie en opmaak
Marije Nieuwenhuizen, COB/Gryffin

Publicatiedatum
10 december 2020

Coverfoto's
Flickr/Kecko

Downloaden
Deze publicatie is gratis te downloaden via www.cob.nl/kennisbank.

Cybersecurity en tunnelveiligheid

Aanbevelingen voor cybersecurity als aspect in toetskader tunnelveiligheid

Dit memo beschrijft hoe inhoud kan worden gegeven aan cybersecurity in relatie tot veiligheid in het algemeen en tunnelveiligheid in het bijzonder. Hiermee kan dit aspect worden geïntegreerd in het toetskader voor tunnelveiligheid, waarmee het een integraal onderdeel wordt van het tunnelveiligheidsdossier van de veiligheidsbeambte.

Een ogenschijnlijk (en op papier) veilige tunnel kan wel degelijk onveilig zijn zonder dat de verantwoordelijke tunnelbeheerder en zijn veiligheidsbeambte zich daarvan bewust zijn. Dat komt doordat cybersecurity vooralsnog geen onderdeel is van het toetskader voor tunnelveiligheid zoals bedoeld in de tunnelwet.

In dit memo worden aanbevelingen gedaan om ook de digitale weerbaarheid van een tunnel te laten meespelen in de beoordeling van de tunnelveiligheid. Daarnaast wordt onder meer ingegaan op de invloed van cybersecurity op betrouwbaarheid, beschikbaarheid en integriteit. Het memo laat ook zien hoe operationele procesbewaking van cybersecurity kan worden geïntegreerd in de bestaande procesbewaking van de tunnel en hoe de informatiestroom zou kunnen verlopen.

COB
Nederlands kenniscentrum voor ondergronds bouwen en ondergronds ruimtegebruik