# MANAGEMENTHANDLEIDING VOOR **TRAININGSPROCEDURES IN HET OPENBAAR VERVOER**

SAFEBUS

Dit project wordt gefinancierd door het Fonds voor interne veiligheid van de Europese Unie – Politie, onder de subsidieovereenkomst nr. 101034233

# INHOUDSOPGAVE

# (1)

# INLEIDING

Vervoersbedrijven zijn verantwoordelijk voor de veiligheid en het welzijn van hun passagiers. Dit betekent niet alleen veilig en betrouwbaar vervoer, maar ook bescherming tegen criminaliteit en mogelijke terroristische aanslagen.

Dit handboek is bedoeld voor beveiligingsmanagers en biedt richtlijnen met betrekking tot beleidsmaatregelen voor het:

- **Beoordelen** in hoeverre een openbaarvervoersorganisatie mogelijk blootstaat aan terroristische activiteiten en wat de mate van beveiliging is.
- **Voorkomen** van terroristische aanslagen en de schade die veroorzaakt zou kunnen worden te beperken.
- **Detecteren** van verdachte situaties en kwaadaardige bedoelingen.
- **Reageren** op noodsituaties.

De opzet en structuur van openbaarvervoersbedrijven lopen sterk uiteen, daarom moeten beveiligingsplannen en -beleid rekening houden met iedere individuele situatie.

Dit handboek is bedoeld als een blauwdruk, met aspecten die moeten worden aangepakt en best practices die kunnen helpen bij het opstellen van bedrijfsspecifieke beveiligingsplannen en -procedures.

# (2)

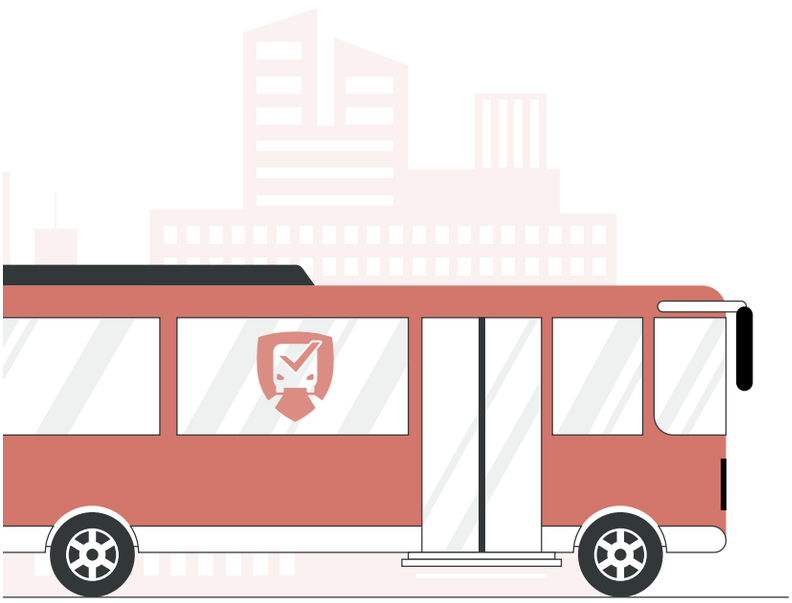
# HANDLEIDING VOOR **TERRORISMEBESTRIJDING**

## CONTEXT

Terrorisme betekent het gebruik van geweld of andere criminele acties als een gerechtvaardigd middel om politieke doelen te bereiken. Helaas zijn openbare vervoersystemen herhaaldelijk het doelwit geweest van terroristische activiteiten, met de bedoeling de werkzaamheden te verstoren en mobiliteitsdiensten te saboteren.

Onze voertuigen en infrastructuur zouden een mogelijk doelwit voor terroristische activiteiten kunnen zijn. Het doel zou ook kunnen zijn om mensen die gebruik maken van het openbaar vervoer schade te berokkenen.

Als vervoersbedrijven zijn wij verantwoordelijk voor de veiligheid en het welzijn van onze passagiers en medewerkers. Dit omvat redelijke maatregelen om incidenten te voorkomen, maar ook dat we voorbereid zijn om te reageren op incidenten en de schade zoveel mogelijk te beperken.



## BEDREIGINGEN EN DOELWITTEN

### RELEVANTE BEDRIJFSMIDDELEN

Busdiensten hebben verschillende bedrijfsmiddelen nodig om hun klanten transportdiensten te kunnen aanbieden. Enkele daarvan zijn openbaar toegankelijk, andere beschermd en hebben alleen beperkte toegang. Relevante bedrijfsmiddelen zijn onder meer:

- **Passagiersgerelateerde bedrijfsmiddelen**, waaronder stations en overstappunten, haltes, verkoop- en informatiecentra, eventueel bagageopslag. Deze faciliteiten zijn open voor het publiek en hebben slechts beperkte mogelijkheden qua toegangscontrole.
- **Bedrijfsgerelateerde bedrijfsmiddelen**, waaronder voertuigen, depots en werkplaatsen, evenals faciliteiten voor brandstofbevoorrading. De toegankelijkheid tot deze faciliteiten varieert.
- **Ondersteunende bedrijfsmiddelen** bestaan uit controlekamers, personeels- en servicefaciliteiten en administratieve gebouwen. Deze zijn vergelijkbaar met de bedrijfsmiddelen van elk ander bedrijf en zijn niet toegankelijk voor het publiek.
- **Digitale bedrijfsmiddelen** worden steeds belangrijker voor busdiensten. Dit kunnen operationele controlesystemen, passagiersinformatie- en controlesystemen zijn, maar ook bedrijfsbeheersystemen voor kaartverkoop, betaling en boeking. Fysieke toegang tot deze bedrijfsmiddelen is normaal gesproken geïntegreerd in bedrijfsgerelateerde of ondersteunende bedrijfsmiddelen, die niet toegankelijk zijn voor het publiek.

### INCIDENTSCENARIO 'S

Op basis van recente gebeurtenissen en incidenten die zich met name in de openbaar vervoersector hebben voorgedaan, kan de volgende (niet-uitputtende) lijst met scenario's in overweging worden genomen.

- **Geïmproviseerd explosief (IED)** - een geïmproviseerd explosief dat in gewone bagage kan worden verborgen of uit het zicht kan worden opgeborgen, mogelijk onder stoelen of in vuilnisbakken. IED's kunnen met een timer of op afstand worden geactiveerd, de aanvaller hoeft niet in de buurt te zijn.
- **Zelfmoordaanslag** – een aanvaller draagt het explosief rechtstreeks naar het bussysteem en laat het direct ontploffen.
- **Vuurwapens** – een aanvaller die gericht of willekeurig schiet, van op afstand of van dichtbij.
- **Steken** – een aanval waarbij een mes of lemmet wordt gebruikt om mensen van dichtbij aan te vallen.
- **Sabotage** – vandalisme, diefstal of manipulatie van apparatuur met als doel de operationele capaciteit en veiligheid in gevaar te brengen.
- **Brandstichting** – het opzettelijk in brand steken om bedrijfsmiddelen te vernietigen.
- **Auto-aanval** – waarbij een extern voertuig wordt gebruikt om tegen passagiers of installaties van de busvervoerder te botsen.
- **Bus-aanval** – een bus gebruiken om op mensen in te rijden.
- **Gijzeling / kaping** – een aanval waarbij mensen met directe bedreiging voor hun leven worden vastgehouden in stations of aan boord van voertuigen.
- **Bombedreiging** – een dreiging om een explosief tot ontploffing te brengen binnen het bussysteem, ongeacht of een dergelijk explosief ook daadwerkelijk bestaat.
- **Cyberaanval** – een aanval gericht op computersystemen, netwerken of apparaten.
- **CBRN-aanval** – een aanval waarbij gebruik wordt gemaakt van chemische, biologische, radiologische of nucleaire stoffen.

## BEVEILIGINGSBELEID EN VEILIGHEIDSMAATREGELENA

### ONDERDELEN VAN HET BEVEILIGINGSCONCEPT

Er zijn een aantal hulpmiddelen en beveiligingsmaatregelen om het openbaar vervoer te beschermen. Een goed beveiligingsconcept maakt gebruik van al deze middelen om een efficiënte mix te ontwikkelen.

**Infrastructuurmaatregelen** leggen de basis om elke aanval af te schrikken en mogelijke schade te beperken. Deze omvatten

- De constructie en het materiaal dat gebruikt wordt om bedrijfsmiddelen te bouwen;
- De lay-out, het ontwerp en de ruimtelijke organisatie van elk ruimte, evenals;
- Het plaatsen van uitkijkposten en toegangscontrole poortjes.

**Technologische** tools helpen om uitgestrekte gebieden te beveiligen, het toezicht te centraliseren en personeel efficiënt in te zetten. Deze omvatten:

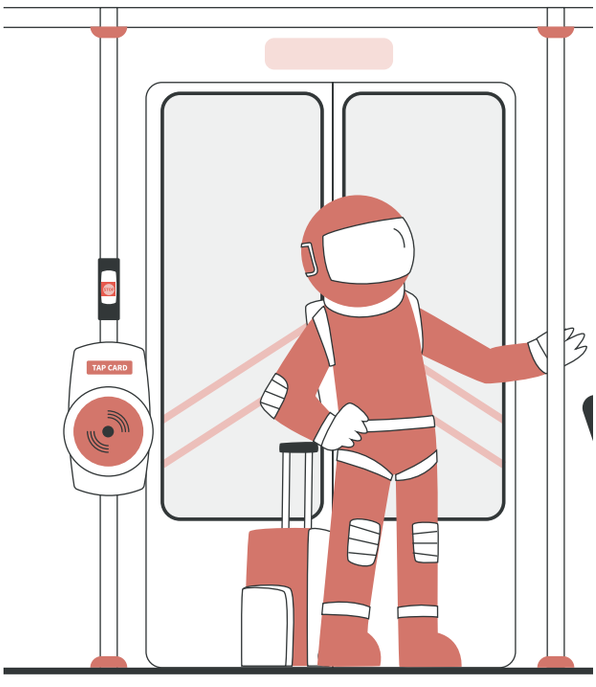
- CCTV-bewaking, video-analyse en forensisch onderzoek,
- Noodpalen en help-knoppen;
- Beveiligingstechnologie, zoals vergrendeling en sleutels of sensoren om mogelijk verdachte situaties te detecteren;
- Communicatietechnologie om de verificatie van incidenten en de reactie daarop te coördineren.

**Personeel** is een belangrijke factor in beveiligingsconcepten en omvat dus toegewijd beveiligingspersoneel, maar ook operationeel en klantenservice personeel. Relevante aspecten zijn:

- Functies en verantwoordelijkheden;
- Planning en procedures;
- Training en opleiding.

**Organisatorische** maatregelen vormen het kader voor het hele beveiligingsconcept en omvatten:

- Bewaking;
- De beveiliging, noodmanagement en crisisorganisatie,
- Het toewijzen van functies en verantwoordelijkheden, en de samenwerking tussen beveiliging en operaties begeleiden;
- Samenwerking met overheidsinstanties, hulpverleners en zakelijke partners.



# PRINCIPES VOOR BEVEILIGINGSBEHEER

***PREVENTIE*** in het openbaar vervoer is van cruciaal belang. Preventiemaatregelen zijn bedoeld om potentiële bedreigingen te identificeren en te beperken voordat ze schade kunnen veroorzaken en om potentiële daders ervan te weerhouden om te proberen openbaar vervoer systemen aan te vallen en te verstoren.

In principe zijn er twee strategieën beschikbaar om deze bedrijfsmiddelen te beschermen: **toegangscontrole** om een afschrikmiddel te creëren en te controleren wie een faciliteit betreedt, en het **versterken van de infrastructuur** om de schade die een potentiële aanval zou kunnen veroorzaken te beperken.

***DETECTIEMAATREGELEN*** zijn een belangrijke aanvulling op preventiemaatregelen. Ze zijn bedoeld om **potentiële veiligheidsbedreigingen te identificeren** en **een snelle en gerichte** reactie mogelijk te maken.

Personeel speelt een belangrijke rol in het opsporen van potentiële bedreigingen, maar door de uitbreiding van bedrijfsmiddelen en netwerken in het openbaar vervoer, biedt technologie een belangrijke ondersteuning om het hele grondgebied te bewaken.

***VOORBEREIDING*** erkent dat preventie kan mislukken en omvat noodplannen waarin functies en verantwoordelijkheden, communicatieprotocollen en responsprocedures worden beschreven, evenals bedrijfscontinuïteitsplanning.

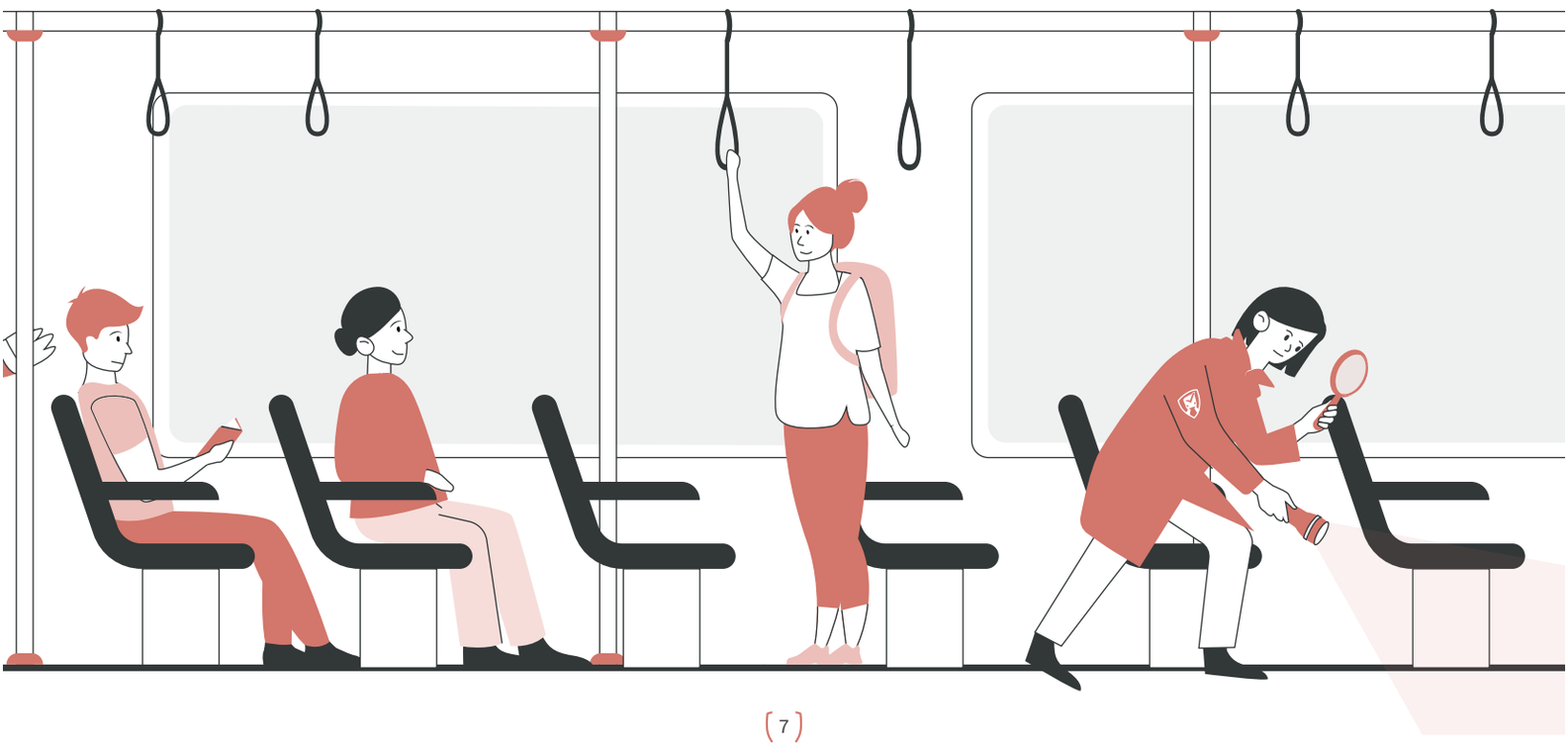
Het personeel heeft regelmatige **training en oefeningen** nodig om vertrouwd te raken met hun rollen en verantwoordelijkheden zodat ze efficiënt op noodsituaties kunnen reageren. **Bedrijfscontinuïteitsplanning** moet de operationele impact van elk incident beperken en noodplannen voorzien.

***INCIDENT RESPONSE*** omvat de mobilisatie van middelen en personeel om te reageren op een noodsituatie. Terroristische aanslagen zullen een noodsituatie waarschijnlijk escaleren tot een crisissituatie.

Behalve het activeren van interne noodcommunicatieprotocollen en het inzetten van interne responsteams, moet er bij crisisbeheersing ook een crisiscel worden geactiveerd en met externe hulpverleners worden gecoördineerd.

Na elke noodsituatie is het belangrijk om een beoordeling uit te voeren om na te gaan hoe de respons op de noodsituatie kan worden verbeterd en wat de mogelijkheden zijn voor betere preventie.

***Als vervoersbedrijven zijn wij verantwoordelijk voor de veiligheid en het welzijn van onze passagiers en werknemers.***



# (3)

# RISICOBEOORDELING EN MONITORING

## DREIGINGSANALYSE

De basis voor elk beveiligingsconcept en -plan is een grondige beoordeling van bedreigingen en risico's waaraan de eigen organisatie kan worden blootgesteld. Hoewel het openbaar vervoer wordt beschouwd als een doelwit voor terroristische activiteiten, varieert het dreigingsniveau afhankelijk van verschillende factoren, zoals de algemene politieke situatie in uw land/regio, de omvang en het economisch belang van uw stad of recente aanslagen die op andere plaatsen werden gepleegd.

Het dreigingsbeeld moet regelmatig worden gevalideerd, aangezien de doelwitprioriteiten en modus operandi van potentiële daders voortdurend veranderen. Ook geplande evenementen op hoog niveau, zoals grote sportevenementen of politieke bijeenkomsten, kunnen het dreigingsniveau tijdelijk verhogen.

De dreigingsniveaus moeten worden beoordeeld in samenwerking met de verantwoordelijke instanties, die een beter inzicht hebben in de huidige wereldwijde en lokale situatie.

## RISICOBEOORDELING

Risico- en kwetsbaarheidsbeoordelingen helpen busbedrijven mogelijke zwakke punten te identificeren en investeringen om hun faciliteiten te upgraden prioriteit te geven. Deze beoordelingen moeten regelmatig worden herhaald om structurele veranderingen of bouwactiviteiten weer te geven, maar ook om afgestemd te zijn op de opkomst van nieuwe bedreigingen en ontwikkelingen op het gebied van modus operandi. Het is belangrijk om risico- en kwetsbaarheidsbeoordelingen niet te beperken tot kritieke bedrijfsmiddelen, maar ook rekening te houden met de openbare ruimten die noodzakelijk zijn om de busdiensten operationeel te houden.

- Het COUNTERACT-project, gecoördineerd door UITP, heeft een **methodologie ontwikkeld voor risico- en kwetsbaarheidsbeoordeling** die specifiek is afgestemd op de sector openbaar vervoer. Deze methodologie wordt voortdurend aangepast aan de veranderende dreigingssituatie en wordt door UITP aanbevolen voor gebruik door openbaarvervoersbedrijven.

## RISICOMONITORING

Een omgeving met veiligheidsrisico's verandert voortdurend, ook voor het busvervoer. Er kunnen nieuwe dreigingsscenario's ontstaan, de renovatie van bedrijfsmiddelen kan leiden tot nieuwe potentiële kwetsbaarheden, gebeurtenissen of nieuwe bouwprojecten in het werkgebied kunnen leiden tot nieuwe mogelijke doelwitten. Het is daarom belangrijk om risico's voortdurend te monitoren om ervoor te zorgen dat risicomanagement strategieën effectief zijn en afgestemd op de veranderende risico-omgeving.

- Op **bedrijfsniveau** kan een nauwe samenwerking met de relevante instanties helpen om in een zo vroeg mogelijk stadium op de hoogte te zijn van wijzigingen in de dreigingsanalyse en mogelijke gevolgen daarvan voor de busdienstverlening.
- Op **operationeel niveau** moeten risico- en kwetsbaarheidsbeoordelingen regelmatig worden herhaald om veranderingen in de infrastructuur, de aankoop van nieuwe voertuigen en technologische ontwikkelingen weer te geven en om stresstests uit te voeren in overeenstemming met de ontwikkeling van incidentscenario's zoals die door de autoriteiten worden meegedeeld of zoals die op andere plaatsen in het openbaar vervoer worden waargenomen.
- Op **siteniveau** helpen regelmatige beveiligingsaudits om vast te stellen of bestaande beveiligingsmaatregelen nog steeds functioneren en geschikt zijn om bedrijfsmiddelen te beschermen.

# (4)

# BEVEILIGING VAN GEBOUWEN

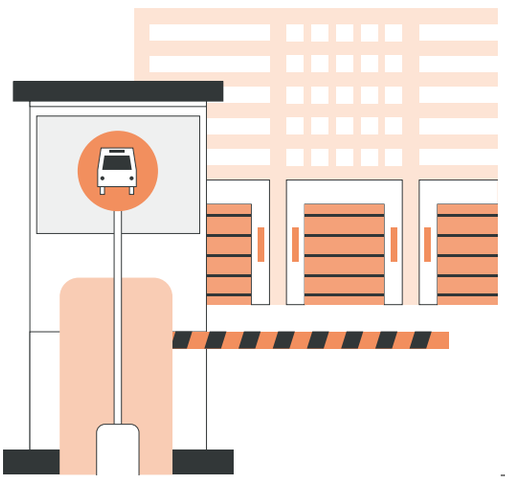
## OPENBARE FACILITEITEN

Faciliteiten voor passagiers zijn openbaar toegankelijk en moeten grote aantallen mensen efficiënt kunnen verwerken. De mogelijkheden voor maatregelen voor toegangscontrole zijn beperkt. Belangrijke beschermingsprincipes voor busstations en -haltes zijn onder andere controle om mogelijk verdachte situaties te identificeren en het versterken van de infrastructuur om de gevolgen van een mogelijke aanval af te schrikken en te beperken.

### ONTWERP EN INFRASTRUCTUUR

Normen en richtlijnen voor de lay-out en het materiaal van stations zijn de afgelopen jaren sterk geëvolueerd en worden gevolgd voor nieuwe constructies of het upgraden van bestaande faciliteiten en apparatuur. Openbare vervoersystemen zijn over het algemeen echter niet nieuw en maken gebruik van een oude infrastructuur die rechtstreeks in de openbare ruimte is ingebed. De belangrijkste maatregelen die in busstations moeten worden overwogen, zijn onder meer:

- **Een duidelijk zicht** op alle passagiers faciliteiten helpt de omgeving te bewaken, voorkomt het creëren van schuilplaatsen en maakt een snelle evacuatie mogelijk als dat nodig is. Meubilair, verkoopautomaten en informatieschermen en -borden moeten gemaakt zijn van vandalismebestendig materiaal en mogen het zicht niet belemmeren.
- **Voldoende verlichting** is noodzakelijk zodat passagiers zich goed kunnen oriënteren en een goed overzicht hebben. Het ondersteunt ook het toezicht en het bewaken van busstations door CCTV-camera's.
- **De lay-out van het station** moet achtergelaten bagage en andere opslagruimtes afscheiden van gangen, perrons en passagiersroutes om de gevolgen van een mogelijke explosie tot een minimum te beperken.
- **Sloten en verzegelingen** kunnen de toegang verhinderen tot kastjes, apparatuurkasten of toegang tot technische installaties, die mogelijk als schuilplaats kunnen worden gebruikt. Als er geen sloten kunnen worden geïnstalleerd, moeten er verzegelingen worden aangebracht.
- Vuilnisbakken moeten worden beschouwd als een plaats waar gevaarlijke voorwerpen en stoffen gemakkelijk kunnen worden verborgen. **Doorzichtige plastic zakken**, opgehangen aan metalen hoepelzakhouders die maximale transparantie bieden, worden als best practice beschouwd. Indien mogelijk moeten vuilnisbakken op plaatsen worden neergezet waar camera's aanwezig zijn om deze te bewaken. Vuilnisbakken moeten regelmatig geleegd worden om de transparantie van de zakken optimaal te benutten.
- Wachtruimtes en bushaltes moeten worden beschermd tegen aanvallen door voertuigen zonder de obstakelvrije toegang voor passagiers in gevaar te brengen. Bescherming kan worden bereikt door **fysieke barrières**, zoals paaltjes of plantenbakken en verhoogde stoepranden.
- Doorzichtige constructies, zoals bushokjes, moeten **veiligheidsglas** hebben om rondvliegend of vallend glas te voorkomen in geval van een explosie. Gelaagd glas of anti-splinter folie om bestaande structuren achteraf aan te passen, kan ook helpen om vandalisme en graffiti te voorkomen.



***Om busstations en - haltes te kunnen beschermen is het belangrijk potentieel verdachte situaties te herkennen.***

## TECHNOLOGIE

Technologische hulpmiddelen kunnen de beveiliging van bussystemen aanzienlijk verbeteren, waarbij gesloten televisiecircuits (CCTV) de meest gebruikte en belangrijkste zijn in het openbaar vervoer.

- **CCTV-camera's** kunnen voornamelijk de bewaking van stations ondersteunen, die vaak te wijdverspreid zijn om efficiënt door personeel te worden bewaakt. Camera's zouden continu een overzicht moeten geven van de situatie in een station. Er moet speciale aandacht worden besteed aan gevoelige locaties, zoals noodhulppunten, apparatuurkasten of toegangspunten tot technische installaties. Om te voorkomen dat er geknoeid wordt of bewijsmateriaal verloren gaat doordat camera's tijdens incidenten vernietigd worden, moeten ze zo geplaatst worden dat ze elkaar dekken.
- **Real-time monitoring** van camerabeelden in de controlekamer maakt het mogelijk om CCTV te gebruiken voor alarmverificatie en incidentmanagement, wat een efficient gebruik van het personeel ondersteunt.
- **CCTV-opnames en audiobeelden** zijn essentieel bewijsmateriaal bij het onderzoeken van eender welke situatie. Opnames worden gedurende een wettelijk bindende periode bewaard voordat ze worden overschreven. Ze moeten van voldoende kwaliteit zijn om toelaatbaar te zijn in juridische procedures.
- **Videoanalyse** in CCTV-camera's kan helpen bij het identificeren van verdachte situaties. Het open karakter van stations en de vaak hoge dichtheid van mensen zorgen voor uitdagende omstandigheden, maar de technologie is nog volop in ontwikkeling. De meest voorkomende algoritmen die voor openbare faciliteiten worden getest, zijn het detecteren van achtergelaten voorwerpen, agressief gedrag of ongebruikelijke passagiersbewegingen.

Sensoren en alarmen kunnen helpen bij het detecteren van mogelijk verdachte situaties. De meest voorkomende installaties zijn inbraakalarmen die deuren en sloten beschermen. Sensoren kunnen rook of chemische stoffen detecteren.

Technologie kan ook passagiers en personeel ondersteunen die hulp nodig hebben.

- **SOS-intercoms** die op grote stations en overstappunten zijn geïnstalleerd, stellen passagiers en personeel in staat om hulp in te roepen. Deze intercoms zijn vaak uitgerust met camera's om misbruik te voorkomen.
- **Bodycamera's** kunnen worden gebruikt om personeel te beschermen. Ze fungeren als een afschrikmiddel tegen agressie, de live beelden helpen het controlekamerpersoneel om situaties te begrijpen en de opnames leveren bewijsmateriaal bij het onderzoek naar incidenten.

## PERSONEEL EN PROCEDURES

Het personeel vervult meerdere veiligheidsfuncties in stations. Hun aanwezigheid werkt als een afschrikmiddel tegen potentiële overtreders, het stelt passagiers gerust en het helpt om een gecontroleerde ruimte te creëren. Attente medewerkers kunnen op efficiënte wijze voldoen aan de doelstellingen op het gebied van passagiersservice en beveiliging.

De proactieve beveiligingsrol van personeel in stations omvat:

- Waakzaamheid in openbare ruimtes om mogelijk verdachte situaties te herkennen. Hieronder vallen ongewoon en ongepast gedrag en onbeheerde voorwerpen. Het personeel moet vertrouwd zijn met de begrippen verdacht gedrag en verdachte voorwerpen. Elke bezorgdheid moet worden gemeld om opheldering of follow-up door beveiligingspersoneel of de politie mogelijk te maken. Om vals alarm te voorkomen, moet er een training worden gegeven over hoe u uw eigen vooroordelen kunt herkennen bij het inschatten van potentiële bedreigingen.
- Regelmatige veiligheidscontroles in het station helpen om de zichtbaarheid van het personeel te vergroten. Patrouilles kunnen door personeelsleden gezamenlijk worden uitgevoerd zodat ze waakzaamheid kunnen combineren met klantenbetrokkenheid en een regelmatige controle van de integriteit van de fysieke beveiligingsmaatregelen. Veiligheidspatrouilles moeten een duidelijk afgebakend gebied hebben dat ze moeten bewaken met gedefinieerde aanraakpunten en instructies (bijv. fysiek controleren of een deur op slot is). Veiligheidspatrouilles moeten tevens onvoorspelbaar zijn.

# FACILITEITEN MET BEPERKTE TOEGANG

Toegangscontrole tot faciliteiten en apparatuur met beperkte toegang is cruciaal om ervoor te zorgen dat alleen bevoegd personeel en geautoriseerd materiaal via gecontroleerde toegangswegen een locatie kunnen betreden. Binnen de gebouwen helpt algemene waakzaamheid ervoor te zorgen dat ongebruikelijke aanwezigheid, gedrag en items worden gemeld.

## ONTWERP EN INFRASTRUCTUUR

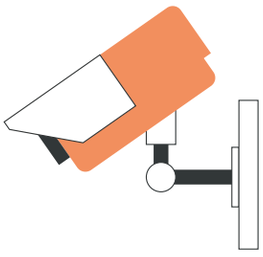
- Fysieke toegangsbarrières zoals muren en hekken moeten de **omtrek van depots, werkplaatsen of andere faciliteiten met beperkte toegang beschermen**. Deze barrières moeten goed worden onderhouden en kunnen worden aangevuld met inbraaksensoren voor extra bescherming.
- Alle deuren tussen openbare ruimtes en beperkte ruimtes moeten op slot zitten of gecontroleerd worden. Bedrijfsmiddelen met beperkte toegang, zoals depots, moeten worden uitgerust met **poorten met gecontroleerde toegang**, zodat alleen bevoegde personen naar binnen kunnen.

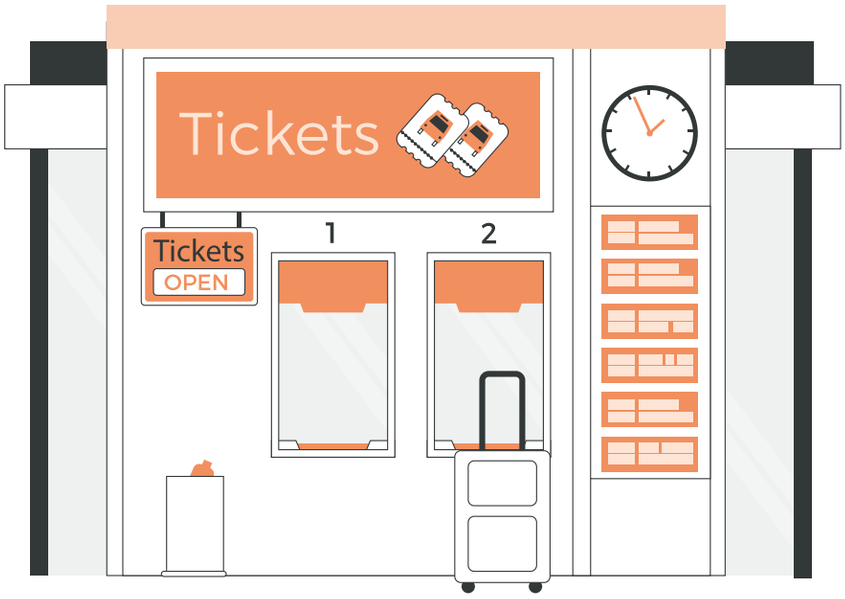
## TECHNOLOGIE

- **CCTV-camera's uitgerust met nachtzicht** kunnen inbraakdetectie ondersteunen door de binnen- en buitenomtrek te bewaken om onbevoegde toegang te voorkomen.
- **Geofencing** kan een virtuele perimeter creëren als extra bescherming of wanneer er geen fysieke barrières kunnen worden opgericht. Dit kan helpen bij het bewaken van de omgeving van de faciliteit of het instellen van een zwaarbeveiligde zone binnen een faciliteit, zoals het parkeerterrein voor rollend materieel.
- **Videoanalyse** biedt extra bescherming op momenten dat faciliteiten met beperkte toegang gesloten zijn en er geen operationele activiteiten plaatsvinden.

## PERSONALE E PROCEDURE

- Een **incheckprocedure** moet ervoor zorgen dat onbevoegd personeel en bezoekers worden gecontroleerd en geregistreerd. Als privé auto's toch op het terrein geparkeerd mogen worden, moeten ze worden gecontroleerd (inclusief bagage) en moeten ze een parkeervergunning hebben.
- **Badges en verstrekte vergunningen** moeten duidelijk zichtbaar zijn om elke persoon of auto als geaccrediteerd te kunnen herkennen. Deze moeten zichtbaar gedragen worden wanneer mensen zich in faciliteiten met beperkte toegang bevinden. Duidelijke in- en uitlogprocedures vergemakkelijken ook een evacuatie indien nodig.
- **Bussen en touringcars moeten bij het binnenkomen en verlaten van faciliteiten met beperkte toegang worden gecontroleerd** om er zeker van te zijn dat er geen onbeheerde voorwerpen of onbevoegde personen aan boord zijn. Deze controles kunnen door de bestuurders worden uitgevoerd en moeten geregistreerd worden.
- **Waakzaamheid van het personeel** en patrouilles in faciliteiten zijn, net als in openbare faciliteiten, van essentieel belang om mogelijk verdachte situaties te herkennen. Mensen die u niet kent, moet u vragen om hun reden te bevestigen en in te checken. Het personeel moet vertrouwd zijn met de begrippen verdacht gedrag en verdachte voorwerpen. Elke bezorgdheid moet worden gemeld om opheldering of follow-up door beveiligingspersoneel of de politie mogelijk te maken.





# (5)

# VOERTUIGBEVEILIGING

Bij het beveiligen van voertuigen moet rekening worden gehouden met sabotage en diefstal en het binnenbrengen van gevaarlijke voorwerpen en stoffen.

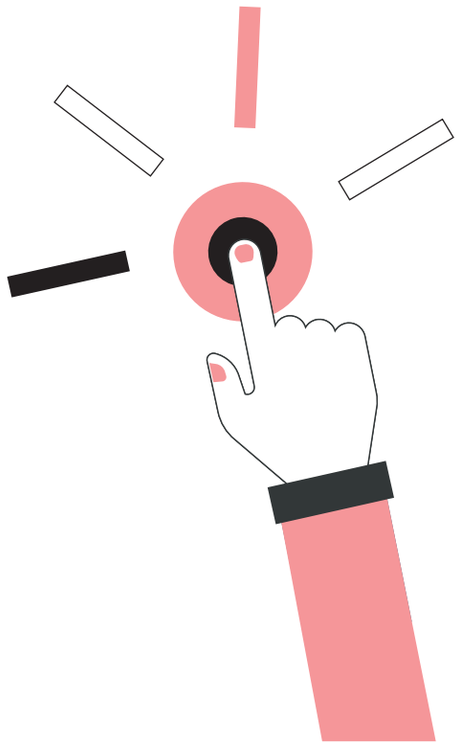
## TECHNOLOGIE

- **Slimme contactsloten voor bussen** kunnen een extra beveiligingslaag bieden met individuele sleutels om ervoor te zorgen dat alleen de geplande en toegewezen chauffeur de bus kan openen en starten.
- Bussen zijn vaak uitgerust met **alarmknoppen voor chauffeurs**, zodat ze rechtstreeks contact kunnen opnemen met de controlekamer of dispatcher. Deze alarmen zijn meestal stil en stellen de controlekamer of de dispatcher in staat om naar de situatie te luisteren en hun situatiebewustzijn te verbeteren.
- **Geautomatiseerde voertuigbewakingssystemen (AVM)** worden steeds vaker gebruikt om busvloten te beheren en te coördineren. Het continu op de hoogte zijn van busposities kan helpen bij het detecteren van afwijkingen en verdachte bewegingen.
- **Geofencing** kan worden gebruikt om de positie en de beweging van bussen te controleren. Het kan worden gebruikt om te voorkomen dat bussen zonder toestemming uit niet-afgesloten depots of parkeerplaatsen worden gehaald en het kan waarschuwen als bussen van hun toegewezen route en dienstpatroon afwijken.

## PERSONEEL EN PROCEDURES

- Toegang tot bussen en bussleutels kan worden gecontroleerd door een **overdrachtsprocedure**, waarbij de sleutels alleen aan de geplande en aangewezen chauffeurs worden overhandigd.
- Een bepaalde vorm van toegangscontrole kan worden uitgevoerd door passagiersstromen te begeleiden. Veel bedrijven hadden al het principe ingevoerd dat passagiers **alleen aan de voorkant van de bus mogen instappen**; passagiers moeten de chauffeur passeren en een kaartje kopen of laten zien. Tijdens de recente pandemie werd deze maatregel echter op veel plaatsen om gezondheids- en veiligheidsredenen ingetrokken.
- Een **instapprocedure** voor busvervoer kan ervoor zorgen dat alleen passagiers met een geldig en gepersonaliseerd ticket op de bus kunnen stappen.
- Voordat er ook maar iets in de bagageruimte van een bus wordt geladen, moet er een **passagier-bagage controle** uitgevoerd worden [controle of de bagage bij de passagier hoort].

***In de beveiliging van voertuigen is het belangrijk rekening te houden met sabotage en diefstal en het binnen brengen van gevaarlijke voorwerpen en stoffen.***



# (6)

# ORGANISATORISCHE BEVEILIGING

## BEVEILIGINGSCULTUUR

Om een sterke beveiligingscultuur in een organisatie op te bouwen, zijn inzet van het management, bewustzijn van de werknemers en voortdurende training nodig. Beveiliging is niet alleen de verantwoordelijkheid van de beveiligingsafdeling, het is een bedrijfsverantwoordelijkheid en elke medewerker speelt een rol.

Een beveiligingsbeleid en -concept kan alleen effectief zijn als de verwachtingen voor alle medewerkers duidelijk zijn, de relevante vaardigheden worden uitgelegd en het senior management het goede voorbeeld geeft.

Een positieve beveiligingscultuur creëert een open, vertrouwde sfeer en moedigt medewerkers aan om proactief te zijn in het beperken van risico's, zodat iedereen er baat bij heeft.

## BEWUSTZIJN

Het is van groot belang dat we erkennen dat beveiliging niet alleen de taak is van beveiligingsmanagers en -medewerkers, maar dat elke medewerker in elke functie hierin een rol speelt.

- Bewustmakingsprogramma's helpen om medewerkers te herinneren aan de algemene regels, verdachte situaties te herkennen en de procedures die gevolgd moeten worden.
- Doelgerichte campagnes kunnen ertoe bijdragen om het algemene beveiligingsbewustzijn op peil te houden en om de vertrouwde regels en procedures weer wat op te frissen.
- Hand-outs en handleidingen die worden uitgedeeld aan het personeel of posters die zichtbaar zijn op de werkplek kunnen belangrijke referenties zijn om belangrijke contacten of procedures binnen handbereik te houden.

## PERSONEELSBEVEILIGING

Personeelsbeveiliging pakt het risico aan dat werknemers hun legitieme toegang tot bedrijfsmiddelen misbruiken voor ongeoorloofde doeleinden.

Zoals in elke organisatie kunnen ook busvervoerders bedreigd worden door een insider.

Dit kan worden tegengegaan door het personeel zorgvuldig te selecteren, duidelijke werkprocedures te definiëren en de discipline bij te brengen om die procedures te volgen en het personeel aan te moedigen om alert te zijn op verdacht gedrag.

- Een kritikaliteitsanalyse van personeelsfuncties helpt om de benodigde toegangsrechten (bijv. controlekamer) en gebruiksrechten (bijv. voertuigen) voor bedrijfsmiddelen te bepalen en een duidelijker framework voor achtergrondcontroles te ontwikkelen.
- Achtergrondonderzoek en doorlichting als onderdeel van het wervingsproces is de eerste stap om te voorkomen dat mensen met kwade bedoelingen bij het bedrijf komen werken. Duidelijke criteria voor sollicitanten, achtergrondonderzoek en eventueel doorlichting helpen bij het screenen op het moment van indiensttreding, maar daarbij moet worden opgemerkt dat zo'n screening slechts een momentopname uit het verleden is.
- Een duidelijk en geprotocolleerd aanmeldingsgegevensbeheer, inclusief een exit-procedure, helpt om sleutels, wachtwoorden, toegangscodes, enz. te beheren en zorgt er ook voor dat de toegang tot bedrijfsmiddelen, systemen en informatie wordt geannuleerd wanneer personeelsleden van functie veranderen of het bedrijf verlaten.
- Insider Threat Awareness training [Training voor het bewustzijn van interne bedreigingen] kan helpen om personeel vertrouwd te maken met potentiële schade die kan worden veroorzaakt door kwade opzet, niet-naleving of misbruik van persoonlijke kwetsbaarheden, tijdens het dienstverband kunnen bewustmakingscampagnes helpen om het personeel te herinneren aan de mogelijke schade die kan worden toegebracht aan passagiers, personeel en bedrijven door insiders.

## INFORMATIE- EN CYBERBEVEILIGING

Digitalisatie heeft een revolutie teweeggebracht in de manier waarop we diensten verlenen en gebruiken. Ook in het busvervoer heeft het innovatieve tools opgeleverd die processen zoals planning of onderhoud efficiënter maken. Het helpt ook bij het creëren van nieuwe klantkanalen en diensten. Daarom moet er in beveiligingsplannen en -concepten niet alleen rekening worden gehouden met fysieke bedrijfsmiddelen, maar ook met digitale bedrijfsmiddelen en processen.

Informatiebeveiliging is gericht op het beschermen van gevoelige gegevens en informatie tegen onbevoegde toegang. Dit omvat, maar is niet beperkt tot, persoonlijke en financiële informatie over personeel of klanten, bedrijfsinformatie of informatie over bedrijfsprocessen, zoals personeelsroosters of onderhoudsschema's. Inbreuken op informatiebeveiliging kunnen leiden tot economische en reputatieschade.

- Gevoelige informatie moet achter slot en grendel worden bewaard en idealiter alleen worden opgeslagen en verwerkt in faciliteiten met beperkte toegang.
- Toegangsrechten mogen alleen worden verleend aan relevante personeelsleden. Inloggegevens en wachtwoorden moeten regelmatig worden vernieuwd.

Cybersecurity is gericht op de integriteit van IT- en computerondersteunde systemen. Een cyberaanval kan de dagelijkse operationele activiteiten verstoren en kan veiligheidssystemen in gevaar brengen, waardoor het leven van het personeel en de passagiers in gevaar kan komen. Het is belangrijk om op te merken dat cyberveiligheid ook een bedrijfsuitdaging is die deel moet uitmaken van de beveiligingscultuur van een onderneming. Dit moet niet alleen aan de IT-afdeling worden overgelaten.

- Waar mogelijk moeten ook digitale middelen fysiek worden beschermd tegen onbevoegde toegang met sloten, zegels, afdekkingen en door ze te installeren in faciliteiten met beperkte toegang.
- Fysieke toegang mag alleen worden verleend aan relevante personeelsleden.
- Wachtwoordniveaus en hernieuwingsvereisten moeten in samenwerking met de IT-afdeling worden gedefinieerd.
- De integriteit van het systeem moet worden gewaarborgd door een correcte instelling, continu beheer en het patchen van softwaresystemen in overeenstemming met de aanbevelingen van de leverancier. Systeemonderhoud en reserveonderdeelbeheer moeten de systeemintegriteit waarborgen.
- Systemen moeten voortdurend worden gecontroleerd op afwijkingen. Een bijzondere uitdaging in de context van cyberbeveiliging is dat systemen gecompromitteerd kunnen zijn zonder dat dit wordt ontdekt.

Nu er nieuwe technologieën worden geïmplementeerd in het busvervoer, zoals e-bussen of oplaadstations, moet er ook rekening worden gehouden met nieuwe risico's op het gebied van cyberbeveiliging. Systemen die als gemonteerde units worden geleverd, kunnen componenten bevatten die door de leverancier zijn verzegeld. Het beoordelen van de mogelijke risico's van slecht functionerende of gecompromitteerde systeemelementen is een uitdaging die in toekomstige risicobeoordelingen moet worden aangepakt.

## BEVEILIGING DOOR DERDEN

Security risk management [Beheer van Beveiligingsrisico's] kan niet beperkt blijven tot de binnenkant van een organisatie. Zakelijke partners kunnen bedrijfsmiddelen delen, leveranciers en dienstverleners kunnen tijdelijk of permanent toegang hebben tot bedrijfsfaciliteiten en -systemen, onderaannemers kunnen toezicht houden op bedrijfsprocessen (bijv. onderhoud of administratieve taken).

Het is van cruciaal belang om het beveiligingsbeleid voor derde partijen een onderdeel te maken van het selectieproces en om duidelijke overeenkomsten, regels en een controlebeleid op te stellen.

# (7)

# BEVEILIGINGSTRAINING

Alle personeelsleden zijn verantwoordelijk voor de beveiliging van het busvervoer. Trainingsprogramma's moeten voor het personeel de rol en de verantwoordelijkheid voor elke functie verduidelijken en werknemers de expertise bieden die ze nodig hebben voor hun werk.

De initiële operationele beveiligingstraining cursussen moeten de algemene vaardigheden en kennis bieden die voor elke functie worden verwacht. Met regelmatig terugkerende operationele beveiligingstraining programma's kan de specifieke kennis worden opgefrist.

## TRAININGSBEHOEFTEN

Medewerkers moeten operationele beveiligingstrainingen krijgen om ervoor te zorgen dat ze zich bewust zijn van hun beveiligingsverantwoordelijkheid en hoe ze op de juiste manier op een aanval kunnen reageren.

- De verantwoordelijkheid van **operationeel en eerstelijnspersoneel** omvat doorgaans alert zijn op verdachte situaties en deze melden, omgaan met conflicten en deze de-escaleren en reageren op een incident wanneer dat nodig is.
- **Werknemers op locaties met beperkte toegang**, zoals controlekamers of depots, moeten op de hoogte zijn van het toegangsbeleid van de locatie waar ze werken en, indien van toepassing, bezoekers kunnen registreren en badges kunnen uitgeven.
- De focus voor het **controlekamerpersoneel** ligt op het afhandelen van noodoproepen of inkomende bedreigingen en eventueel de beveiligingsprotocollen activeren.

## TRAININGSDOSSIERS

Om een overzicht te hebben van de gegeven beveiligingstrainingen en om de benodigde opfristrainingen te plannen, is het raadzaam om voor alle personeelsleden een trainingsdossier bij te houden, met daarin:

- de datum en inhoud van de eerste training die ze hebben gevolgd;
- trainingsonderwerpen en sessiedatums van opfristrainingen;
- alle speciale vaardigheden waarin ze getraind zijn.

Het is ook aan te raden om het trainingsdossier door de deelnemers te laten ondertekenen om te bevestigen dat ze de training hebben gevolgd.

## OEFENINGEN

Regelmatige beveiligingsoefeningen helpen om het niveau van paraatheid binnen een organisatie te controleren en inzicht te krijgen in tekortkomingen en kwetsbaarheden.

- **Interne table-top oefeningen** kunnen worden gebruikt om de reactie op specifieke incidenten te simuleren en het activeren van de crisisorganisatie te oefenen.
- **Table-top oefeningen met externe partners** kunnen helpen om plannen, procedures en verantwoordelijkheden op elkaar af te stemmen.
- **Bij live oefeningen** moeten ook alle relevante externe partners worden betrokken. Ze zijn ook van cruciaal belang om ervoor te zorgen dat eerstehulpverleners vertrouwd zijn met de lay-out van de infrastructuur, het rollend materieel en de veiligheidsvoorschriften voor het busvervoer.

***Veiligheid in de bus is de verantwoordelijkheid van alle personeelsleden.***

# (8)
# NOODBEHEER

## CRISISBEHEER

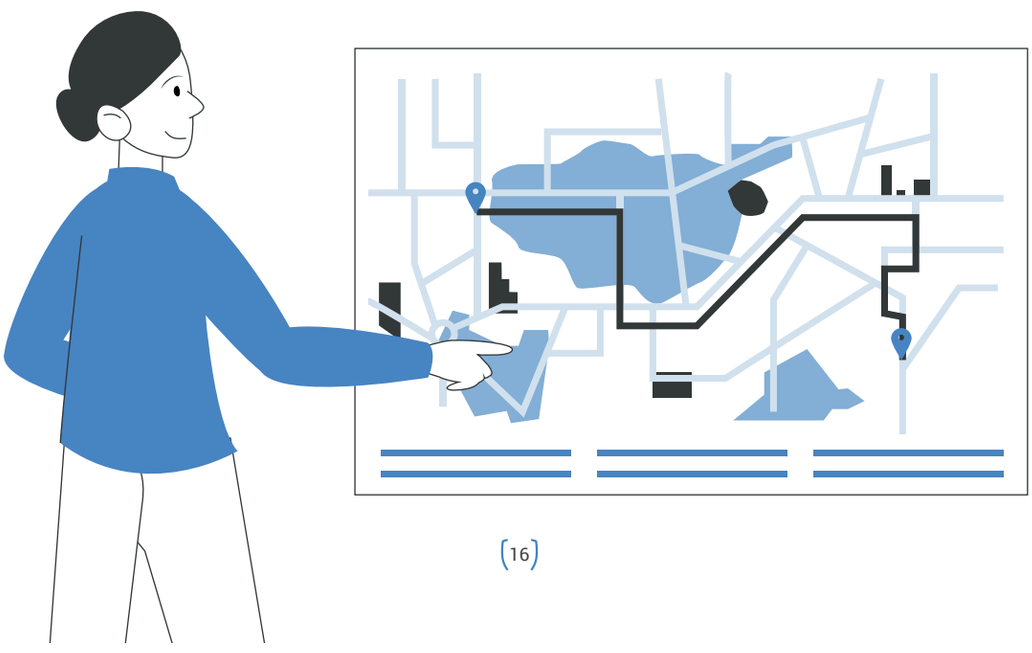
Gezien de complexiteit van de vervoerssystemen en de flexibiliteit van het busvervoer, omvat crisisbeheer niet alleen het afhandelen van de crisis op zich, maar ook de gevolgen beheersen van een crisis op één locatie voor de rest van het bedrijf. Een crisis aanpakken betekent niet automatisch de hele onderneming stilleggen, omdat er te veel mensen afhankelijk zijn van de beschikbaarheid. Er moet formeel een crisiscel worden opgericht. Alle afdelingen van de organisatie moeten erbij betrokken zijn en het moet zo snel mogelijk geactiveerd kunnen worden zodat het de leiding kan nemen over het crisisbeheer.

- Een **crisisbeheerplan** verduidelijkt de rol en de verantwoordelijkheden van alle afdelingen op het gebied van crisisbeheer en operationeel management onder gedegradeerde operationele omstandigheden, waarbij buslijnen worden omgeleid en diensten worden ingekort.
- Er moet een **crisiscommunicatieplan** worden opgesteld dat helpt om te gaan met de media-aandacht na een incident.

## BEDRIJFSCONTINUÏTEIT

Behalve de afhandeling van het eigenlijke incident, moet het noodbeheer ook rekening houden met bedrijfscontinuïteitsaspecten - diensten aanpassen en omleiden waar mogelijk en passagiers informeren over beschikbare diensten. Bedrijfscontinuïteitsplanning moet het volgende omvatten:

- Er moeten **back-up faciliteiten** voor kritieke functies worden geïdentificeerd (voertuigparkeerplaatsen of -onderhoud, voorlopige bushaltes of klantenservice faciliteiten), die gebruikt kunnen worden om de werkzaamheden voort te zetten als de standaard faciliteiten niet meer operationeel zijn of niet toegankelijk zijn.
- Er moeten **alternatieve routes** of een verkort busnetwerk worden uitgestippeld om te kunnen reageren op de verstoringen en incidenten langs de route of de gedeeltelijke onbeschikbaarheid van de busvloot.
- **Vervangende busdiensten** uitstippelen kan ook helpen om minder flexibele vervoerswijzen, zoals de trein of metro, te ondersteunen bij evenementen of grote verstoringen van het mobiliteitsnetwerk.



# (9)

# TRAININGSRICHTLIJNEN

## INLEIDING

In dit hoofdstuk wordt aandacht besteed aan een basisles in beveiligingstraining voor operationeel personeel in het openbaar vervoer. Het doel van de les is om het algemene beveiligingsbewustzijn te vergroten, de rol en verantwoordelijkheid van operationeel personeel te verduidelijken, hen aan te moedigen om bij te dragen en het vertrouwen te geven om de juiste actie te ondernemen. Het beschrijft de vaardigheden en competenties die nodig zijn om:

- Er toe bij te dragen dat openbare vervoersruimten gecontroleerde en beheerde ruimten zijn;
- Verdachte situaties te herkennen en te begrijpen hoe deze te melden;
- Te reageren op noodsituaties, waarbij passagiers worden beschermd zonder hun eigen veiligheid in gevaar te brengen.

Deze trainingsrichtlijnen zijn ontwikkeld aan de hand van een aantal basisscenario's, waarbij het waarschijnlijk is dat operationele medewerkers de eerste personen zijn die geconfronteerd zullen worden en zullen moeten ingrijpen. Deze zijn gebaseerd op Deliverable 4.1 «Handleiding voor chauffeurs voor beveiliging in het openbaar vervoer», die als referentie kan worden uitgedeeld aan het personeel.

***Deze richtlijnen zijn ontwikkeld rond een aantal basisscenario's.***

# INHOUD VAN DE TRAINING

## TERRORISMEBESTRIJDING

In het inleidende deel van de training wordt uitgelegd wat terrorisme is en waarom het een belangrijk onderwerp is voor openbaarvervoersbedrijven.

*Referentie 1 – Handleiding voor chauffeurs "Terrorismebestrijding"*

Terrorisme betekent het gebruik van geweld of andere criminele acties als een gerechtvaardigd middel om politieke doelen te bereiken. Het doel is om mensen bang te maken, gemeenschappen te verzwakken of economieën te destabiliseren.

Helaas zijn openbare vervoersystemen herhaaldelijk het doelwit geweest van terroristische activiteiten, met de bedoeling de werkzaamheden te verstoren en mobiliteitsdiensten te saboteren.

Mogelijke doelwitten voor terroristische activiteiten kunnen onze voertuigen en infrastructuur zijn, zoals stations, depots en werkplaatsen, klantencentra of administratieve gebouwen. Het doel zou ook kunnen zijn om mensen die gebruik maken van het openbaar vervoer schade te berokkenen.

Als vervoerders zijn wij verantwoordelijk voor de veiligheid en het welzijn van onze passagiers. Dit houdt in dat je op verdachte situaties en activiteiten moet letten en waarnemingen moet melden, maar ook dat je moet kunnen omgaan met noodsituaties en bedreigingen.

## PREVENTIE

In dit hoofdstuk wordt uitgelegd hoe enkele «basismaatregelen» kunnen bijdragen om te voorkomen dat onbevoegden toegang krijgen tot beperkte openbaarvervoersfaciliteiten en bedrijfsmiddelen en hoe je ongewone situaties in de gaten kunt houden.

Het is belangrijk om deelnemers eraan te herinneren dat de vereiste aandacht niets toevoegt aan hun professionele rol en dat er niet van hen wordt verwacht dat ze buiten het beleid en de procedures van de organisatie handelen.

*Referentie 2 – Handleiding voor chauffeurs "Preventie"*

Een belangrijke beschermingsmaatregel is het vermijden van onbevoegde toegang tot faciliteiten met beperkte toegang. Dit zijn onder andere depots, werkplaatsen, kleedkamers en administratieve gebouwen, maar ook de bestuurdersplaats in voertuigen.

- Als je een **onbekende persoon** ziet op een depot of locatie, controleer dan wie het is en bied hulp aan.
- **Zorg ervoor dat uw deuren gesloten** zijn elke keer dat u een voertuig onbeheerd achterlaat.

Openbare faciliteiten, zoals stations, bushaltes of klantencentra hebben een beperkte toegangscontrole. Het is belangrijk om hier op ongewoon gedrag of ongewone situaties te letten.

- **Wees alert** op mensen die zich verdacht en nerveus gedragen in de bus, op stations of bij haltes.
- **Controleer uw voertuig regelmatig** op verdachte voorwerpen en verloren voorwerpen telkens wanneer u het depot verlaat, zo vaak mogelijk tussen ritten door en elke keer u terugkeert naar het depot.

## VERDACHTE SITUATIES

Dit hoofdstuk is erop gericht deelnemers in staat te stellen verdachte situaties te herkennen en hen aan te moedigen dergelijke situaties te melden. Het is belangrijk om deelnemers eraan te herinneren dat ze geen risico's moeten nemen en dat hun veiligheid prioriteit heeft. De basisscenario's die voor deze training zijn geselecteerd, worden in twee delen behandeld:

- Hoe kun je merken dat dit een verdachte situatie is?
- Wat moet je doen als er reden tot bezorgdheid is?

De hieronder voorgestelde responsprocedures zijn algemeen en zijn bedoeld als algemene richtlijnen. Ze kunnen worden aangepast aan het bestaande bedrijfsbeleid.

De volgende situaties werden geselecteerd:

### VIJANDIGE VERKENNING

Een cruciale stap in het voorbereiden van elke criminele activiteit is vijandige verkenning. Vijandige verkenning betekent het verzamelen van informatie over onze faciliteiten en activiteiten die bij een aanval kunnen worden misbruikt. Kritieke informatie kan worden verzameld door medewerkers te observeren of rechtstreeks om informatie te vragen.

Indicatoren voor vijandige verkenning zijn onder meer:

- Foto's of video's maken van stations of andere bedrijfsfaciliteiten;
- Herhaalde of ongewoon lange aanwezigheid van mensen op stations zonder gebruik te maken van een busdienst;
- Proberen om faciliteiten met beperkte toegang te betreden of veiligheidsmaatregelen, zoals poorten en hekken, te omzeilen;
- Ongepaste of ongebruikelijke vragen stellen over beveiligingsmaatregelen of operationele procedures.

Als u gedrag waarneemt dat niet overeenkomt met de normale dagelijkse activiteiten van passagiers, volg dan deze instructies:

| | |
|---|---|
| **Bied hulp aan** | *Als u zich veilig voelt, benader de persoon dan en bied hulp aan.* |
| **Informeer dispatching** | *Geef details over het incident of dat uw reden voor bezorgdheid moet worden vastgelegd.* |

*Referentie 3 – Handleiding voor chauffeurs "Vijandige verkenning"*

### VERDACHTE VOORWERPEN

Passagiers laten vaak bagage of voorwerpen achter. Achtergelaten voorwerpen kunnen echter opzettelijk zijn achtergelaten en gevaarlijke stoffen bevatten, zoals explosieven of chemicaliën.

Achtergelaten voorwerpen mogen alleen worden opgehaald en overgedragen aan de dienst Verloren Voorwerpen als er geen reden tot bezorgdheid is. Het No-touch protocol [Niet-aanraken protocol] helpt om verdachte voorwerpen te identificeren.

Een verdacht voorwerp is een achtergelaten voorwerp dat één van de volgende kenmerken heeft:

| | |
|---|---|
| **NO-T** | **Niet typisch voor de omgeving (waarschijnlijk geen verloren voorwerp).** |
| **OU** | **Heeft duidelijk verdachte eigenschappen (het voorwerp is nat of vuil, heeft een vreemde geur, is afgesloten met touw of tape).** |
| **C** | **De omstandigheden geven aanleiding tot bezorgdheid (achtergelaten in een drukke omgeving, bedekt met poeder, met zichtbare kabel of aluminiumfolie).** |
| **H** | **Opzettelijk verborgen (geen reden om hier te zijn, neergezet op een ongebruikelijke locatie - onder een stoel of naast een vuilnisbak).** |

Als u een voorwerp vindt dat reden tot bezorgdheid geeft, volgt u deze instructies:

- ✓ *Let **WEL** vanop een afstand op verdachte tekens!*
- ✓ *Waarschuw **WEL** het OCC en geef relevante details over het voorwerp! (De exacte locatie, vorm, grootte, enz.)*
- ✓ *Probeer **WEL** de eigenaar te vinden!*
- ✓ *Waarschuw **WEL** de mensen in de buurt en instrueer hen om uit de buurt te blijven!*
- ✓ *Observeer het voorwerp **WEL** vanop een afstand tot het beveiligingspersoneel arriveert!*
- ✗ *Raak het voorwerp **NIET** aan, niet schudden en niet openen!*
- ✗ *Gebruik **GEEN** communicatieapparaat of gsm in de buurt van het verdachte voorwerp!*
- ✗ *Rook **NIET** in de buurt van het voorwerp!*
- ✗ *Veroorzaak **GEEN** paniek bij het publiek dat op de locatie aanwezig is!*
- ✗ *Gebruik **GEEN** metalen voorwerpen in de buurt van het voorwerp!*

*Referentie 4 – Handleiding voor chauffeurs "Verdachte voorwerpen"*

## VERDACHT GEDRAG VAN PASSAGIERS

Verdachte aanwijzingen kunnen afkomstig zijn van het uiterlijk of het gedrag van de passagier en bestaan uit indicatoren zoals:

- Ongepaste kleding voor de plaats, tijd en plaatselijke omstandigheden;
- Bagage die niet bij het uiterlijk past;
- Bagage die disproportioneel zwaar is.
- Zenuwachtigheid of angst;
- Stiekem contact met andere passagiers;
- Weigeren om mee te werken met het personeel;
- Ongerechtvaardigde aanwezigheid of rondhangen.

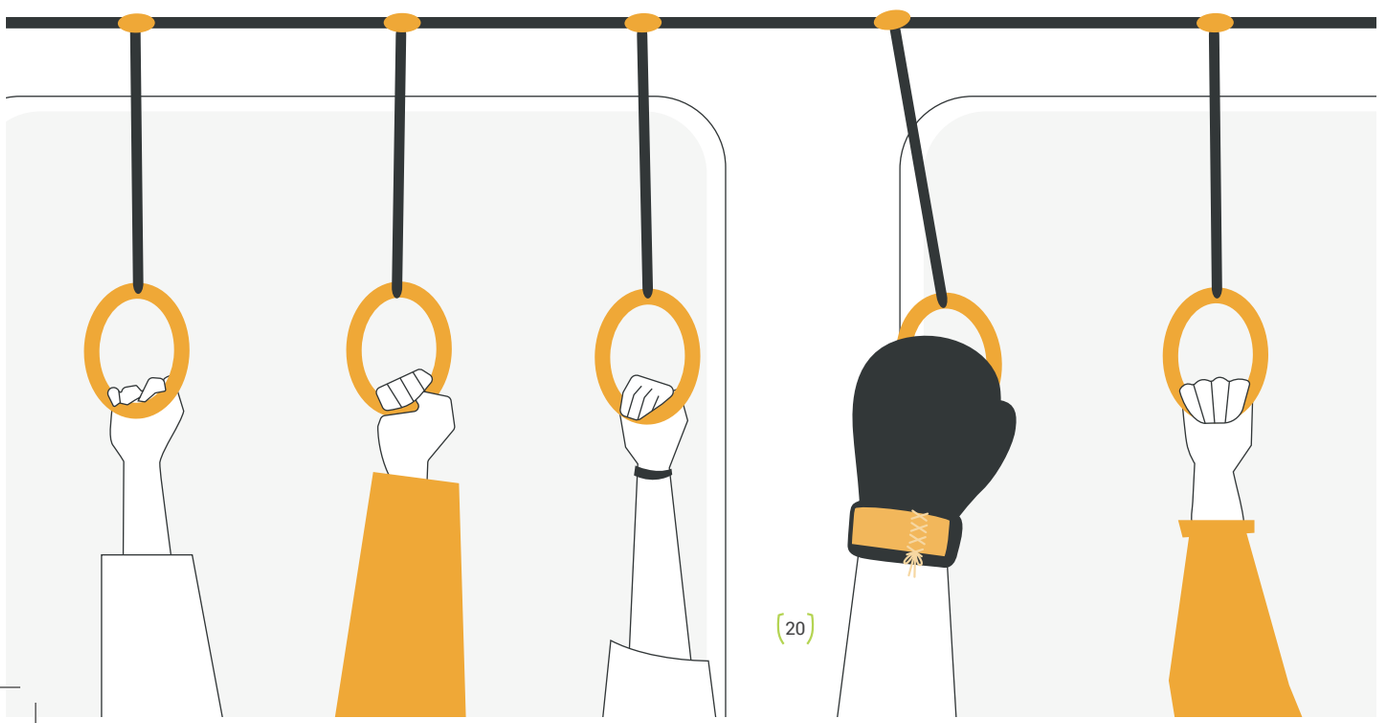
Als het gedrag van een passagier reden tot bezorgdheid geeft, volgt u deze instructies:

| | |
|---|---|
| **Stop het voertuig!** | *Stop op een veilige plaats, zet de motor af en blijf kalm. Informeer de passagiers en suggereer dat het voertuig een defect heeft.* |
| **Neem contact op met Dispatch!** | *Meld uw reden voor bezorgdheid en beschrijf de situatie.* |
| **Evacueer het voertuig!** | *Evacueer uzelf en uw passagiers op een veilige afstand!* |
| **Houd de passagier in de gaten** | *Blijf de verdachte passagier zo mogelijk vanop een veilige afstand in de gaten houden!* |
| **Wacht op hulp** | *Blijf tot een verantwoordelijke persoon bevestigt dat u mag vertrekken.* |

*Referentie 5 – Handleiding voor chauffeurs "Verdacht gedrag van passagiers"*

Er wordt aan de deelnemers uitgelegd hoe de meldingen worden gecontroleerd en afgehandeld. Het is belangrijk om uit te leggen waarom er misschien geen zichtbare opvolging gebeurt (controle met CCTV-camera's, geplande herstellingswerken, enz.). Het is ook belangrijk om in de training aandacht te besteden aan hoe mensen hun eigen vooroordelen kunnen herkennen en ze zich daarvan bewust zijn wanneer ze potentiële bedreigingen moeten inschatten.

***Het is belangrijk om personeel dat melding maakt van verdachte situaties daarvoor te waarderen. Het houdt hen oplettend en moedigt anderen aan waakzaam te zijn.***



## NOODSITUATIES

Het laatste hoofdstuk geeft instructies over hoe te reageren op noodsituaties, voornamelijk voor medewerkers die met klanten te maken hebben. Nogmaals, het is belangrijk om deelnemers eraan te herinneren dat ze geen risico's moeten nemen en dat hun veiligheid prioriteit heeft. Nadat u een alarmmelding hebt gegenereerd, is het aan te raden om elke instructie te baseren op het Run-Hide-Report principe.

- **DRUK OP HET ALARM – waarschuw Dispatch indien mogelijk, zodat deze op de hoogte is van de noodsituatie en de juiste reactie in gang kan zetten.**
- **RUN [REN] – Loop zo snel mogelijk weg van het gevaar.**
- **HIDE [VERBERG JE] – Blijf uit het zicht.**
- **REPORT [MELD] – Bel Dispatch met meer details zodra het veilig is.**

De hieronder voorgestelde responsprocedures zijn algemeen en zijn bedoeld als algemene richtlijnen. Ze kunnen worden aangepast aan het bestaande bedrijfsbeleid.

De volgende scenario's werden geselecteerd:

### AANVAL AAN BOORD

Volg deze instructies in het geval van een onmiddellijke bedreiging voor uzelf en/of het leven en de gezondheid van een passagier.

| | |
|---|---|
| **Druk op het alarm!** | *Druk op de alarmknop.* |
| **Open de deuren!** | *Stop het voertuig zodat passagiers kunnen ontsnappen. Instrueer hen om, indien mogelijk, te vertrekken.* |
| **Ren weg en verberg je!** | *Ga weg van het gevaar en zet uw telefoon op stil.* |
| **Meld details!** | *Zodra u verborgen bent, bel Dispatch met meer informatie.* |

*Referentie 5 – Handleiding voor chauffeurs "Aanval aan boord"*

### AANVAL BUITEN HET VOERTUIG

Als u een aanval bij een halte of station waarneemt of als uw voertuig van buitenaf wordt aangevallen, volgt u deze instructies:

| | |
|---|---|
| **Druk op het alarm!** | *Druk op de alarmknop.* |
| **Niet stoppen!** | *Blijf rijden en stop niet (indien mogelijk)! Informeer de passagiers.* |
| **Bel dispatch!** | *Geef zo snel mogelijk meer informatie.* |

*Referentie 6 – Handleiding voor chauffeurs "Aanval buiten het voertuig"*

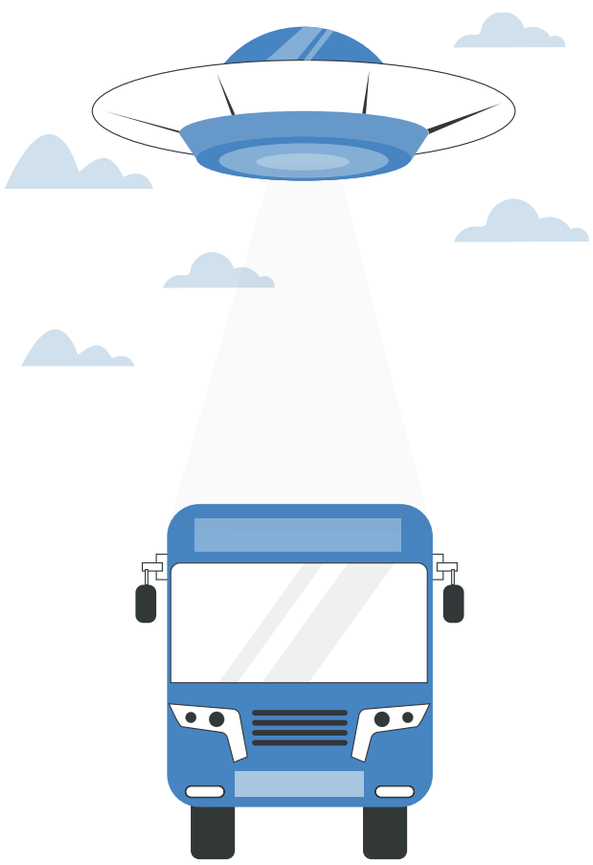
### KAPING EN GIJZELING

Als een voertuigkaping of gijzeling een bedreiging vormt voor uzelf en/of het leven en de gezondheid van uw passagiers, volg dan deze instructies:

| | |
|---|---|
| **Druk op het alarm!** | *Druk indien mogelijk discreet op de alarmknop.* |
| **Blijf kalm** | *Verzet u niet, spreek hen niet tegen, gehoorzaam de instructies van de dader.* |
| **Trek geen aandacht** | *Probeer geen aandacht te trekken, vermijd oogcontact, maak geen plotselinge bewegingen.* |

*Referentie 7 – Handleiding voor chauffeurs "Kaping en gijzeling"*

***Vergeet nooit dat jouw veiligheid prioriteit heeft.***



# 1

SAFEBUS