

PODRĘCZNIK ZARZĄDZANIA PROCEDURAMI SZKOLENIOWYMI W TRANSPORCIE



SPIS TREŚCI

(1)	Wprowadzenie	4
(2)	Poradnik antyterrorystyczny	5
	Informacje o projekcie	5
	Zagrożenia i cele	5
	Zasady i środki bezpieczeństwa	
(3)	Ocena i monitorowanie ryzyka	8
	Ocena zagrożeń	8
	Ocena ryzyka	8
	Monitorowanie ryzyka	8
(4)	Bezpieczeństwo budynku	9
	Obiekty użyteczności publicznej	9
	Obiekty o ograniczonym dostępie	11
(5)	Bezpieczeństwo pojazdu	12
(6)	Bezpieczeństwo organizacyjne	13
	Kultura bezpieczeństwa	13
	Świadomość	13
	Bezpieczeństwo osobowe	13
	Informacja i cyberbezpieczeństwo	14
	Bezpieczeństwo stron trzecich	14
(7)	Szkolenie w zakresie bezpieczeństwa	15
	Potrzeby w zakresie szkolenia	15
	Dokumentacja szkoleń	15
	Ćwiczenia	15
(8)	Zarządzanie w sytuacji kryzysowej	16
	Zarządzanie kryzysowe	16
	Ciągłość działania	16
(9)	Porady szkoleniowe	17
	Wprowadzenie	17
	Treść szkolenia	18

(1)

WPROWADZENIE

Operatorzy transportu są odpowiedzialni za bezpieczeństwo i dobre samopoczucie swoich pasażerów. Oprócz zapewnienia bezpiecznego i niezawodnego transportu obejmuje to również ochronę przed przestępczością i potencjalnymi aktami terroryzmu.

Niniejszy podręcznik jest przeznaczony dla kierowników ds. bezpieczeństwa i zawiera wskazówki dotyczące środków i polityk mających na celu:

- **Ocenę** potencjalnego narażenia organizacji transportu publicznego na działalność terrorystyczną.
- **Zapobieganie** atakom terrorystycznym i ograniczanie szkód, które mogą zostać wyrządzone.
- **Wykrywanie** podejrzanych sytuacji i złych intencji.
- **Reagowanie** na sytuacje awaryjne.

Struktura i kontekst operatorów transportu publicznego są bardzo zróżnicowane, a plany i polityki bezpieczeństwa muszą uwzględniać indywidualną sytuację.

Niniejszy podręcznik ma być schematem, przedstawiającym aspekty, które należy uwzględnić, oraz najlepsze praktyki, które mogą pomóc w opracowaniu planów i procedur bezpieczeństwa specyficznych dla firmy.

(2)

PORADNIK ANTYTERRORYSTYCZNY

INFORMACJE O PROJEKCIE

Terroryzm oznacza użycie przemocy lub innych czynów przestępczych jako uzasadnionych środków do osiągnięcia celów politycznych. Niestety, systemy transportu publicznego wielokrotnie były celem działań terrorystycznych, mających na celu zakłócenie funkcjonowania i sabotowanie usług mobilności.

Potencjalnymi celami działań terrorystycznych mogą być nasze pojazdy i infrastruktura. Celem może być również wyrządzenie szkody osobom korzystającym z transportu publicznego.

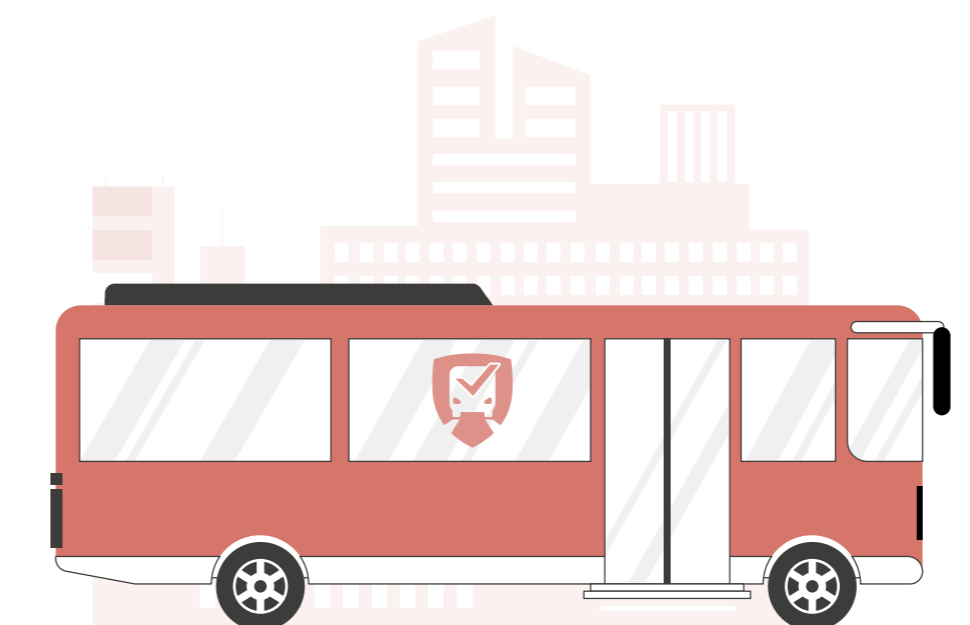
Jako przewoźnicy odpowiedzialni jesteśmy za bezpieczeństwo i dobro naszych pasażerów i personelu. Obejmuje to rozsądne środki zapobiegające incydom, ale także gotowość do reagowania na nie i ograniczanie szkód w jak największym stopniu.

ZAGROŻENIA I CELE

ISTOTNE ZASOBY

Do świadczenia usług w zakresie transportu na rzecz swoich klientów autobusy potrzebują różnorodnych zasobów, z których część jest publicznie dostępna, a część chroniona lub z ograniczonym dostępem. Istotne zasoby obejmują:

- **Zasoby związane** z pasażerami, w tym dworce i węzły przesiadkowe, przystanki, centra handlowe i informacyjne, ewentualnie przechowalnie bagażu. Obiekty te są ogólnodostępne z ograniczonymi możliwościami kontroli dostępu.
- **Zasoby związane** z eksploatacją, które obejmują pojazdy, zajezdnie i warsztaty, a także obiekty zaopatrzenia w paliwo. Dostępność tych obiektów jest różna.
- **Zasoby pomocnicze** obejmują pomieszczenia kontrolne, personel i obiekty usługowe oraz budynki administracyjne. Są one porównywalne z zasobami każdej innej firmy i nie są dostępne publicznie.
- **Zasoby cyfrowe** mają coraz większe znaczenie dla działalności autobusów. Mogą one obejmować systemy kontroli operacyjnej, systemy informacji pasażerskiej oraz systemy zarządzania biznesowego do sprzedaży biletów, płatności i rezerwacji. Fizyczny dostęp do tych zasobów jest zwykle zintegrowany z zasobami związanymi z operacją lub zasobami pomocniczymi, które nie są otwarte dla publiczności.



SCENARIUSZE INCYDENTÓW

W oparciu o ostatnie ogólne wydarzenia i incydenty, w szczególności w sektorze transportu publicznego, można rozważyć poniższą (niewyczerpującą) listę scenariuszy.

- **Improwizowane urządzenie wybuchowe (IED)** – prowizoryczne urządzenie wybuchowe, które jest schowane w zwykłym bagażu lub ukryte poza zasięgiem wzroku, ewentualnie pod siedzeniami lub w pojemnikach na śmieci. Urządzenia IED mogą być wyzwalone za pomocą zegara lub zdalnie, nie ma potrzeby, aby atakujący znajdował się w pobliżu.
- **Atak samobójczy** – atakujący przenosi ładunek wybuchowy bezpośrednio do systemu autobusowego i uruchamia go bezpośrednio.
- **Atak bronią palną** – atakujący strzelający do celu lub na oślep, z odległości lub z bliska.
- **Atak nożem** – atakowanie ludzi nożami lub ostrzami z bliskiej odległości.
- **Sabotaż** – wandalizm, kradzież lub manipulacja sprzętem mająca na celu naruszenie zdolności operacyjnej i bezpieczeństwa.
- **Podpalenie** – celowe podpalenie w celu zniszczenia zasobów.
- **Atak samochodowy** – użycie pojazdu do zderzenia z pasażerami lub autobusem.
- **Atak autobusowy** – użycie autobusu do zderzenia się z ludźmi w dowolnym miejscu.
- **Wzięcie zakładników/porwanie** – atak polegający na przetrzymywaniu ludzi z bezpośrednim zagrożeniem dla ich życia, na przystankach lub na pokładzie pojazdów.
- **Zagrożenie bombowe** – groźba zdetonowania urządzenia wybuchowego w systemie autobusowym, niezależnie od tego, czy takie urządzenie faktycznie istnieje.
- **Cyberatak** – atak ukierunkowany na komputerowe systemy informacyjne, sieci lub urządzenia.
- **Atak CBRN** – atak z użyciem substancji chemicznych, biologicznych, radiologicznych lub jądrowych.

ZASADY I ŚRODKI BEZPIECZEŃSTWA

ELEMENTY KONCEPCJI BEZPIECZEŃSTWA

Dostępnych jest wiele narzędzi i zabezpieczeń chroniących transport publiczny. Rozsądna koncepcja bezpieczeństwa wykorzystuje je wszystkie, aby stworzyć skuteczną mieszankę.

Środki **infrastrukturalne** stanowią podstawę do odstraszenia wszelkich ataków i ograniczania potencjalnych szkód. Obejmują one następujące elementy:

- Konstrukcja i materiały użyte do budowy dowolnego składnika zasobów,
- Układ, projekt i organizacja przestrzenna dowolnego obszaru,
- Rozmieszczenie słupków ochronnych i bram kontroli dostępu.

Narzędzia **technologiczne** pomagają zabezpieczyć rozległe obszary, scentralizować monitoring i sprawną dyspozycję personelu. Obejmują one:

- Monitoring CCTV, analitykę wideo i kryminalistykę,
- Słupy awaryjne i przyciski pomocy,
- Technologie bezpieczeństwa, takie jak zamki i klucze lub czujniki wykrywające potencjalnie podejrzane sytuacje,
- Technologię komunikacyjną koordynującą weryfikację i reagowanie na incydenty.

Personel jest kluczowym czynnikiem w koncepcjach bezpieczeństwa, a zatem obejmuje wyspecjalizowanych pracowników ochrony, ale także pracowników operacyjnych i obsługi klienta. Istotnymi aspektami są:

- Role i obowiązki,
- Harmonogramy i procedury,
- Szkolenia i edukacja.

Środki organizacyjne stanowią ramy dla całej koncepcji bezpieczeństwa i obejmują:

- Monitoring,
- Bezpieczeństwo, zarządzanie kryzysowe i organizację kryzysową,
- Przydzielanie ról i obowiązków, a także kierowanie współpracą między działami bezpieczeństwa i operacji,
- Współpracę w zakresie bezpieczeństwa z władzami, służbami ratunkowymi i partnerami biznesowymi.

ZASADY ZARZĄDZANIA BEZPIECZEŃSTWEM

ZAPOBIEGANIE w bezpieczeństwie transportu publicznego ma kluczowe znaczenie. Środki zapobiegawcze mają na celu identyfikację i łagodzenie potencjalnych zagrożeń zanim wyrządzą one jakąkolwiek szkodę oraz zniechęcenie potencjalnych przestępców do podejmowania prób ataków i zakłócania systemów transportu publicznego.

Zasadniczo dostępne są dwie strategie ochrony tych zasobów - **kontrola dostępu** w celu stworzenia środka odstraszonego i monitorowania kto wchodzi do obiektu, oraz **wzmocnienie infrastruktury** w celu ograniczenia szkód, które mogą być spowodowane potencjalnym atakiem.

Środki **WYKRYWANIA** są ważnym uzupełnieniem środków zapobiegawczych. Mają one na celu **identyfikację potencjalnych zagrożeń dla bezpieczeństwa oraz ułatwienie szybkiej i ukierunkowanej reakcji**.

Personel odgrywa kluczową rolę w wykrywaniu potencjalnych zagrożeń, ale biorąc pod uwagę rozszerzenie obsługiwanych zasobów i sieci w transporcie publicznym, technologia zapewnia ważne wsparcie w monitorowaniu całego terytorium.

GOTOWOŚĆ zakłada, że zapobieganie może zawieść i obejmuje plany awaryjne określające role i obowiązki, protokoły komunikacji i procedury reagowania, a także planowanie ciągłości działania.

Personel potrzebuje regularnych **szkoleń i ćwiczeń**, aby zapoznać się ze swoimi rolami i obowiązkami w celu zapewnienia skutecznej reakcji na sytuacje awaryjne. **Planowanie ciągłości działania** musi zapewniać ograniczenie wpływu operacyjnego wszelkich incydentów i przewidywać plany awaryjne.

REAGOWANIE NA INCYDENTY obejmuje mobilizację personelu i zasobów w celu zareagowania na sytuację kryzysową. Ataki terrorystyczne mogą doprowadzić do eskalacji sytuacji kryzysowej.

Oprócz aktywacji wewnętrznych protokołów komunikacji kryzysowej i rozmieszczenia wewnętrznych zespołów reagowania, zarządzanie kryzysowe wymaga aktywacji komórki kryzysowej i koordynacji z zewnętrznymi służbami ratowniczymi.

Po każdej sytuacji awaryjnej ważne jest przeprowadzenie oceny w celu sprawdzenia, w jaki sposób można poprawić reagowanie w sytuacjach awaryjnych i ocenić potencjał poprawy profilaktyki.

Operatorzy transportu są odpowiedzialni za bezpieczeństwo i dobre samopoczucie swoich pasażerów.



(3)

OCENA I MONITOROWANIE RYZYKA

OCENA ZAGROZEŃ

Podstawą każdej koncepcji i planu bezpieczeństwa jest dokładna ocena zagrożeń i ryzyka, na które potencjalnie narażona jest organizacja. Chociaż transport publiczny jest uważany za cel działań terrorystycznych, poziom zagrożenia różni się w zależności od kilku czynników, takich jak ogólna sytuacja polityczna w danym kraju/regionie, wielkość i znaczenie gospodarcze danego miasta lub niedawne ataki przeprowadzone w innym miejscu.

Obraz zagrożenia musi być regularnie weryfikowany, ponieważ docelowe priorytety i sposób działania potencjalnych przestępców stale się zmieniają. Ponadto planowane wydarzenia na wysokim szczeblu, takie jak duże imprezy sportowe lub zgromadzenia publiczne, mogą tymczasowo ten poziom podnieść.

Poziom zagrożenia powinien być oceniany we współpracy z odpowiednimi władzami, które będą miały głębszy wgląd w obecną sytuację globalną i lokalną.

OCENA RYZYKA

Oceny ryzyka i podatności na zagrożenia pomagają operatorom autobusowym zidentyfikować potencjalne słabe punkty i ustalić priorytety inwestycji w modernizację ich obiektów. Oceny te powinny być regularnie powtarzane, aby odzwierciedlić zmiany strukturalne lub działania budowlane. Należy je ponadto dostosowywać do pojawiania się nowych zagrożeń i rozwoju sposobu działania. Istotne jest, aby nie ograniczać oceny ryzyka i podatności na zagrożenia do zasobów krytycznych, ale również uwzględnić przestrzenie publiczne potrzebne do funkcjonowania usług autobusowych.

- W ramach projektu COUNTERACT, koordynowanego przez UITP, opracowano metodologię oceny ryzyka i podatności na zagrożenia specjalnie dostosowaną do sektora transportu publicznego. Jest ona stale aktualizowana w związku ze zmieniającą się sytuacją zagrożenia i jest zalecana przez UITP do stosowania przez operatorów transportu publicznego.

MONITOROWANIE RYZYKA

Środowisko ryzyka związanego z bezpieczeństwem, również w przypadku operacji autobusowych, stale się zmienia. Mogą pojawić się nowe scenariusze zagrożeń, renowacja zasobów firmy może stworzyć nowe potencjalne słabe punkty, zdarzenia lub nowe projekty budowlane w obszarze operacyjnym mogą skutkować nowymi potencjalnymi celami. Dlatego tak ważne jest ciągłe monitorowanie ryzyka. Ma zapewnić, że strategie zarządzania nim są skuteczne i dostosowane do zmieniającego się środowiska ryzyka.

- Na **poziomie korporacyjnym** ścisła współpraca z odpowiednimi organami może pomóc w jak najwcześniejszym poznaniu zmian w ocenie zagrożeń i potencjalnych konsekwencji dla funkcjonowania przewozów autobusowych.
- Na **poziomie operacyjnym** należy regularnie powtarzać oceny ryzyka i podatności na zagrożenia, aby odzwierciedlić zmiany w infrastrukturze, zakup nowych pojazdów, rozwój technologii oraz przeprowadzać testy warunków skrajnych zgodnie z ewolucją scenariuszy incydentów, o których informują władze lub które miały miejsce w innych organizacjach transportu publicznego.
- Na **poziomie lokalizacji** regularne audyty bezpieczeństwa pomagają ustalić, czy istniejące zabezpieczenia są nadal funkcjonalne i odpowiednie do ochrony zasobów firmy.

(4)

BEZPIECZEŃSTWO BUDYNKU

OBIEKTY UŻYTECZNOŚCI PUBLICZNEJ

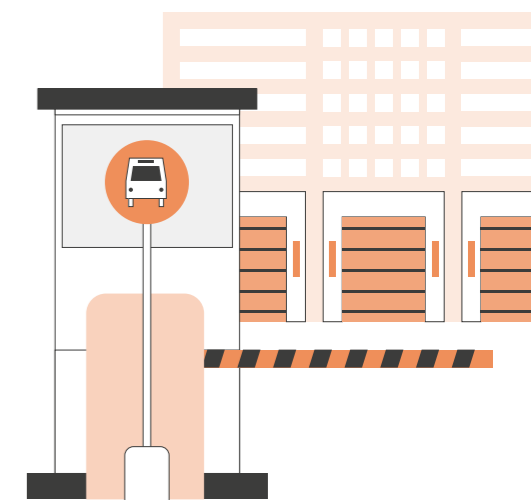
Obiekty związane z pasażerami są publicznie dostępne i muszą być w stanie sprawnie obsłużyć dużą liczbę osób. Potencjał środków kontroli dostępu jest ograniczony. Kluczowe zasady ochrony dworców i przystanków autobusowych obejmują monitorowanie w celu identyfikacji potencjalnie podejrzanych sytuacji oraz wzmocnienie infrastruktury w celu powstrzymania i ograniczenia skutków potencjalnego ataku.

PROJEKTOWANIE I INFRASTRUKTURA

Normy i wytyczne dotyczące rozmieszczenia dworca i materiałów bardzo się zmieniły w ostatnich latach i są przestrzegane przy nowych konstrukcjach lub modernizacji istniejących obiektów i urządzeń. Ogólnie rzecz biorąc, systemy transportu publicznego są jednak nowe i obejmują starą infrastrukturę bezpośrednio osadzoną w przestrzeni publicznej. Kluczowe środki, które należy uwzględnić na dworcach autobusowych, obejmują:

- **Dobre pole widzenia** w każdym obiekcie związanym z pasażerami pomaga monitorować obszar, unikać tworzenia obszarów ukrycia i ułatwiać szybką ewakuację w razie potrzeby. Meble, automaty sprzedające oraz ekrany i tablice informacyjne powinny być wykonane z materiałów odpornych na akty wandalizmu i powinny być ustawione tak, aby nie zasłaniały widoku.
- **Odpowiednie oświetlenie** jest niezbędne dla dobrej orientacji i widoczności pasażerów. Pomaga również w nadzorze i monitoringu dworców autobusowych przez kamery CCTV.
- **Układ dworca** powinien oddzielać pozostawiony bagaż i inne obiekty magazynowe od hal, peronów i tras przepływu pasażerów, aby zminimalizować wpływ potencjalnego wybuchu.

- **Zamki i plomby** mogą uniemożliwić dostęp do szafek na kubki, skrzynek ze sprzętem lub dostęp do instalacji technicznych, które mogą być potencjalnie wykorzystywane jako miejsca ukrycia. Tam, gdzie nie można zainstalować zamków, należy zamontować plomby zabezpieczające.
- Kosze na śmieci należy uznać za miejsce łatwego ukrycia niebezpiecznych przedmiotów i substancji. **Przezroczyste plastikowe worki** zawieszane na metalowych uchwytach na obręcze pozwalają na maksymalną przejrzystość i są uważane za najlepszą praktykę. Jeśli to możliwe, kosze na śmieci należy umieścić w miejscach objętych monitoringiem, aby je obserwować. Kosze na śmieci należy regularnie opróżniać, aby jak najlepiej wykorzystać przezroczystość worków.
- Poczekalnie i przystanki autobusowe powinny być zabezpieczone przed atakami pojazdów bez narażania pasażerów na dostęp wolny od przeszkód. Ochronę można uzyskać za pomocą **barier fizycznych**, takich jak pachoły lub donice, a także podniesionych krawężników.
- Przezroczyste konstrukcje, takie jak wiaty przystankowe, powinny być wyposażone w **szyby ochronne**, aby uniknąć latającego lub spadającego szkła w przypadku wybuchu. Szkło laminowane lub folia przeciwoodpryskowa do modernizacji istniejących konstrukcji może również pomóc w zapobieganiu wandalizmowi i graffiti.



Kluczowe zasady ochrony dworców i przystanków autobusowych obejmują monitorowanie w celu identyfikacji potencjalnie podejrzanych sytuacji.

TECHNOLOGIA

Narzędzia technologiczne mogą znacznie pomóc w poprawie ochrony systemów autobusowych, a telewizja przemysłowa (CCTV) jest najczęściej używanym i najważniejszym narzędziem w transporcie publicznym.

- **Kamery CCTV** mogą zasadniczo wspierać monitorowanie dworców, ale często są zbyt szeroko rozpowszechnione, aby mogły być skutecznie pokryte przez personel. Kamery powinny stale dawać podgląd sytuacji na dworcu. Szczególny nacisk należy położyć na newralgiczne miejsca, takie jak punkty pomocy w nagłych wypadkach, skrzynki na sprzęt lub punkty dostępu do instalacji technicznych. Aby uniknąć manipulacji lub utraty dowodów w przypadku zniszczenia kamer podczas incydentów, powinny one być ustawione tak, aby się wzajemnie zakrywały.
- **Monitorowanie obrazu** z kamer w czasie rzeczywistym w pomieszczeniu kontrolnym pozwala na wykorzystanie CCTV do weryfikacji alarmów i zarządzania incydentami, wspierając efektywne wykorzystanie personelu.
- **Nagrania z kamer przemysłowych i nagrania audio** są niezbędnym dowodem w każdej sytuacji. Są one przechowywane przez prawnie wiążący okres, zanim zostaną nadpisane. Muszą mieć wystarczającą jakość, aby mogły być dopuszczone w procedurach prawnych.
- **Analityka wideo** w kamerach CCTV może pomóc w identyfikacji podejrzanych sytuacji. Otwarty charakter dworców i często duże zagęszczenie ludzi sprawiają, że warunki są trudne, ale technologia się rozwija. Najczęściej testowane algorytmy dla obiektów użyteczności publicznej obejmują wykrywanie porzuconych przedmiotów, agresywnych zachowań lub nietypowych ruchów pasażerów.

Czujniki i alarmy mogą pomóc w wykrywaniu potencjalnie podejrzanych sytuacji. Najczęściej instalacje dotyczą alarmów antywłamaniowych chroniących drzwi i zamki. Czujniki mogą wykrywać dym lub substancje chemiczne.

Technologia może również wspierać pasażerów i personel potrzebujący pomocy.

- **Interkomy sos** zainstalowane na głównych dworcach i węzłach umożliwiają pasażerom i personelowi wezwanie pomocy. Często interkomy te są wyposażone w kamery, aby zapobiec niewłaściwemu użyciu.
- **Kamery na ciele** mogą być używane do ochrony personelu. Działają jako środek odstraszcający przed agresją, ich obrazy na żywo pomagają personelowi dyspozytorni zrozumieć sytuację, a nagrania dostarczają dowodów w dochodzeniu w sprawie incydentów.

PERSONEL I PROCEDURY

Personel odgrywa wiele ról związanych z bezpieczeństwem na dworcach. Jego obecność działa odstraszcająco na potencjalnych sprawców i uspokaja pasażerów, pomagając stworzyć zarządzaną przestrzeń. Uważni pracownicy mogą skutecznie spełniać cele związane z obsługą pasażerów i bezpieczeństwem.

Proaktywna rola bezpieczeństwa personelu na stanowiskach obejmuje:

- **Czułość** w przestrzeni publicznej w celu identyfikacji potencjalnie podejrzanych sytuacji. Uwzględnia to nietypowe i niewłaściwe zachowanie, a także przedmioty pozostawione bez nadzoru. Personel musi być zaznajomiony z pojęciami podejrzanych zachowań i przedmiotów. Wszelkie obawy powinny być zgłaszane w celu umożliwienia wyjaśnienia lub podjęcia działań następczych przez pracowników ochrony lub policję. Aby uniknąć fałszywych alarmów, należy przeprowadzać szkolenie w zakresie rozpoznawania własnych uprzedzeń podczas oceny potencjalnych zagrożeń.
- **Regularne kontrole bezpieczeństwa** i patrolowanie dworca pomagają zwiększyć widoczność personelu. Patrole mogą być prowadzone wspólnie przez pracowników i mogą łączyć czułość z zaangażowaniem klientów i regularnym sprawdzaniem integralności fizycznych środków bezpieczeństwa. Patrole ochrony powinny mieć wyraźnie zarysowany obszar, który należy pokryć określonymi punktami styku i instrukcjami (np. fizyczne sprawdzenie, czy drzwi są zamknięte). Patrole bezpieczeństwa muszą być nieprzewidywalne i powinny być rejestrowane.

OBIEKTY O OGRANICZONYM DOSTĘPIE

Kontrola dostępu do obiektów i urządzeń o ograniczonym dostępie ma kluczowe znaczenie dla zapewnienia, że tylko upoważniony personel i materiały mogą dostać się na teren zakładu kontrolowanymi drogami wejściowymi. Wewnątrz lokalu ogólna czujność pomaga zapewnić zgłaszanie nietypowej obecności, zachowania i przedmiotów.

PROJEKTOWANIE I INFRASTRUKTURA

- Fizyczne bariery dostępu, takie jak ściany i ogrodzenia, powinny **chronić obszar** zajezdni, warsztatów lub innych obiektów o ograniczonym dostępie. Bariery te należy utrzymywać w dobrym stanie technicznym i można je uzupełnić o czujniki antywłamaniowe w celu zapewnienia dodatkowej ochrony.
- Wszystkie drzwi między strefami publicznymi i o ograniczonym dostępie powinny być zamknięte lub kontrolowane. Zasoby o ograniczonym dostępie, takie jak zajezdnie, powinny być wyposażone w **kontrolowane bramki dostępu**, umożliwiające wejście tylko upoważnionym osobom.

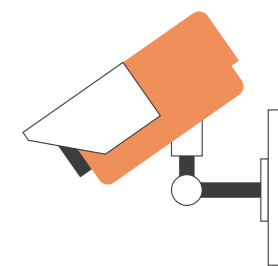
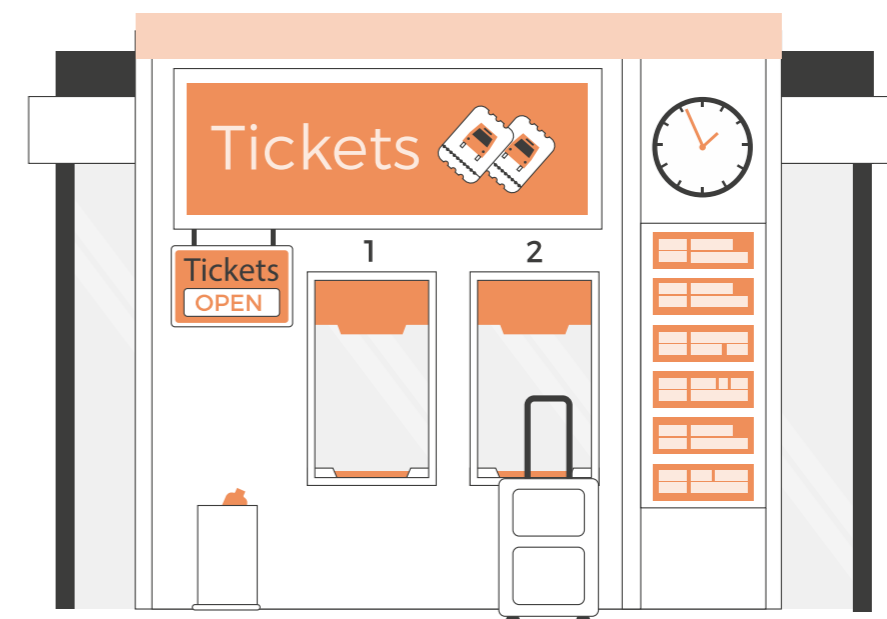
TECHNOLOGIA

- Kamery CCTV wyposażone w noktowizor mogą wspierać wykrywanie włamań poprzez monitorowanie wewnętrznego i zewnętrznego obwodu, aby zapobiec nieuprawnionemu dostępowi.
- Geofencing może stworzyć wirtualny obwód jako dodatkową ochronę tam, gdzie nie można wznieść barier fizycznych. Może to pomóc w monitorowaniu otoczenia obiektu lub ustanowieniu strefy wysokiego poziomu bezpieczeństwa w obiekcie, takiej jak obszar parkowania nowego taboru.

- Analityka wideo zapewnia dodatkową ochronę w czasie, gdy obiekty o ograniczonym dostępie są zamknięte i nie odbywają się żadne działania operacyjne.

PERSONEL I PROCEDURY

- **Procedura odprawy** powinna zapewnić, że nieupoważniony personel i goście są sprawdzani i rejestrowani. Jeśli można zaparkować samochody prywatne, należy je skontrolować wraz z bagażem i poddać systemowi zezwoleń na parkowanie.
- Wydane **identyfikatory i zezwolenia** powinny być widoczne, aby zidentyfikować każdą osobę lub samochód jako akredytowany. Powinny być noszone w sposób widoczny, gdy ludzie znajdują się w zamkniętych obiektach. Jasne procedury logowania/wypisywania ułatwiają również ewakuację w razie potrzeby.
- **Autobusy i autokary** powinny być sprawdzane przy wchodzeniu i wychodzeniu z obiektów o ograniczonym dostępie w celu zapewnienia, że na pokładzie nie znajdują się żadne przedmioty bez nadzoru ani osoby nieupoważnione. Kontrole te mogą być przeprowadzane przez kierowców i powinny być rejestrowane.
- **Czułość personelu** i patrole obiektów, podobnie jak w obiektach publicznych, są kluczowe dla zapewnienia identyfikacji potencjalnie podejrzanych sytuacji. Należy zaangażować nieznanne osoby, aby potwierdzić ich cel i zamiary. Personel musi być zaznajomiony z pojęciami podejrzanych zachowań i przedmiotów. Wszelkie obawy powinny być zgłaszane w celu umożliwienia wyjaśnienia lub podjęcia działań przez pracowników ochrony lub policję.



(5)

BEZPIECZEŃSTWO POJAZDU

Ochrona pojazdów musi uwzględniać zapobieganie sabotażowi i kradzieży, a także przedostawaniu się niebezpiecznych przedmiotów i substancji.

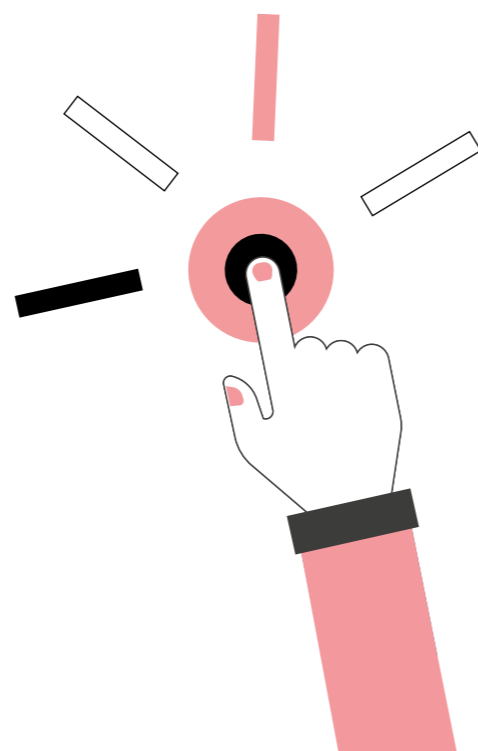
TECHNOLOGIA

- **Inteligentne blokady zapłonu** autobusu mogą stanowić dodatkową warstwę ochrony dzięki indywidualnym kluczom, które zapewniają, że tylko zaplanowany i przypisany kierowca ma dostęp do autobusu i może go uruchomić.
- Autobusy są często wyposażone w **przyciski alarmowe dla kierowców**, umożliwiające im bezpośrednie połączenie ze sterownią lub dyspozytorem. Często alarmy te są ciche i pozwalają dyspozytorowi na wsłuchanie się w sytuację w celu poprawy świadomości sytuacyjnej.
- **Systemy automatycznego monitorowania pojazdów (AVM)** są coraz powszechniejszą praktyką zarządzania i koordynowania flot autobusowych. Ciągła świadomość pozycji autobusów może pomóc w wykrywaniu odchyłeń i podejrzanych ruchów.
- **Geofencing** może służyć do monitorowania położenia i ruchu autobusów. Można go stosować do zapobiegania nieuprawnionemu usuwaniu autobusów z nieogrodzonych zajezdni lub miejsc parkingowych oraz ostrzegania w przypadku odchylenia autobusów od wyznaczonej trasy i wzorca obsługi.

Ochrona pojazdów musi uwzględniać zapobieganie sabotażowi i kradzieży, a także przedostawaniu się niebezpiecznych przedmiotów i substancji.

PERSONEL I PROCEDURY

- Dostęp do autobusów i kluczyków do autobusów można kontrolować za pomocą **procedury przekazywania kluczyków** wyłącznie zaplanowanym i przydzielonym kierowcom.
- Pewna forma kontroli dostępu może być realizowana poprzez kierowanie potokami pasażerów. Wielu operatorów wdrożyło zasadę **wsiadania do autobusów tylko przednimi drzwiami**, zobowiązując pasażerów do przejścia obok kierowcy i zakupu lub okazania biletu. W czasie ostatniej pandemii środek ten został jednak w wielu miejscach odwołany ze względów BHP.
- **Procedura wejścia na pokład** w przypadku usług autokarowych może pomóc zapewnić, że tylko pasażerowie z ważnym i spersonalizowanym biletom mogą wejść do autokaru.
- Przed załadowaniem jakiegokolwiek przedmiotu do przedziału bagażowego autokaru powinno odbyć się **uzgadnianie bagażu pasażera**.



(12)

(6)

BEZPIECZEŃSTWO ORGANIZACYJNE

KULTURA BEZPIECZEŃSTWA

Budowanie silnej kultury bezpieczeństwa w organizacji wymaga zaangażowania kierownictwa, świadomości pracowników i ciągłego szkolenia. Bezpieczeństwo nie może być zapewniane wyłącznie przez dział bezpieczeństwa, jest to odpowiedzialność korporacyjna, a każdy pracownik odgrywa w tym rolę.

Każda polityka i koncepcja bezpieczeństwa może być skuteczna tylko wtedy, gdy oczekiwania wobec wszystkich pracowników są jasne, odpowiednie kompetencje są określone, a kierownictwo wyższego szczebla daje przykład.

Pozytywna kultura bezpieczeństwa tworzy otwartą, opartą na zaufaniu atmosferę i zachęca pracowników do proaktywnego ograniczania ryzyka z korzyścią dla wszystkich.

ŚWIADOMOŚĆ

Kluczowym aspektem jest uznanie, że bezpieczeństwo to nie tylko zadanie kierowników i personelu ds. bezpieczeństwa, ale że każdy pracownik na każdym stanowisku ma do odegrania swoją rolę.

- **Programy informacyjne** pomagają przypominać pracownikom o ogólnych zasadach, rozpoznawać podejrzane sytuacje i procedury, których należy przestrzegać.
- **Ukierunkowane kampanie** mogą przyczynić się do utrzymania ogólnej świadomości bezpieczeństwa, a także odświeżenia znajomości zasad i procedur.
- **Materiały informacyjne i podręczniki** rozdawane pracownikom lub **plakaty** widoczne w miejscu pracy mogą być ważnymi odniesieniami, aby mieć pod ręką ważne kontakty lub procedury.

BEZPIECZEŃSTWO OSOBOWE

Bezpieczeństwo personelu odnosi się do ryzyka wykorzystywania przez pracowników ich legalnego dostępu do zasobów firmy do nieautoryzowanych celów. Podobnie jak każda organizacja, również przewoźnicy autobusowi mogą być zagrożeni przez osobę z wewnątrz.

Można temu przeciwdziałać poprzez staranny dobór zatrudnianego personelu, poprzez określenie jasnych procedur pracy i wprowadzenia dyscypliny w zakresie przestrzegania tych procedur oraz zachęcanie personelu do czujności na podejrzane zachowania.

- **Analiza krytyczności stanowisk pracowników** pomaga określić niezbędny dostęp (np. do pomieszczenia kontrolnego) i prawa użytkownika zasobów firmy (np. pojazdów) oraz opracować bardziej przejrzyste ramy kontroli przeszłości.
 - **Sprawdzanie przeszłości i weryfikacja** w ramach procesu rekrutacji to pierwszy krok do zapobiegania dołączaniu do firmy osób o złych zamiarach. Jasne kryteria dla kandydatów, sprawdzenie przeszłości i potencjalnie weryfikacja pomagają w momencie zatrudnienia, ale należy zauważyć, że taka kontrola stanowi jedynie migawkę przeszłości.
 - Przejrzyste i protokołowane **zarządzanie uprawnieniami**, w tym procedura wyjścia, pomaga zarządzać kluczami, hasłami, kodami dostępu itp., a także umożliwia anulowanie dostępu do zasobów, systemów i informacji, gdy pracownicy zmieniają stanowisko lub odchodzą z firmy.
 - **Szkolenie informujące o zagrożeniach wewnętrznych** może pomóc w zapoznaniu personelu z potencjalnymi szkodami, które mogą powstać w wyniku złych intencji, nieprzestrzegania przepisów lub wykorzystywania osobistych słabych punktów.
- Podczas zatrudnienia **kampanie informacyjne** mogą pomóc przypomnieć pracownikom o potencjalnych szkodach dla pasażerów, personelu i firmy, które mogą być spowodowane przez osoby mające dostęp do informacji poufnych.

(13)

INFORMACJA I CYBERBEZPIECZEŃSTWO

Cyfryzacja rewolucjonizuje sposób, w jaki świadczymy usługi i z nich korzystamy. Również w transporcie autobusowym wprowadzono innowacyjne narzędzia, dzięki którym procesy takie jak planowanie czy konserwacja są bardziej wydajne. Pomaga też w tworzeniu nowych kanałów i usług dla klientów. W związku z tym, oprócz fizycznych aktywów firmy, w planach i koncepcjach bezpieczeństwa należy uwzględnić również zasoby i procesy cyfrowe.

Bezpieczeństwo informacji koncentruje się na ochronie wrażliwych danych i informacji przed nieuprawnionym dostępem. Obejmuje między innymi informacje osobiste i finansowe dotyczące personelu lub klientów, informacje korporacyjne lub informacje dotyczące procesów biznesowych, takie jak listy pracowników lub harmonogramy konserwacji. Naruszenie bezpieczeństwa informacji może prowadzić do szkód ekonomicznych i wizerunkowych.

- Wrażliwe informacje powinny być przechowywane pod kluczem, a najlepiej przechowywane i przetwarzane wyłącznie w obiektach o ograniczonym dostępie.
- Prawa dostępu powinny być przyznawane wyłącznie odpowiednim członkom personelu. Poświadczenia i hasła muszą być regularnie odnawiane.

Cyberbezpieczeństwo koncentruje się na integralności systemów informatycznych i komputerowych. Atak cybernetyczny może zakłócić codzienne czynności operacyjne i może zagrozić systemom bezpieczeństwa, potencjalnie zagrażając życiu personelu i pasażerów. Należy zauważyć, że również cyberbezpieczeństwo jest wyzwaniem korporacyjnym, które powinno być częścią kultury bezpieczeństwa przedsiębiorstwa. Nie należy go zostawiać samemu działowi IT.

- Tam, gdzie to możliwe, również zasoby cyfrowe powinny być fizycznie chronione przed nieautoryzowanym dostępem do zamków, uszczeltek, pokryw i instalowania ich w obiektach o ograniczonym dostępie.
- Fizyczny dostęp powinien być przyznawany wyłącznie odpowiednim członkom personelu.
- Poziomy haseł i wymagania dotyczące ich odnawiania należy zdefiniować we współpracy z działem IT.
- Należy zapewnić integralność systemu poprzez prawidłową konfigurację, ciągłe zarządzanie i łatanie systemów oprogramowania zgodnie z zaleceniami dostawcy. Konserwacja systemu i zarządzanie częściami zamiennymi muszą zapewniać integralność systemu.
- Systemy powinny być stale monitorowane pod kątem anomalii. Szczególnym wyzwaniem w kontekście cyberbezpieczeństwa jest to, że systemy mogą zostać naruszone i nie zostanie to wykryte.

Wraz z wdrażaniem nowych technologii w operacjach autobusowych, takich jak autobusy elektryczne lub stacje ładowania, należy również wziąć pod uwagę nowe zagrożenia dla bezpieczeństwa cybernetycznego. Systemy dostarczane jako zmontowane jednostki mogą zawierać komponenty zaplombowane przez dostawcę. Ocena ryzyka potencjalnie stwarzanego przez nieprawidłowo działające lub naruszone elementy systemu jest wyzwaniem, które należy rozwiązać w przyszłych ocenach ryzyka.

BEZPIECZEŃSTWO STRON TRZECICH

Zarządzanie ryzykiem bezpieczeństwa nie może ograniczać się do wnętrza organizacji. Partnerzy biznesowi mogą współdzielić aktywa, dostawcy i usługodawcy mogą mieć tymczasowy lub stały dostęp do obiektów i systemów firmy, podwykonawcy mogą nadzorować procesy biznesowe (np. role konserwacyjne lub administracyjne).

Kluczowe znaczenie ma włączenie zasad bezpieczeństwa stron trzecich do procesu selekcji oraz posiadanie jasnych umów, zasad i polityk monitorowania.



(7)

SZKOLENIE W ZAKRESIE BEZPIECZEŃSTWA

Bezpieczeństwo w ruchu autobusowym jest obowiązkiem wszystkich pracowników. Programy szkoleniowe muszą wyjaśniać rolę i odpowiedzialność personelu na każdym stanowisku oraz zapewniać pracownikom wiedzę niezbędną do wykonywania ich pracy.

Wstępne szkolenia w zakresie bezpieczeństwa operacyjnego powinny zapewniać ogólne umiejętności i wiedzę oczekiwaną na każdym stanowisku. Cykliczne programy szkoleniowe w tym zakresie można wykorzystać do odświeżenia określonego know-how.

POTRZEBY W ZAKRESIE SZKOLENIA

Personel powinien przejść szkolenie z zakresu bezpieczeństwa operacyjnego, aby upewnić się, że jest świadomy swojej odpowiedzialności za bezpieczeństwo i jak odpowiednio zareagować na atak.

- Odpowiedzialność **personelu operacyjnego i pierwszej linii** zazwyczaj obejmuje czujność i zgłaszanie podejrzanych sytuacji, rozwiązywanie konfliktów i deeskalację, a w razie potrzeby reagowanie na incydenty.
- **Pracownicy w miejscach o ograniczonym dostępie**, takich jak pomieszczenia kontrolne lub zajezdnie, muszą być świadomi zasad dostępu do miejsca pracy oraz, w stosownych przypadkach, muszą móc rejestrować odwiedzających i wydawać identyfikatory.
- **Personel dyspozytorski** skupia się na obsłudze połączeń alarmowych lub przychodzących zagrożeń oraz potencjalnej aktywacji protokołów bezpieczeństwa.

DOKUMENTACJA SZKOLEŃ

Aby mieć wgląd w przeprowadzone szkolenia z zakresu bezpieczeństwa i zaplanować potrzebne kursy przypominające, zaleca się prowadzenie dokumentacji szkoleniowej dla całego personelu, w szczególności:

- termin i treść odbycia szkolenia wstępnego;
- tematyka szkoleń i terminy sesji kursów utrwalających wiedzę;
- nabyte umiejętności specjalistyczne podczas szkolenia

Zaleca się również posiadanie dokumentacji szkoleniowej podpisanej przez uczestników, potwierdzającej odbycie szkolenia.

ĆWICZENIA

Regularne ćwiczenia z zakresu bezpieczeństwa pomagają monitorować poziom gotowości w organizacji i zrozumieć niedociągnięcia i luki w zabezpieczeniach.

- **Wewnętrzne ćwiczenia** można wykorzystać do symulowania reakcji na określone incydenty i ćwiczenia zdolności organizacji do zarządzania kryzysowego.
- **Ćwiczenia wewnętrzne z partnerami zewnętrznymi** mogą pomóc w dostosowaniu planów, procedur i odpowiedzialności.
- **Ćwiczenia na żywo** powinny również angażować wszystkich odpowiednich partnerów zewnętrznych. Mają również kluczowe znaczenie dla zapewnienia, że osoby udzielające pierwszej pomocy są zaznajomione z układem infrastruktury, taborem kolejowym i przepisami bezpieczeństwa dotyczącymi eksploatacji autobusów.

Bezpieczeństwo w ruchu autobusowym jest obowiązkiem wszystkich pracowników.

(8)

ZARZĄDZANIE W SYTUACJI KRYZYSOWEJ

ZARZĄDZANIE KRYZYSOWE

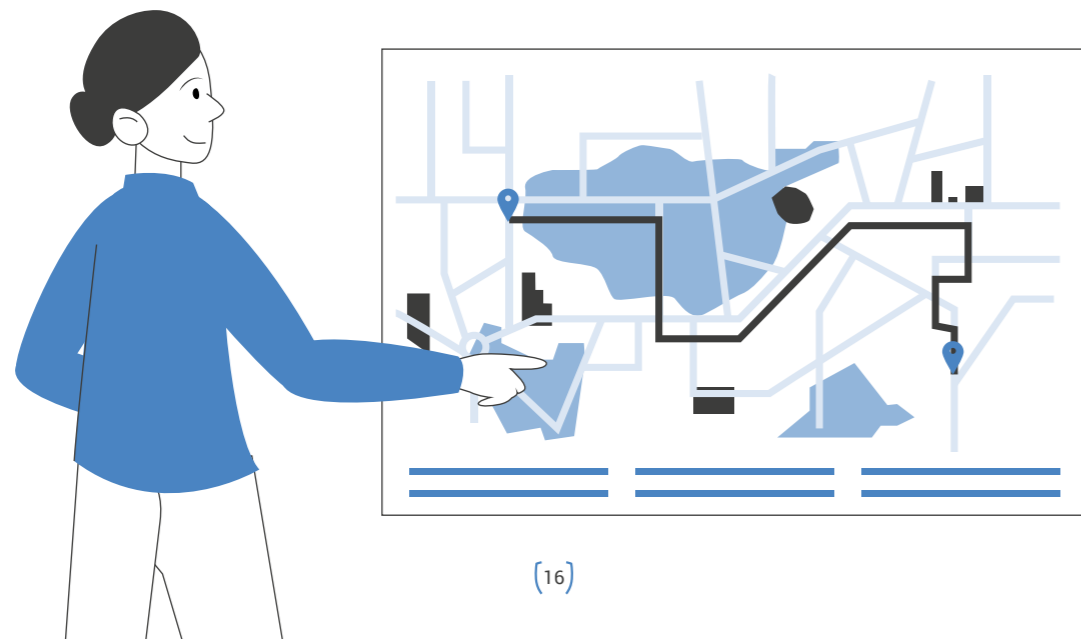
Biorąc pod uwagę złożoność systemów transportowych i elastyczność operacji autobusowych, zarządzanie kryzysowe obejmuje radzenie sobie z samym kryzysem, ale także zarządzanie wpływem kryzysu w jednym miejscu na resztę operacji. Konieczność radzenia sobie z kryzysem nie oznacza automatycznego zamknięcia całej operacji, ponieważ zbyt wiele zależy od dostępności. **Komórka kryzysowa** powinna zostać formalnie utworzona. Powinna ona angażować wszystkie działy organizacji i umożliwiać aktywację z minimalnym opóźnieniem w celu przejęcia odpowiedzialności za zarządzanie kryzysowe.

- **Plan zarządzania kryzysowego** wyjaśnia role i obowiązki wszystkich działów w ramach zarządzania kryzysowego i zarządzania w trybach awaryjnych, obejmujących przekierowane linie autobusowe i ograniczenie usługi.
- Należy przygotować **plan komunikacji kryzysowej**, który pomoże poradzić sobie z uwagą mediów po każdym incydencie.

CIĄGŁOŚĆ DZIAŁANIA

Oprócz radzenia sobie z rzeczywistym incydem, zarządzanie kryzysowe musi również uwzględniać aspekty ciągłości działania – dostosowywanie i zmianę trasy usług tam, gdzie to możliwe oraz informowanie pasażerów o dostępnych zmianach. Planowanie ciągłości działania powinno obejmować:

- Należy zidentyfikować **obiekty zapasowe** dla krytycznych funkcji (parkowanie lub konserwacja pojazdów, tymczasowe przystanki autobusowe lub obiekty obsługi klienta), które można wykorzystywać do kontynuowania operacji w przypadku, gdy standardowe obiekty przestaną działać lub nie będą dostępne.
- Należy określić **alternatywne trasy** lub okrojona sieć autobusową, aby reagować na zakłócenia i incydenty na trasie lub częściową niedostępność floty autobusowej.
- Określenie **zastępczych usług autobusowych** może również pomóc w obsłudze mniej elastycznych środków transportu, takich jak kolej lub metro, w przypadku zdarzeń lub poważnych zakłóceń w sieci mobilności.



(16)

(9)

PORADY SZKOLENIOWE

WPROWADZENIE

Niniejszy rozdział skupia się na podstawowym szkoleniu z zakresu bezpieczeństwa dla personelu operacyjnego transportu publicznego. Lekcja ma na celu poprawę ogólnej świadomości bezpieczeństwa, wyjaśnienie roli i odpowiedzialności personelu, zachęcenie do wniesienia wkładu i dodanie pewności siebie w celu podjęcia właściwych działań. Określa umiejętności i kompetencje, które są potrzebne do:

- Przyczyniania się do zapewnienia, że pomieszczenia i obszary transportu publicznego są kontrolowane i zarządzane;
- Rozpoznawania podejrzanych sytuacji i znajomości procedur, jak je zgłaszać;
- Reagowania na sytuacje awaryjne, ochrony pasażerów bez narażania własnego bezpieczeństwa.

Te wytyczne szkoleniowe opracowano w oparciu o szereg podstawowych scenariuszy, w których pracownicy operacyjni najprawdopodobniej będą pierwszymi osobami, z którymi się zetkną i będą musieli interweniować. Są one dostosowane do Rezultatu 4.1 „Podręcznik kierowcy dotyczący bezpieczeństwa w transporcie publicznym”, który może być rozdawany pracownikom jako punkt odniesienia.

Te wytyczne szkoleniowe opracowano w oparciu o szereg podstawowych scenariuszy.



(17)

TREŚĆ SZKOLENIA

ANTYTERRORYZM

Część wprowadzająca szkolenia powinna wyjaśniać, czym jest terrorizm i dlaczego jest to ważny temat dla operatorów transportu publicznego.

Terroryzm oznacza użycie przemocy lub innych czynów przestępczych jako uzasadnionych środków do osiągnięcia celów politycznych. Celem jest zastraszenie ludzi, osłabienie społeczności lub destabilizacja gospodarek. Niestety, systemy transportu publicznego wielokrotnie były celem działań terrorystycznych, mających na celu zakłócenie funkcjonowania i sabotowanie usług mobilności.

Potencjalnymi celami działań terrorystycznych mogą być nasze pojazdy i infrastruktura, takie jak dworce, magazyny i warsztaty, centra obsługi klienta lub budynki administracyjne. Celem może być również wyrażenie szkody osobom korzystającym z transportu publicznego.

Jako dostawcy usług jesteśmy odpowiedzialni za bezpieczeństwo i dobre samopoczucie naszych pasażerów. Obejmuje to monitorowanie podejrzanych sytuacji i działań, a także umiejętność radzenia sobie z sytuacjami awaryjnymi i zagrożeniami.

Odniesienie 1 – Podręcznik kierowcy „Antyterroryzm”



ZAPOBIEGANIE

Ta sekcja zawiera informacje na temat tego, w jaki sposób podstawowe „porządki” mogą przyczynić się do uniknięcia nieautoryzowanego dostępu do obiektów i zasobów transportu publicznego o ograniczonym dostępie oraz jak monitorować nietypowe sytuacje.

Ważne jest, aby przypomnieć uczestnikom, że wymagana uwaga nie jest niczym dodatkowym w stosunku do ich roli zawodowej i że nie oczekuje się od nich działania poza zasadami i procedurami organizacyjnymi.

Kluczowym środkiem ochrony jest unikanie nieuprawnionego dostępu do obiektów o ograniczonym dostępie. Obejmuje to zajezdnie, warsztaty, szatnie i budynki administracyjne, ale dotyczy również stanowiska kierowcy pojazdów.

- Jeśli widzisz **nieznaną osobę** w magazynie lub na miejscu, sprawdź kim ona jest i zaoferuj pomoc.
- **Upewnij się, że drzwi są zamknięte** za każdym razem, gdy pozostawiasz pojazd bez nadzoru.

Obiekty publiczne, takie jak dworce, przystanki autobusowe lub centra obsługi klienta, mają ograniczoną kontrolę dostępu. Tutaj ważne jest, aby uważać na nietypowe zachowania lub sytuacje.

- **Zachowaj czujność wobec** osób zachowujących się podejrzanie i nerwowo w autobusach, na dworcach lub przystankach.
- **Regularnie sprawdzaj swój pojazd** pod kątem podejrzanych przedmiotów i zagubionego mienia za każdym razem, gdy opuszczasz zajadnię, tak często, jak to możliwe między podróżami i za każdym razem, gdy wracasz do zajadni.

Odniesienie 2 – Podręcznik kierowcy – „Zapobieganie”



(18)

PODEJRZANE SYTUACJE

Celem sekcji jest umożliwienie uczestnikom rozpoznawania podejrzanych sytuacji i zachęcenie ich do zgłaszania takich sytuacji. Ważne jest, aby przypomnieć uczestnikom, że nie powinni podejmować ryzyka, a ich bezpieczeństwo jest priorytetem. Podstawowe scenariusze wybrane do tego szkolenia są omówione w dwóch częściach:

- Jak rozpoznać tę sytuację jako podejrzaną?
- Co zrobić, jeśli istnieje powód do niepokoju?

Sugerowane poniżej procedury reagowania mają charakter ogólny i mają na celu zapewnienie ogólnych wytycznych. Mogą one zostać zmienione w celu dostosowania do istniejących zasad firmy.

Wybrano następujące sytuacje:

WROGI REKONESANS

Krytycznym krokiem w przygotowaniu jakiegokolwiek działalności przestępczej jest wrogi rekonesans.

Rozpoznanie wroga oznacza zebranie informacji o naszych obiektach i działaniach, które mogłyby zostać wykorzystane w ataku. Informacje krytyczne mogą być gromadzone poprzez obserwację lub bezpośrednie kontaktowanie się z personelem w celu uzyskania informacji.

Wskaźniki rozpoznania wrogiego obejmują:

- Wykonywanie zdjęć lub nagrań wideo dworców lub innych obiektów firmy;
- Cykliczna lub nietypowo przedłużająca się obecność na dworcach osób, które nie korzystają z autobusów;
- Próba wejścia do obiektów o ograniczonym dostępie lub omińnięcia środków bezpieczeństwa, takich jak bramy i ogrodzenia;
- Zadawanie nieodpowiednich lub nietypowych pytań dotyczących środków bezpieczeństwa lub procedur operacyjnych.

Jeśli zaobserwujesz zachowanie niezgodne z codziennymi czynnościami pasażerów, postępuj zgodnie z poniższymi instrukcjami:

Zaoferuj pomoc	Jeżeli czujesz się bezpiecznie, podejdz do osoby i zaoferuj pomoc.
Poinformuj dyspozytora	Podaj szczegóły incydentu lub zgłoszenia, które mają zostać zarejestrowane.

Odniesienie 3 – Podręcznik kierowcy „Wrogi rekonesans”

PODEJRZANE PRZEDMIOTY

Pasażerowie często zostawiają bagaż lub przedmioty. Jednak porzucone przedmioty mogą się tam znajdować celowo i zawierać niebezpieczne substancje, takie jak materiały wybuchowe lub chemikalia.

Porzucone przedmioty powinny być zbierane i przekazywane do działu rzeczy znalezionych tylko wtedy, gdy nie ma powodu do niepokoju. Protokół bezdotykowy pomaga identyfikować podejrzane przedmioty.

Przedmiot podejrzany to porzucony przedmiot, który ma jedną z następujących cech:

Nietypowy dla otoczenia (prawdopodobnie nie jest to utracone mienie)

Przedmiot ma podejrzane cechy (jest mokry lub brudny, ma dziwny zapach, jest zamknięty liną lub taśmą)

Okoliczności sugerują zaniepokojenie (pozostawienie w ruchliwym miejscu, pokryte proszkiem, z widocznym kablem lub folią aluminiową)

Celowo ukryte (bez powodu, umieszczone w nietypowym miejscu – pod siedzeniem lub obok kosza na śmieci)

Jeśli znajdziesz przedmiot, który daje powód do niepokoju, postępuj zgodnie z poniższymi instrukcjami:

- ✓ Wypatruj podejrzanych znaków z dużej odległości!
- ✓ Powiadom OCC i podaj odpowiednie szczegóły dotyczące przedmiotu! (Dokładna lokalizacja, kształt, rozmiar itp.)
- ✓ Spróbuj zlokalizować właściciela!
- ✓ Ostrzeż ludzi w pobliżu i poinstruuj ich, aby się odsunęli!
- ✓ Do czasu przybycia pracowników ochrony obserwuj przedmiot z pewnej odległości!
- ✗ **Nie** dotykaj, potrząsaj ani otwieraj przedmiotu!
- ✗ **Nie** używaj urządzenia komunikacyjnego ani telefonu komórkowego w pobliżu podejrzanego przedmiotu!
- ✗ **Nie** pal w pobliżu przedmiotu!
- ✗ **Nie** wywołuj paniki wśród osób obecnych na miejscu zdarzenia!
- ✗ **Nie** używaj metalowych przedmiotów w pobliżu!

Odniesienie 4 – Podręcznik kierowcy „Podejrzone przedmioty”

(19)

PODEJRZANE ZACHOWANIE PASAŻERÓW

Podejrzone oznaki mogą wynikać z wyglądu lub zachowania pasażera i obejmują wskaźniki, takie jak:

- Odzież nieodpowiednia do miejsca, czasu i warunków lokalnych;
- Bagaż niezgodny z ogólnym wyglądem;
- Bagaż, który jest nieproporcjonalnie ciężki;
- Nerwowość lub strach;
- Ukryty kontakt z innymi pasażerami;
- Odmowa współpracy z personelem;
- Nieuzasadniona obecność lub wałęsanie się.

Jeśli zachowanie pasażera daje powód do niepokoju, postępuj zgodnie z poniższymi instrukcjami:

Zatrzymaj pojazd! *Zatrzymaj się w bezpiecznym miejscu, wyłącz silnik i zachowaj spokój. Poinformuj pasażerów sugerując usterkę pojazdu.*

Skontaktuj się z dyspozytorem! *Zgłoś swoje obawy i opisz sytuację.*

Ewakuuj pojazd! *Ewakuuj siebie i pasażerów na bezpieczną odległość!*

Monitoruj pasażera *Jeśli to możliwe, obserwuj podejrzanego pasażera z bezpiecznej odległości!*

Poczekaj na pomoc *Pozostań, dopóki osoba odpowiedzialna nie potwierdzi, że możesz odejść.*

Uczestnikom należy wyjaśnić, w jaki sposób raporty będą weryfikowane i przetwarzane. Ważne jest, aby wyjaśnić, dlaczego nie może dojść do widocznych działań następczych (weryfikacja za pomocą kamer CCTV, planowane prace naprawcze itp.). Ważne jest również uwzględnienie w szkoleniu sposobu rozpoznawania i bycia świadomym swoich uprzedzeń podczas oceny potencjalnych zagrożeń.

Powiązane szkolenia dla członków personelu przetwarzających zgłoszenia o podejrzanym zachowaniu pasażerów powinny zawsze obejmować uznanie poświęconej uwagi i przedłożone zgłoszenie, aby zachęcić ludzi do pozostania uważnymi i współpracy.

SYTUACJE WYJĄTKOWE

Ostatnia sekcja zawiera instrukcje dotyczące reagowania na sytuacje awaryjne, głównie dla pracowników mających kontakt z klientem. Ponownie, ważne jest, aby przypomnieć uczestnikom, że nie powinni podejmować ryzyka, a ich bezpieczeństwo jest priorytetem. Zaleca się, aby wszelkie instrukcje po wygenerowaniu alarmu opierały się na zasadzie „Run-Hide-Report”.

- **NACIŚNIJ ALARM** – jeśli to możliwe, powiadom dyspozytora, aby był świadomy sytuacji awaryjnej i zainicjował odpowiednią reakcję.
- **UCIEKAJ** – uciekaj przed niebezpieczeństwem tak szybko, jak to możliwe.
- **UKRYJ SIĘ** – pozostań poza zasięgiem wzroku.
- **ZGŁOŚ** – zadzwoń do dyspozytora, podając więcej szczegółów, gdy tylko będzie to bezpieczne.

Sugerowane poniżej procedury reagowania mają charakter ogólny i mają na celu zapewnienie ogólnych wytycznych. Mogą one zostać zmienione w celu dostosowania do istniejących zasad firmy.

Wybrano następujące scenariusze:

ATAK NA POKŁADZIE

W przypadku bezpośredniego zagrożenia dla siebie i/lub życia i zdrowia pasażera należy postępować zgodnie z poniższymi instrukcjami:

Naciśnij alarm! *Naciśnij przycisk alarmu*

Otwórz drzwi! *Zatrzymaj pojazd, aby umożliwić pasażerom ucieczkę. Poinstruuj ich, aby wyszli, jeśli to możliwe.*

Uciekaj i ukryj się! *Uciekaj przed niebezpieczeństwem i wycisz telefon.*

Zgłoś szczegóły! *Po ukryciu zadzwoń do dyspozytora, aby uzyskać więcej informacji*

ATAK POZA POJAZDEM

Jeśli zauważysz atak na przystanku lub dworcu, lub Twój pojazd jest atakowany z zewnątrz, postępuj zgodnie z poniższymi instrukcjami:

Naciśnij alarm! *Naciśnij przycisk alarmu.*

Nie zatrzymuj się! *Jedź dalej i nie zatrzymuj się (jeśli to możliwe)! Poinformuj pasażerów.*

Zadzwoń do dyspozytora! *Podaj więcej szczegółów tak szybko, jak to możliwe*

UPROWADZENIE I WZIĘCIE ZAKŁADNIKÓW

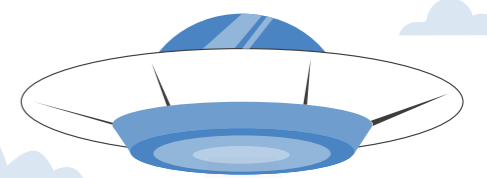
W przypadku napadu, który zagraża życiu lub zdrowiu pasażera lub wzięcia zakładnika, należy postępować zgodnie z poniższymi instrukcjami:

Naciśnij alarm *Naciśnij przycisk alarmu jeśli to możliwe.*

Zachowaj spokój *Nie stawiaj oporu, nie kłóć się, wykonuj polecenia sprawcy.*

Unikaj uwagi *Unikaj zwracania na siebie uwagi, unikaj kontaktu wzrokowego, nie wykonuj gwałtownych ruchów.*

Zawsze pamiętaj, że Twoje bezpieczeństwo jest priorytetem.



NOTATKI



(SAFEBUS)