ZAGROŻENIA DLA CYBERBEZPIECZEŃSTWA W TRANSPORCIE MIEJSKIM[1]

KARINA WCISŁO
inż., studentka Politechniki Krakowskiej, Wydział Informatyki i Telekomunikacji, 31-155 Kraków, ul. Warszawska 24, e-mail: karina.wcislo@student.pk.edu.pl
JAN ALEKSANDROWICZ
dr inż., Politechnika Krakowska, Wydział Inżynierii Lądowej, 31-155 Kraków, ul. Warszawska 24, e-mail: jan.aleksandrowicz@pk.edu.pl

Streszczenie: Artykuł poświęcono problemowi cyberbezpieczeństwa w transporcie miejskim. Omówione zostały zagrożenia, jakie związane są z udostępnianiem i przesyłaniem informacji w sieci internetowej na temat elementów systemu transportowego. W artykule przedstawiono elementy miejskiego systemu transportowego najbardziej narażone na ataki cybernetyczne oraz podjęto się próby przedstawienia sposobów przeciwdziałania im. Analizę zagrożeń cybernetycznych w artykule przeprowadzono dla: systemów informacji pasażerskiej, planerów podróży, systemów nawigacji drogowej, systemów sterowania ruchem drogowym, automatycznych systemów zliczania pasażerów oraz systemów opłat parkingowych i sprzedaży biletów. W artykule opisane zostały skutki udanych ataków oraz przykłady tego typu działań, które miały już miejsce na terenie Polski. Artykuł zakończono podsumowaniem i wnioskami będącymi wstępem do dalszych prac nad opracowaniem standardów mających na celu przeciwdziałanie zagrożeniom cybernetycznym w transporcie miejskim.
Słowa kluczowe: cyberbezpieczeństwo, transport miejski, zagrożenia cybernetyczne.

Wprowadzenie

Zaawansowane technologie informatyczne w dużym stopniu przyczyniły się do dynamicznego rozwoju transportu w miastach. Największą zmianę można zauważyć w systemach informatycznych, które rozpoczęły pracę w sieci internetowej. Powszechny dostęp do systemów informatycznych transportu istotnie skrócił czas wymiany informacji i ułatwił przemieszczanie się. Niestety, wraz z dynamicznym rozwojem, systemy informatyczne transportu stały się celem ataków cybernetycznych, których zadaniem jest manipulacja lub kradzież danych. Technologie informatyczne w transporcie są obecnie wykorzystywane we wszystkich obszarach transportu, zapewniając wymianę informacji w czasie rzeczywistym pomiędzy wszystkimi jego elementami. W celu ochrony danych wrażliwych przed nieuprawnionym dostępem i ich manipulowaniem coraz większą rolę odgrywa cyberbezpieczeństwo.

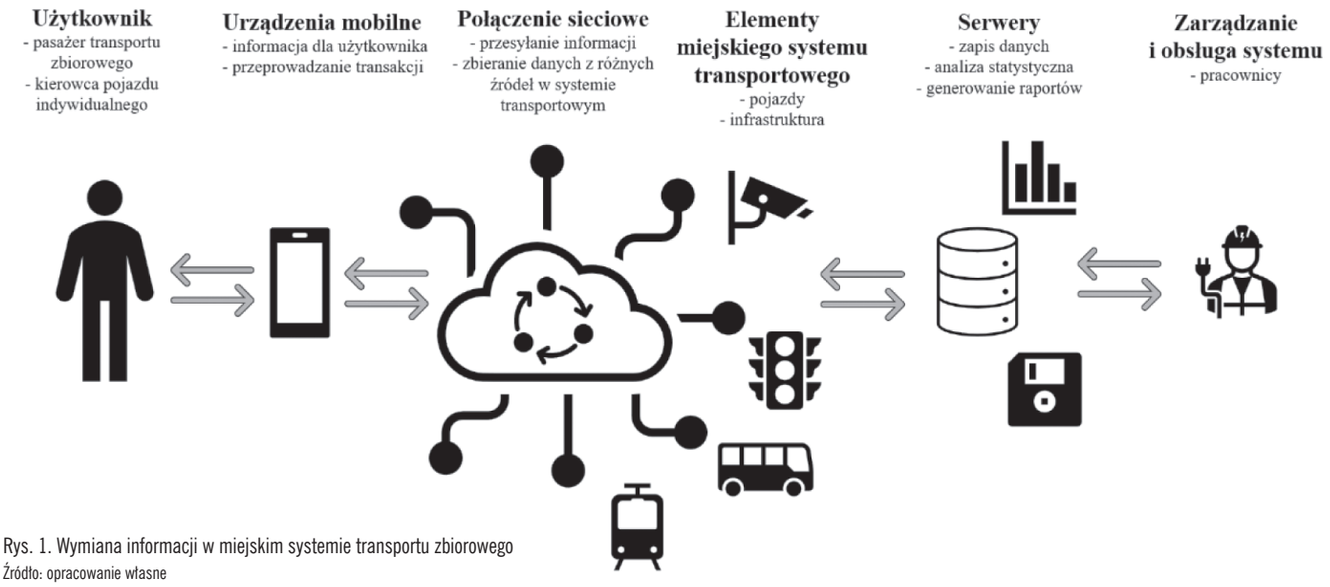
Cyberbezpieczeństwo to działania podejmowane w celu ochrony urządzeń, programów i baz danych przed atakami mającymi na celu uszkodzenie elementów sieci informatycznej lub kradzieży danych. W transporcie cyberbezpieczeństwem można nazywać odporność wykorzystywanych systemów informatycznych na nieautoryzowany dostęp oraz ataki sieciowe. Zadaniem cyberbezpieczeństwa jest zapewnienie ochrony podczas zapisu i przesyłania informacji między elementami systemów informatycznych [5, 6, 7, 8, 9, 10, 11].

Rozwój technologii pozyskiwania danych umożliwił zbieranie danych i ich wykorzystanie w czasie rzeczywistym w procesie zarządzania i nadzoru nad transportem w miastach. Zbierane masowo dane narażone są na różnego rodzaju zagrożenia cybernetyczne. Do elementów miejskiego systemu transportowego, najbardziej narażonych na manipulację danymi, należy zaliczyć [7]:

- informację pasażerską w pojazdach i na przystankach oraz planery podróży,
- systemy nawigacji drogowej,
- systemy sterowania ruchem drogowym i sygnalizacją świetlną,
- automatyczne systemy zliczania pasażerów,
- systemy opłat parkingowych i sprzedaży biletów.

Wymiana informacji w miejskim systemie transportowym realizowana jest pomiędzy wszystkimi elementami z wykorzystaniem różnego rodzaju połączeń. Systemy, w których wprowadzono pełną integrację podsystemów, funkcjonują z wykorzystaniem sieci bezprzewodowej (w połączeniach z ruchomymi elementami systemu) oraz przewodowej (pomiędzy nieruchomymi elementami systemu). Informacja przesyłana jest jedno- lub dwukierunkowo. Przykładem połączenia jednokierunkowego jest przesyłanie informacji na temat natężenia ruchu drogowego z detektorów ruchu. Połączeniem dwukierunkowym jest między innymi system sprzedaży biletów, w których użytkownik przesyła do systemu informacje związane z podróżą i płatnością, a system potwierdza odbiór środków finansowych oraz generuje zakupiony bilet. Zintegrowane systemy transportu miejskiego są ze sobą połączone, a informacja jest płynnie przekazywana pomiędzy wszystkimi jego elementami. Na rysunku 1 przedstawiono w sposób schematyczny połączenie informacyjne pomiędzy elementami systemu. Każdy z przedstawionych na schemacie elementów narażony jest na ataki cybernetyczne i nieautoryzowany dostęp. Począwszy od użytkownika, który może zostać wprowadzony w błąd lub zmanipulowany w celu pozyskania danych wrażliwych, po pracowników, których zadaniem jest nadzór, zarządzanie i obsługa systemu. Nieautoryzowany dostęp do danych może spowodować kradzież danych, ich zmianę lub usunięcie zapisanych informacji. Efekty ataków cybernetycznych dla użytkowników miejskiego systemu transportowego mogą być różnej skali i zależą od celu, w jakim został przeprowadzony atak. Przykładem efektów działań o małym zakresie może być utrudniony dostęp do informacji pasażerskiej lub błędne jej prezentowanie. Efektami dużych ataków mogą być: kradzież środków finansowych, awaria systemów elektronicznych, a na-

[1] ©Transport Miejski i Regionalny, 2023. Wkład autorów w publikację: K. Wcisło 50%, J. Aleksandrowicz 50%.



Rys. 1. Wymiana informacji w miejskim systemie transportu zbiorowego
Źródło: opracowanie własne

wet zwiększenie ryzyka wypadków drogowych (np. poprzez atak na systemy sterowania ruchem drogowym).

W artykule skupiono się na przedstawieniu zagrożeń cybernetycznych, na jakie narażone są wybrane elementy miejskiego systemu transportowego. Dla każdego z nich podjęto próby wskazania sposobów przeciwdziałania zagrożeniom oraz przedstawienia przyczyn zagrożenia cybernetycznego.

Informacja pasażerska i planery podróży

Wraz z wprowadzaniem do ruchu nowoczesnych pojazdów oraz modernizacją infrastruktury dla miejskiego transportu zbiorowego wiele miast zyskało dostęp do rozbudowanej informacji pasażerskiej opierającej się na tablicach zmiennej treści. Tekturowe lub blaszane tablice z informacją o numerze linii, pętli końcowej oraz przystankach pośrednich na początku trzeciej dekady dwudziestego pierwszego wieku stały się symbolem przeszłości w transporcie zbiorowym. Obecnie tego typu informacje są wyświetlane na ekranach led lub monitorach wewnątrz pojazdów. W przypadku informacji pasażerskiej na przystankach transportu publicznego coraz częściej stosowane są ledowe wyświetlacze informujące pasażerów o kolejnych kursach linii zatrzymujących się na przystanku. Papierowe rozkłady jazdy często pełnią funkcję awaryjną, a niektórzy organizatorzy transportu rozpoczęli wprowadzanie e-papieru, jako sposobu prezentowania rozkładów jazdy na przystankach (rozwiązanie to wdrożyły między innymi władze województwa małopolskiego w 2023 roku w Wieliczce). Dzięki zastosowaniu nowoczesnych systemów informacji pasażerskiej na przystankach pasażerowie znają dokładny czas odjazdu kolejnych kursów linii autobusowych i tramwajowych, ewentualny czas opóźnienia poszczególnych kursów oraz poznają informacje na temat awarii w systemie transportowym miasta.

Źródłem informacji pasażerskiej przekazywanej w formie wizualnej są bazy danych, w których przewoźnicy gromadzą dane między innymi na temat aktualnych tras i rozkładów jazdy, lokalizacji poszczególnych pojazdów w sieci, liczbie pasażerów w pojazdach. Dane te gromadzone są w sposób ciągły, a te, przekazywane pasażerom, są na bieżąco aktualizowane. Dzięki temu informacje podawane w formie wizualnej ułatwiają pasażerom szybkie podejmowanie decyzji na temat wyboru środka transportu.

Rozwój urządzeń mobilnych oraz szeroki dostęp do bezprzewodowego połączenia z internetem spowodowały rozwój aplikacji i programów umożliwiających dostęp do informacji pasażerskiej na tej samej zasadzie, jak z wykorzystaniem tablic led i ekranów w pojazdach. Aplikacje tego typu nie tylko informują pasażera o aktualnych rozkładach jazdy, ale także umożliwiają zweryfikowanie punktualności poszczególnych kursów, zakup biletu i zaplanowanie poszczególnych etapów podróży, pełniąc funkcję planera podróży. Aby wykorzystać pełne możliwości aplikacji mobilnych do planowania podróży, pasażer jest zmuszony do utrzymywania stałej łączności z internetem. Często, aby uzyskać szybciej informacje na temat dostępnych połączeń transportem miejskim, pasażer musi udostępnić swoją lokalizację. Korzyści płynące z aplikacji mobilnych oferujących dostęp do informacji pasażerskiej są duże, ale mogą stać się także celem ataków cybernetycznych.

Dane zbierane w systemie transportowym gromadzone są na serwerach podmiotów odpowiedzialnych za ich gromadzenie. Często podmiotami tymi są przewoźnicy transportu publicznego. Aby umożliwić wykorzystanie danych w czasie rzeczywistym w sieci i w aplikacjach mobilnych, niezbędne jest udostępnianie danych w internecie. Dostęp do danych w sieci może także nieść ze sobą pewne zagrożenie związane z atakami cybernetycznymi. Do przyczyn zagrożenia cybernetycznego zaliczamy:

- włamanie fizyczne do pomieszczenia serwerowni,
- nieświadome błędy i pomyłki operatora baz danych,
- awarie instalacji (m.in. elektrycznej lub wodnej) wewnątrz pomieszczenia serwerowni,
- świadome działanie wewnętrzne osób odpowiedzialnych za dane na serwerach,
- kradzież sprzętu umożliwiającego zdalny dostęp administracyjny do serwerów,
- zdalny atak na serwery baz danych i kradzież danych osobowych.

Wymienione przyczyny nie są jednoznaczne z atakiem cybernetycznym, ale w dużym stopniu ułatwiają jego przeprowadzenie.

Celem ataków cybernetycznych na systemy informacji pasażerskiej może być kradzież danych, ich usunięcie oraz manipulacja danymi na serwerach. Tego typu działanie może mieć na celu wprowadzenie pasażerów w błąd poprzez: złe wyznaczenie czasu lub trasy przejazdu, błędną informację na temat lokalizacji poszczególnych przystanków, ich nazw oraz zatrzymujących się linii transportu publicznego. Celem może być również atak na serwer, aby całkowicie uniemożliwić świadczenie usług – w tym przypadku uniemożliwienie działania aplikacji przekazującej informacje pasażerom. Taki rodzaj zagrożenia to atak typu DOS (Denial of Service) polegający na zalewaniu serwera nadmiarową liczbą połączeń w celu jego przeciążenia i w efekcie odmowie działania. W przypadku integracji w ramach jednego systemu wszystkich elementów informacji pasażerskiej w danym obszarze za pomocą ataku cybernetycznego możliwe jest błędne nadawanie komunikatów na tablicach zmiennej treści, komunikatów głosowych, a nawet informacji na temat numeru linii i kierunku, w którym realizowany jest kurs w poszczególnych pojazdach.

Aby przeciwdziałać tego typu atakom, w ramach systemu informacji pasażerskiej i planerów podróży niezbędne jest wprowadzanie standardów zabezpieczeń danych – zarówno sieciowych, jak i fizycznych. Niezbędne jest przeszkolenie pracowników odpowiedzialnych za administrowanie danymi na serwerach o możliwych do zastosowania zabezpieczeniach, sposobie formułowania haseł dostępu, szyfrowania danych oraz zabezpieczeniach na wypadek włamania lub kradzieży. Niezbędne jest też ciągłe monitorowanie i weryfikowanie informacji gromadzonych i prezentowanych w planerach podróży, co zabezpieczy użytkowników transportu miejskiego przed błędnymi danymi z winy aplikacji mobilnych, które także mogą być celem ataków cybernetycznych.

Systemy nawigacji drogowej

Systemy nawigacji drogowej, takie jak GPS, są obecnie podstawowym wyposażeniem większości nowych urządzeń mobilnych i pojazdów. Dzięki nim możliwe jest odpowiednie wytyczenie trasy, która dla określonych kryteriów będzie najlepsza. Systemy nawigacji drogowej umożliwiają także zbieranie i prezentowanie informacji na temat natężenia ruchu drogowego, średnich czasów przejazdu odcinkami drogowymi dla wybranej pory dnia oraz personalizację wyświetlanych informacji, na przykład ze względu na wybrany środek transportu. Aplikacje korzystające z systemów nawigacyjnych, dzięki utrzymywaniu stałego połączenia z internetem, umożliwiają użytkownikowi dostęp do wszystkich aktualnych informacji na temat warunków drogowych. Aby jednak możliwe było korzystanie z tego typu systemów, użytkownik musi wyrazić zgodę na dostęp przez system do jego aktualnej lokalizacji. Ze względu na łatwość obsługi systemów nawigacji drogowej oraz zakres prezentowanych informacji systemy tego typu są bardzo często wykorzystywane, a proponowane trasy są realizowane (nawet bez weryfikacji) przez prowadzących pojazdy.

Aplikacje, dzięki informacjom na temat lokalizacji poszczególnych użytkowników, mogą także proponować zmianę trasy w celu skrócenia czasu dojazdu. W przypadku ataku cybernetycznego może dojść do kradzieży danych na temat przemieszczania się poszczególnych użytkowników. Pozyskanie tego typu danych może posłużyć cyberprzestępcom do fizycznego przestępstwa.

Drugim problematycznym skutkiem ataków cybernetycznych może być wprowadzenie do systemu fałszywych informacji – atak typu *spoofing*, polega na tym, że odbiornik GPS zostaje oszukany w celu nadawania fałszywych sygnałów, w efekcie czego może dojść do sztucznego wywołania kongestii drogowej w wybranym miejscu. Działania tego typu są niezwykle niebezpieczne, ponieważ umożliwiają zablokowanie wybranego odcinka drogi lub przekierowanie ruchu po odcinkach niebezpiecznych lub z czasowym ograniczeniem ruchu. Aplikacje mobilne z nawigacją drogową dzięki swoim funkcjonalnościom są obecnie wykorzystywane do weryfikowania czasów przejazdu poszczególnymi odcinkami drogowymi. Prowadzący pojazdy, nawet znając trasę przejazdu, decydują się przejechać odcinkami proponowanymi przez aplikację. Jest to zjawisko, które zmniejsza odporność kierujących na fałszywe i niezweryfikowane informacje.

Przeciwdziałać atakom skierowanym na systemy nawigacji drogowej nie jest łatwo, ponieważ w wielu aplikacjach o utrudnieniach mogą informować sami użytkownicy, wciskając na ekranie aplikacji podczas przejazdu odpowiedni przycisk. Wprowadzenie tej samej informacji kilkukrotne przez różnych użytkowników może spowodować, że aplikacja zmieni chwilowo trasę dla wielu innych prowadzących korzystających z tej samej aplikacji. W przypadku świadomych ataków cybernetycznych chwilowe trudności mogą zmienić się w realne problemy w dłuższym przedziale czasu. Przeciwdziałać kradzieży danych na temat tras przejazdów poszczególnych użytkowników należy poprzez anonimowość użytkowników już na etapie przesyłania informacji o swojej lokalizacji oraz indywidualną kontrolę swoich urządzeń mobilnych pod kątem złośliwego oprogramowania. Istotnym elementem jest również zagłuszanie sygnałów GPS poprzez generator sygnału transmisji w celu opóźnienia odbioru (urządzenia typu Jammer). W tym przypadku sygnał GPS zostaje zakłócony, przez co lokalizatory nie są w stanie ustalić pozycji pojazdu. Z punktu widzenia lokalizatorów pojazd wydaje się nie przemieszczać, aż do momentu odłączenia urządzenia.

Systemy sterowania ruchem drogowym

Sterowanie ruchem drogowym i sygnalizacją świetlną jako element inteligentnych systemów transportowych jest jednym z kluczowych elementów miejskiego systemu transportowego. To, w jak wydajny sposób funkcjonuje sygnalizacja świetlna lub obszarowe systemy sterowania ruchem, decyduje o płynności ruchu drogowego w danym obszarze miasta. W nowoczesnych systemach sterowania ruchem drogowym dane zbierane są w sposób automatyczny z różnego rodzaju detektorów drogowych (od detekcji indukcyjnej po wideo detektory) [1]. W zależności od typu systemu dane są gromadzone i archiwizowane lub wykorzystywane w czasie rzeczywistym bez ich

archiwizacji. W pierwszym przypadku dane można wykorzystać jako element okresowych pomiarów ruchu drogowego. W drugim przypadku dane służą jedynie na potrzeby zmiennoczasowych programów sygnalizacji świetlnej. W obu przypadkach bezpieczeństwo systemu zależy od metody dostępu do zbieranych danych. W przypadku systemów izolowanych wykorzystujących dane w czasie rzeczywistym bez ich zapisu przeprowadzenie ataku cybernetycznego mogącego mieć realne, negatywne skutki jest niezwykle trudne. Inaczej jest w przypadku systemów, które zbierają dane z wykorzystaniem połączenia internetowego oraz zapisują je w celu dalszej analizy. Tego typu systemy, zapewniające bardzo przydatne dane z punktu widzenia analizy miejskiego systemu transportowego, mogą stać się celem ataków cybernetycznych. Ataki tego typu mogą mieć na celu zaburzenie pracy systemu, awarię jego działania lub działanie w sposób niezgodny z przeznaczeniem. W przypadku wprowadzenia do systemu nieprawdziwych danych na temat natężenia ruchu drogowego na poszczególnych odcinkach drogowych i użycie ich przez system do kalibracji programów sygnalizacji świetlnej działających w ramach wybranego obszaru miasta może dojść do wywołania kongestii drogowej i spowodowania sytuacji skrajnie niebezpiecznych z punktu widzenia bezpieczeństwa ruchu drogowego.

Na zagrożenia cybernetyczne są także narażone systemy zarządzania ruchem drogowym odpowiedzialne między innymi za: ograniczanie wjazdu do wybranych obszarów, informację o przejezdności tuneli, automatyczne kontrolowanie prędkości pojazdów i sczytywaniu tablic rejestracyjnych (ANPR) lub wyświetlanie informacji na znakach zmiennej treści VMS. Włamanie do baz danych zbieranych i udostępnianych przez tego typu systemy może wiązać się nie tylko z wyświetlaniem błędnych informacji na tablicach zmiennej treści, ale także dostępem do informacji wrażliwych na temat wykroczeń drogowych poszczególnych kierowców. Manipulowanie danymi w tego typu bazach danych może skutkować na przykład wykasowaniem informacji na temat wykroczeń dokonanych przez pojazdy o wybranych numerach rejestracyjnych, umożliwienie wjazdu do strefy o ograniczonym wjeździe pojazdom niepożądanym lub, w przypadku akcji ratunkowej, utrudnienie wjazdu pojazdom służb ratunkowych.

W celu zabezpieczenia systemów zarządzania i sterowania ruchem drogowym niezbędne jest wprowadzanie standardów i zabezpieczeń mających na celu ochronę danych na przykład poprzez szyfrowanie danych gromadzonych w bazach danych. Kolejnym sposobem utrudnienia dostępu do systemów przez osoby niepożądane jest szkolenie pracowników oraz zawężanie grona osób mających dostęp administracyjny do systemu. Ważnym aspektem bezpieczeństwa jest także przeprowadzanie okresowej zmiany haseł oraz wprowadzanie certyfikatów uwierzytelniających poszczególnych użytkowników (umożliwia wykrycie podszywania się pod wybranych pracowników w trakcie ich nieobecności lub poza godzinami pracy).

Automatyczne systemy zliczania pasażerów

Systemy automatycznie liczące pasażerów wsiadających i wysiadających z pojazdów transportu publicznego, ze względu na różnice w wykorzystywanych czujnikach ruchu, mogą zbierać mniej lub bardziej szczegółowe dane [2]. Podstawowe systemy opierające się na czujnikach laserowych lub na podczerwień są w stanie zbierać informacje jedynie na temat liczby wejść i wyjść z pojazdu na każdym z przystanków. Wykorzystanie obrazu z kamer, umożliwia w bardziej zaawansowanych systemach rozpoznawanie poszczególnych pasażerów. W ten sposób zbierane dane dają możliwość określenia pełnych tras podróży realizowanych przez pasażerów, nawet tych, podczas których pasażerowie przesiadali się pomiędzy różnymi pojazdami. Zbierane w ten sposób dane są bardzo cenne z punktu widzenia organizatora miejskiego transportu zbiorowego, ponieważ umożliwiają określenie dokładnej macierzy podróży pasażerów, co przekłada się na możliwość lepszego dopasowania oferty przewozowej do aktualnego popytu. Dodatkowo dane zbierane w sposób ciągły umożliwiają wykorzystanie ich w czasie rzeczywistym do zarządzania flotą pojazdów [4] oraz informowania pasażerów o wolnych miejscach w pojazdach [3]. Automatyczne systemy zliczania pasażerów umożliwiają tworzenie w krótkim czasie bardzo dużych zbiorów danych. Tego typu dane są z reguły gromadzone przez operatorów w celu ich wykorzystania przez organizatora miejskiego transportu zbiorowego do poprawienia oferty przewozowej.

Bezpieczeństwo cybernetyczne danych zebranych przez systemy zliczające pasażerów uzależnione jest od sposobu przesyłania danych pomiędzy pojazdami a serwerami przewoźnika oraz weryfikacji osób upoważnionych do dostępu do zebranych danych. W pierwszym przypadku dane mogą być przesyłane w czasie rzeczywistym połączeniem bezprzewodowym lub zgrywane z pojazdu dopiero po zjeździe do zajezdni (w sposób przewodowy lub bezprzewodowy). W obu metodach przesyłania danych istnieje ryzyko nieautoryzowanego dostępu. Aby zmniejszyć ryzyko ataku i kradzieży lub manipulowania danymi, transmisja danych powinna być prowadzona w sposób zaszyfrowany, uniemożliwiający dostęp osób trzecich. W przypadku transmisji danych realizowanej w zajezdni przewoźnika istotne w kontekście cyberbezpieczeństwa jest to, czy transmisja (przewodowa lub bezprzewodowa) odbywa się w sposób automatyczny, czy wymaga dostępu administracyjnego. W przypadku automatycznej szyfrowanej transmisji danych ryzyko utraty lub zmiany przesyłanych danych jest mniejsze. W procesie przesyłania danych wymagających dostępu administracyjnego ważną rolę odgrywa przeszkolenie i odpowiedzialność pracowników odpowiedzialnych za przeprowadzenia czynności. Ryzyko udanego ataku cybernetycznego można także ograniczyć poprzez zachowanie anonimowości zebranych danych (np. w przypadku danych zebranych przez system wideo zapis powinien obejmować jedynie informacje dotyczące danych transportowych, a nagranie nie powinno być archiwizowane).

W przypadku automatycznych systemów zliczania pasażerów utrata lub manipulacja danymi spowodowana przez atak cybernetyczny wpływa na dwa elementy miejskiego systemu transportu zbiorowego. Pierwszym z nich jest przydział taboru do poszczególnych brygad, realizowany na podstawie okresowych analiz popytu. W przypadku danych zmienionych w wyniku ataku cybernetycznego tabor przydzielano by na podstawie błędnych wyników analiz, co skut-

kowałoby spadkiem komfortu na wybranych liniach transportu publicznego oraz wzrostem kosztu obsługi innych. Drugim elementem, na który ma wpływ atak cybernetyczny, jest przekazywanie informacji o liczbie pasażerów do informacji pasażerskiej lub planerów podróży. Błędne dane spowodowałyby problemy w przemieszczaniu się wielu osób i spadek zaufania pasażerów do informacji pasażerskiej, jak i całego systemu miejskiego transportu zbiorowego.

Systemy opłat parkingowych i sprzedaży biletów

Wraz z szybkim rozpowszechnianiem się urządzeń mobilnych (takich jak telefony komórkowe) oraz ich ciągłym rozwojem rozwinęły się aplikacje umożliwiające zakup biletu na miejski transport zbiorowy lub dokonanie opłaty za miejsce postojowe w strefie płatnego parkowania. Aplikacje te zapewniają transakcje realizowane w sposób szybki i bezgotówkowy. Dodatkowo umożliwiają zakup biletu parkingowego lub na transport zbiorowy tylko na ten czas, w którym była realizowana usługa. Użytkownik ma możliwość wyboru metody płatności, a wszystkie formalności są realizowane automatycznie. Wraz z rozwojem tego typu narzędzi oraz wzrostem liczby płatności bezgotówkowych wzrosło też zagrożenie atakiem cybernetycznym. Ataki te mają na celu kradzież danych logowania do aplikacji lub danych wrażliwych umożliwiających kradzież środków finansowych z konta ofiary. Mimo wielu zabezpieczeń, jakie mają aplikacje na urządzenia mobilne wykorzystujące płatności bezgotówkowe, to niektóre ataki udaje się przeprowadzić skutecznie. Jednym z poważniejszych ataków cybernetycznych w Polsce był przeprowadzony w nocy z 7 na 8 lutego 2023 roku na centralny system Śląskiej Karty Usług Publicznych umożliwiającej płatności za przejazdy transportem publicznym. Atak ten pokazuje, że nawet zabezpieczone systemy nie są w pełni odporne na zagrożenia cybernetyczne.

Zagrożenia w systemach opłat parkingowych i sprzedaży biletów można zauważyć w kilku elementach każdego z systemów. Pierwszym z nich jest zagrożenie dla systemu centralnego i serwerów obsługujących podsystemy. Drugim jest zagrożenie indywidualne dla użytkowników poprzez złośliwe oprogramowanie szpiegujące, kopiujące informacje wprowadzane poprzez urządzenie mobilne. Przykładem takiego zagrożenia może być atak typu *Man in the Middle*, którego konsekwencją może być kradzież danych kartowych poprzez odczyt podawanych informacji przez użytkownika/płatnika parkingu. W obu przypadkach metodą ograniczenia szans na udany atak jest odpowiednia wiedza i przestrzeganie standardów bezpieczeństwa. W przypadku indywidualnych użytkowników ważne jest monitorowanie pracy urządzenia mobilnego oraz rozważne wprowadzanie danych wrażliwych do urządzenia, zwłaszcza w miejscach zatłoczonych (przystanki lub pojazdy miejskiego transportu zbiorowego). W przypadku serwerów i systemu centralnego niezbędne jest odpowiednie szkolenie pracowników odpowiedzialnych za administrowanie systemu oraz przyjęcie szczegółowych procedur postępowania i wystawiania certyfikatów dostępu do systemu. Niezbędne jest także częste weryfikowanie haseł oraz fizycznych zabezpieczeń do kluczowych pomieszczeń. Inną metodą poprawy zabezpieczeń sieciowych systemów opłat parkingowych i sprzedaży biletów jest wprowadzanie odpowiedniego szyfrowania danych wrażliwych oraz monitorowanie nieautoryzowanych prób zewnętrznego dostępu do systemu.

Podsumowanie i wnioski

Rozwój sieci internetowych, którego efektem był dynamiczny rozwój urządzeń i aplikacji mobilnych, spowodował poprawę dostępności do informacji na temat transportu zbiorowego. Obecnie, przy wykorzystaniu czujników w pojazdach, tablic zmiennej treści oraz łączności bezprzewodowej, możliwe jest przesyłanie informacji i ich wykorzystanie w czasie rzeczywistym. Pasażerowie uzyskali dostęp do pełnej informacji na temat transportu zbiorowego. Zintegrowanie ze sobą poszczególnych elementów systemu z wykorzystaniem szybkich połączeń internetowych umożliwiło także przeprowadzanie ataków cybernetycznych, których celem jest kradzież lub manipulowanie danymi. Zagrożenia te wymuszają ciągłe udoskonalanie systemów zabezpieczeń i szyfrowania danych wrażliwych. Wiąże się to także z wprowadzaniem standardów postępowania na wypadek ataku cybernetycznego oraz postępowania mającego zapobiec atakom.

Przedstawione w artykule zagadnienia są jedynie wstępem do dalszych prac mających na celu zaproponowanie standardów dla cyberbezpieczeństwa w transporcie miejskim. Standardy te umożliwiłyby lepsze zabezpieczenie systemów oraz ocenę już stosowanych zabezpieczeń.

Literatura

1. Aleksandrowicz J., Piwowarczyk M., *Sposoby detekcji pojazdów transportu zbiorowego i ich funkcjonalność*, „Transport Miejski i Regionalny", 2016, nr 6.
2. Aleksandrowicz J., *Przydatność automatycznych systemów zliczania pasażerów w celach predykcji popytu na usługi transportowe*, „Transport Miejski i Regionalny", 2018, nr 4.
3. Aleksandrowicz J., *Informowanie pasażerów o wolnych miejscach w pojazdach miejskiego transportu zbiorowego z wykorzystaniem automatycznych systemów zliczania pasażerów*, „Transport Miejski i Regionalny", 2019, nr 8.
4. Aleksandrowicz J., *Wielokryterialna optymalizacja przydziału taboru do linii miejskiego transportu zbiorowego*, „Transport Miejski i Regionalny", 2022, nr 6.
5. Kochan A., Koper E., *Cyberbezpieczeństwo systemów kierowania ruchem kolejowym*, „TTS", 2017, nr 12.
6. Krawiec K., Kłos M. J., Markusik S., Bułkowski A., *Ocena systemu transportowego opartego o napęd elektryczny z punktu widzenia cyberbezpieczeństwa*, Prace Naukowe Politechniki Warszawskiej, „Transport", 2019, z. 124.
7. Lévy-Bencheton C., Darra E., *Cyber Security and Resilience of Intelligent Public Transport Good practices and recommendations*, ENISA, 2016.
8. Pawlik M., *Wytyczne dotyczące cyberbezpieczeństwa dla pracowników podmiotów kolejowych*, „Problemy Kolejnictwa Railway Report", 2021, z. 191.
9. Pawlik M., *Czas na kompleksowe podejście do bezpieczeństwa systemów transportowych opartych na predefiniowanych drogach przebiegu (bezpieczeństwo, ochrona, cyberbezpieczeństwo)*, „TTS", 2019, nr 7–8.
10. Pawlik M., *Systemowa ocena bezpieczeństwa kolei – metodologia oceny dla systemów transportowych*, Zeszyty Naukowo–Techniczne SITK RP, Oddział w Krakowie, 2019, nr 2 (119).
11. Poliński J., Ochociński K., *Cyfryzacja w transporcie kolejowym*, „Problemy Kolejnictwa Railway Report", 2020, z. 188.