psnm NEW MOBILITY ASSOCIATION

WARSZAWA 2026

Cyberbezpieczeństwo Nowej Mobilności

odporność
bezpieczeństwo
suwerenność technologiczna
wzmocnienie kompetencji sektora motoryzacyjnego
rozwój obszaru R&D w Polsce
budowa przewag konkurencyjnych i local content

PARTNERZY MERYTORYCZNI

Łukasiewicz
Przemysłowy Instytut Motoryzacji

Łukasiewicz
Instytut Sztucznej Inteligencji
i Cyberbezpieczeństwa

OSW

WYDAWCA
Polskie Stowarzyszenie Nowej Mobilności (PSNM)
psnm.org

ZESPÓŁ REDAKCYJNY
Polskie Stowarzyszenie Nowej Mobilności
Jan Wiśniewski

Ośrodek Studiów Wschodnich
Autorka: Paulina Uznańska
Redakcja merytoryczna: Jakub Jakóbowski
Współpraca: Anna Lipiec

Sieć Badawcza Łukasiewicz-Przemysłowy Instytut Motoryzacji
Autor: dr inż. Karol Zielonka

Sieć Badawcza Łukasiewicz - Instytut Sztucznej Inteligencji i Cyberbezpieczeństwa
Jan Kozak
Barbara Probierz
Monika Ingram

PARTNERZY
Ośrodek Studiów Wschodnich
Sieć Badawcza Łukasiewicz – Przemysłowy Instytut Motoryzacji
Sieć Badawcza Łukasiewicz – Instytut Sztucznej Inteligencji i Cyberbezpieczeństwa

PROJEKT GRAFICZNY I SKŁAD
Natalia Minksztym

Warszawa, 2026

Spis treści

Słowo wstępne

Nowa mobilność – obejmująca elektryfikację, digitalizację oraz autonomizację – staje się jednym z fundamentów funkcjonowania nowoczesnego państwa. Wraz z transformacją technologiczną coraz większego znaczenia nabiera konieczność budowy odporności na zagrożenia cyfrowe. Polska, jako jeden z kluczowych ośrodków sektora automotive w Europie, stoi przed historyczną szansą zdobycia wiodącej pozycji w europejskim i globalnym łańcuchu wartości cyberbezpieczeństwa. Zbudowanie kompetencji w tym obszarze wymaga skoordynowanego działania administracji, przemysłu i nauki.

Postępująca transformacja wykracza poza same zmiany napędowe. Pojazdy stopniowo przekształcają się w platformy cyfrowe, funkcjonujące w oparciu o dziesiątki milionów linii kodu. Infrastruktura ładowania w coraz większym stopniu integruje się z siecią elektroenergetyczną, a dane generowane przez mobilność coraz częściej postrzega się jako strategiczne aktywa. Wraz z rosnącym nasyceniem obszaru mobilności technologiami cyfrowymi zmieniają się również rodzaje i skala wyzwań, związanych z funkcjonowaniem systemu transportowego i energetycznego.

Na podstawie najnowszych danych Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), transport jest drugim – po administracji publicznej – sektorem, w którym notuje sie najwięcej przypadków incydentów naruszenia cyberbezpieczeństwa. Z perspektywy bezpieczeństwa państwa, nowa mobilność staje się więc obszarem krytycznym. Elektryczne, połączone i autonomiczne pojazdy tworzą ekosystem cyfrowy zintegrowany z sieciami energetycznymi, telekomunikacyjnymi i transportowymi, który jednocześnie jest podatny na ataki, również te o skutkach systemowych.

Od kradzieży danych użytkowników, przez wywoływanie awarii urządzeń i infrastruktury aż po paraliż transportowy lub energetyczny. Zagrożenia, które jeszcze niedawno były powszechnie rozpatrywane w kategorii czystego science-fiction stają się coraz bardziej realne i obejmują nie tylko strefę prywatną, ale również publiczną. W tym kontekście cyberbezpieczeństwo przestaje być domeną wyłącznie inżynierów IT – nabiera strategicznego znaczenia bezpieczeństwa państwa, konkurencyjności i suwerenności.

Prezentowany white paper zawiera syntetyczną analizę zagrożonych obszarów, kluczowych regulacji prawnych, rozwiązań bezpieczeństwa oraz potencjału Polski jako jednego z centrów rozwoju zdolności w zakresie cyberbezpieczeństwa. Przedstawiamy również rekomendacje adresowane do kluczowych interesariuszy sektora publicznego oraz prywatnego.

Niniejsze opracowanie powstało w oparciu o wiedzę i zasoby kluczowych interesariuszy polskiego łańcucha wartości cyberbezpieczeństwa. W tym miejscu chciałbym serdecznie podziękować naszym Partnerom za wkład merytoryczny, bez którego powstanie raportu nie byłoby możliwe. Należą do nich: Sieć Badawcza Łukasiewicz – Przemysłowy Instytut Motoryzacji, Sieć Badawcza Łukasiewicz – Instytut Sztucznej Inteligencji i Cyberbezpieczeństwa oraz Ośrodek Studiów Wschodnich.

Tak szerokie zaplecze eksperckie gwarantuje, że złożona problematyka cyberbezpieczeństwa została ujęta w sposób kompleksowy, w oparciu o najwyższe standardy wiedzy i praktyki.

Serdecznie zapraszam Państwa do lektury,

Maciej Mazur
Dyrektor Zarządzający PSNM

Źródło: Sieć Badawcza Łukasiewicz - Przemysłowy Instytut Motoryzacji

1 Wyzwania sektora nowej mobilności w obszarze cyberbezpieczeństwa

1

Wyzwania sektora nowej mobilności w obszarze cyberbezpieczeństwa

Pojazdy

Postępująca transformacja transportu obejmuje nakładające się na siebie wymiary, w tym elektryfikację napędów, cyfryzację architektury pojazdów oraz łączność z infrastrukturą zewnętrzną. Każdy z tych wymiarów stanowi potencjalne pole do cyberataków i wprowadza nowe klasy zagrożeń.

Konstrukcja samochodów elektrycznych obecnej generacji opiera się na ponad 100 elektronicznych jednostkach sterujących (ECU), połączonych sieciami komunikacyjnymi. Zarządzają one wieloma układami pojazdów, zapewniając komfortową i bezpieczną jazdę. Nowoczesne samochody należą do najbardziej złożonych urządzeń konsumenckich pod względem liczby linii kodu, która często przekracza 200 mln. Architektura SDV (Software-Defined Vehicle) sprawia, że pojazdy stały się platformami usługowymi aktualizowanymi przez cały okres użytkowania. Technologie umożliwiające łączność pojazdów z otoczeniem (V2X: Vehicle-to-Everything), z siecią elektroenergetyczną (V2G: Vehicle-to-Grid), z siecią telekomunikacyjną (V2N: Vehicle-to-Network), czy wreszcie ze sobą nawzajem (V2V: Vehicle-to-Vehicle) tworzą rozległy, dynamiczny ekosystem cyfrowy. Dane generowane przez pojazdy połączone – telematyka, nawigacja, dane behawioralne kierowcy, dane diagnostyczne, nagrania z kamer – stanowią zasób o rosnącej wartości ekonomicznej i strategicznej. Szacuje się, że samochód wyposażony w zaawansowane systemy wspomagania jazdy może generować nawet kilkadziesiąt gigabajtów danych na godzinę jazdy.

Pojazdy połączone, elektryczne i zautomatyzowane należy traktować jako systemy cyberfizyczne, w których cyberbezpieczeństwo wpływa bezpośrednio na bezpieczeństwo funkcjonalne, niezawodność eksploatacji, ochronę danych oraz odpowiedzialność producenta. Wymagania homologacyjne i regulacyjne, w szczególności związane z zarządzaniem cyberbezpieczeństwem pojazdu oraz aktualizacjami oprogramowania, powodują, że bezpieczeństwo cyfrowe powinno być oceniane w całym cyklu życia pojazdu: od projektu, przez produkcję i dopuszczenie do ruchu, po eksploatację, serwis, aktualizacje oraz wycofanie pojazdu z ruchu.

Podatność pojazdów na cyberataki wynika przede wszystkim z rosnącej liczby elektronicznych jednostek sterujących, zewnętrznych interfejsów komunikacyjnych, aplikacji mobilnych, systemów zdalnego dostępu, usług chmurowych, funkcji aktualizacji OTA oraz integracji z ekosystemem

V2X i V2G. Potencjalne zagrożenia obejmują m.in. nieautoryzowany dostęp do funkcji pojazdu, przejęcie konta użytkownika, manipulację danymi diagnostycznymi, zakłócenie działania systemów wspomagania kierowcy, instalację nieautoryzowanego oprogramowania, zablokowanie funkcji pojazdu, kradzież danych lokalizacyjnych lub wykorzystanie floty pojazdów jako elementu szerszego ataku na infrastrukturę cyfrową.

Teoretyczny scenariusz incydentu

Atakujący wykorzystuje podatność w aplikacji mobilnej lub interfejsie API producenta, uzyskuje dostęp do wybranych funkcji pojazdu i wykonuje zdalne polecenia, takie jak odblokowanie pojazdu, uruchomienie klimatyzacji, odczyt lokalizacji albo manipulacja ustawieniami profilu użytkownika. Przy większej skali incydentu skutkiem może być utrata zaufania do producenta, naruszenie prywatności, konieczność masowej aktualizacji oprogramowania oraz czasowe ograniczenie funkcjonalności pojazdów.

Studium przypadku

Zdalna eksploatacja podatności w pojeździe połączonym

Jeden z najbardziej znanych przykładów ryzyka cyberbezpieczeństwa w motoryzacji obrazuje badanie przeprowadzone przez Charliego Millera i Chrisa Valaska, w którym wykazano możliwość zdalnej eksploatacji podatności w seryjnym pojeździe. Wykorzystanie słabości w warstwie komunikacyjnej oraz oprogramowaniu systemu infotainment pozwoliło badaczom uzyskać wpływ na wybrane funkcje pojazdu. Przypadek ten pokazał, że niewystarczająca separacja systemów, błędy w oprogramowaniu i niekontrolowane kanały komunikacji mogą prowadzić do sytuacji, w której zagrożenie cyfrowe oddziałuje na funkcje istotne dla bezpieczeństwa użytkownika. Wnioskiem dla sektora nowej mobilności jest konieczność projektowania pojazdów w architekturze ograniczającej możliwość propagacji ataku między systemami, systematycznego zarządzania podatnościami oraz walidacji aktualizacji oprogramowania w całym cyklu życia pojazdu.

Infrastruktura ładowania

Infrastruktura ładowania, będąca filarem systemu nowej mobilności, ulega systematycznej rozbudowie na całym świecie. W Polsce tylko w latach 2024-2025 r. sieć publicznie dostępnych punktów powiększyła się niemal dwukrotnie (z ok. 5,9 tys. do prawie 11,8 tys. punktów).

Stacje ładowania to połączone ze sobą urządzenia IoT, mające możliwość m.in. dokonywania płatności zbliżeniowych, pobierania poufnych danych czy sterowania mocą w czasie rzeczywistym. Również funkcjonowanie infrastruktury ładowania opiera się na coraz bardziej skomplikowanym oprogramowaniu, obejmującym często kilkanaście milionów linii kodu. Technologie takie jak smart charging czy Vehicle-to-Grid sprawiają, że stacje ładowania stają się integralnym elementem systemu energetycznego, mającym pozytywny wpływ na elastyczność sieci.

W rezultacie infrastruktura ładowania stanowi nowy, strategiczny segment infrastruktury krytycznej, funkcjonujący na granicy systemu transportowego i elektroenergetycznego. Jednocześnie każda nowoczesna stacja ładowania to urządzenie sieciowe zarządzane zdalnie, podatne na ataki cybernetyczne o potencjalnie kaskadowych skutkach dla mobilności i sieci energetycznej.

Infrastrukturę ładowania należy postrzegać jako rozproszony system cyberfizyczny, który obejmuje nie tylko samo urządzenie ładowania, lecz także pojazd, system operatora, aplikację użytkownika, system płatności, platformy roamingowe, zaplecze chmurowe oraz elementy systemu elektroenergetycznego. Z tego względu cyberbezpieczeństwo infrastruktury ładowania obejmuje całość ekosystemu technicznego i organizacyjnego, w którym ryzyka mogą powstawać w warstwie komunikacji, autoryzacji, rozliczeń, aktualizacji oprogramowania, zdalnej diagnostyki oraz sterowania mocą. Atak na jeden z tych elementów może oddziaływać nie tylko na dostępność pojedynczej stacji, lecz także na ciągłość świadczenia usług ładowania, bezpieczeństwo danych użytkowników, rozliczenia finansowe oraz stabilność lokalnych elementów systemu elektroenergetycznego.

Podatność infrastruktury ładowania wynika z jej masowej skali, zdalnego zarządzania, wykorzystywania standardów komunikacyjnych, integracji z systemami płatności oraz coraz silniejszego powiązania z siecią elektroenergetyczną. Zagrożenia mogą obejmować przejęcie kont operatora, manipulację ceną lub rozliczeniem energii, wyciek danych użytkowników, nieautoryzowane aktualizacje oprogramowania, wyłączenie punktów ładowania, zmianę parametrów ładowania, ataki na mechanizmy Plug & Charge, zakłócenie pracy flot pojazdów oraz skoordynowaną manipulację poborem mocy.

Teoretyczny scenariusz incydentu

Atakujący uzyskuje dostęp do systemu zarządzania operatora infrastruktury ładowania i wysyła polecenia ograniczające dostępność dużej liczby stacji w aglomeracji lub przy głównych korytarzach transportowych. Skutkiem może być paraliż ładowania flot, utrudnienie transportu miejskiego lub logistycznego, szkody wizerunkowe operatora, straty finansowe oraz konieczność awaryjnego przełączenia systemów w tryb ręczny.

Studium przypadku

Przegląd podatności infrastruktury ładowania EVSE opracowany przez Sandia National Laboratories

Badanie przygotowane przez zespół Sandia National Laboratories wskazuje, że infrastruktura ładowania pojazdów elektrycznych jest narażona na podatności występujące w samych urządzeniach EVSE, komunikacji między pojazdem a ładowarką, usługach chmurowych dostawców infrastruktury, systemach stron trzecich oraz powiązaniach z operatorami sieci. Zakres potencjalnych skutków obejmuje przejęcie lub zakłócenie pracy pojedynczych ładowarek, manipulację danymi i usługami operatora, utratę dostępności ładowania, a w scenariuszach większej skali również wpływ na transport i system elektroenergetyczny. Badanie to potwierdza, że infrastruktura ładowania wymaga ochrony zarówno w warstwie urządzeń, komunikacji i oprogramowania, jak i w warstwie usług operatorskich oraz integracji z siecią energetyczną.

Przemysł nowej mobilności

Cyberbezpieczeństwo to kwestia o coraz większym znaczeniu nie tylko na poziomie pojazdów czy infrastruktury, ale również szeroko pojętego przemysłu nowej mobilności.

Sektor motoryzacyjny charakteryzuje się wielowarstwową strukturą, w ramach której OEM (producenci pojazdów) opierają się na dostawcach Tier 1 (systemów), Tier 2 (modułów) i Tier 3 (komponentów). W ekosystemie cyfrowym nowej mobilności do tego łańcucha dołączają dostawcy oprogramowania, usług chmurowych, map i danych, a także chipów i modułów komunikacyjnych. Każdy element tego złożonego systemu może stać się celem cyberprzestępców.

Przemysł nowej mobilności tworzy rozbudowany łańcuch wartości, w którym cyberbezpieczeństwo jest cechą całego produktu i procesu jego powstawania, a nie wyłącznie finalnego produktu. Ryzyko może zostać wprowadzone na wielu etapach: przez komponent elektroniczny, moduł komunikacyjny, system bateryjny, bibliotekę oprogramowania, narzędzie diagnostyczne, dostawcę usług chmurowych, system produkcyjny lub proces aktualizacji. Oznacza to, że odporność cybernetyczna pojazdu, infrastruktury ładowania lub usługi mobilności zależy od jakości zarządzania ryzykiem w całym łańcuchu dostaw, w tym od oceny dostawców, dokumentowania pochodzenia komponentów i oprogramowania, zarządzania podatnościami oraz spójnych wymagań bezpieczeństwa dla uczestników łańcucha wartości.

Szczególne ryzyka dotyczą małych i średnich dostawców, którzy mogą nie posiadać wystarczających zasobów do wdrożenia zaawansowanych systemów zarządzania cyberbezpieczeństwem, mimo że ich komponenty trafiają do produktów o wysokim znaczeniu dla bezpieczeństwa. Dla Polski, jako ważnego ogniwa europejskiego sektora automotive, oznacza to konieczność rozwijania kompetencji wspierających dostawców w zakresie projektowania bezpiecznych komponentów, testowania, dokumentacji technicznej, audytów i przygotowania do wymagań globalnych producentów.

Teoretyczny scenariusz incydentu

Podatność zostaje wprowadzona do komponentu lub modułu komunikacyjnego dostarczanego przez podmiot zewnętrzny i trafia do wielu modeli pojazdów albo urządzeń infrastruktury. Po jej ujawnieniu producent musi przeprowadzić analizę wpływu, przygotować aktualizację, skoordynować działania z dostawcą i poinformować właściwe podmioty. Skutkiem może być opóźnienie produkcji, kosztowna akcja serwisowa, utrata reputacji i osłabienie pozycji dostawcy w łańcuchu wartości.

Studium przypadku

Atak na dostawcę jako ryzyko dla ciągłości działania przemysłu

Incydenty dotyczące dostawców oprogramowania, usług cyfrowych lub systemów produkcyjnych pokazują, że cyberatak na jeden podmiot może zakłócić funkcjonowanie wielu uczestników łańcucha wartości. W sektorze nowej mobilności taki scenariusz może dotyczyć dostawcy komponentów elektronicznych, oprogramowania diagnostycznego, modułów komunikacyjnych, systemów bateryjnych, usług chmurowych albo narzędzi wykorzystywanych w produkcji. Skutkiem może być czasowe zatrzymanie produkcji, opóźnienie dostaw, konieczność odłączenia systemów, przeprowadzenie audytu bezpieczeństwa, przygotowanie aktualizacji lub wymiana podatnego komponentu. W konsekwencji cyberbezpieczeństwo łańcucha dostaw powinno być traktowane jako element odporności przemysłowej, ciągłości działania i konkurencyjności dostawców.

Dane użytkowników, platformy cyfrowe i prywatność

Nowa mobilność opiera się na ciągłej wymianie danych między pojazdem, jego użytkownikiem i usługami zewnętrznymi. Wokół pojazdu połączonego funkcjonuje rozbudowany ekosystem platform cyfrowych: aplikacje producentów, usługi współdzielenia pojazdów i MaaS (Mobility-as-a-Service), platformy operatorów i roamingu ładowania, systemy płatności oraz brokerzy danych pojazdowych.

Każda z tych usług przetwarza dane osobowe, w tym dane lokalizacyjne, płatnicze i behawioralne, a wiele z nich buduje na tych danych modele biznesowe. Rozporządzenie (UE) 2023/2854 w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania (Data Act), stosowany od września 2025 r., poszerza krąg podmiotów uprawnionych do dostępu do danych generowanych przez pojazdy. Zwiększa to wartość rynkową danych i skalę ich cyrkulacji, a jednocześnie mnoży liczbę systemów, w których może dojść do naruszenia.

Podatność tego obszaru wynika z koncentracji danych w środowiskach chmurowych producentów i operatorów, z rozbudowanych interfejsów API, z długiego łańcucha podmiotów przetwarzających oraz z roli konta użytkownika jako jedynej warstwy kontroli dostępu do funkcji pojazdu i historii

podróży. Znaczenie ma również praktyka projektowa. Wymogi privacy by design oraz oceny skutków dla ochrony danych (DPIA) bywają realizowane po zakończeniu prac rozwojowych zamiast na etapie architektury systemu. EDPB wskazuje dane lokalizacyjne z pojazdów jako kategorię wymagającą szczególnej ochrony, ponieważ ujawniają one wzorce życia właścicieli, od miejsca zamieszkania i pracy po miejsca kultu lub leczenia. Odrębnym problemem są dane rezydualne w pojazdach współdzielonych i odsprzedawanych, w których pozostają profile, kontakty i historia tras poprzednich użytkowników.

Zagrożenia obejmują wyciek lub kradzież danych lokalizacyjnych i behawioralnych, przejęcia kont użytkowników dające dostęp do funkcji pojazdu, ataki ransomware z eksfiltracją danych wymierzone w platformy usług mobilności oraz obrót danymi bez ważnej podstawy prawnej. Skutki wykraczają poza odpowiedzialność pojedynczego administratora. Masowy wyciek danych lokalizacyjnych umożliwia rekonstrukcję tras, identyfikację miejsc zamieszkania i pracy oraz śledzenie osób pełniących funkcje publiczne, przez co naruszenie prywatności nabiera wymiaru bezpieczeństwa państwa. „ENISA Threat Landscape 2025" wskazuje zagrożenia dla danych wśród głównych kategorii incydentów w Unii Europejskiej,zaś raport Upstream z 2026 r. odnotowuje dalszy wzrost liczby incydentów obejmujących dane w sektorze motoryzacyjnym.

Teoretyczny scenariusz incydentu

Atakujący wykorzystuje podatność interfejsu API platformy współdzielenia pojazdów i pobiera dane lokalizacyjne oraz płatnicze kilkuset tysięcy użytkowników. Zestawienie historii tras z ogólnodostępnymi rejestrami pozwala przypisać przejazdy do konkretnych osób, w tym funkcjonariuszy i pracowników instytucji publicznych. Skutki obejmują obowiązki notyfikacyjne wynikające z RODO, odpowiedzialność administracyjną i cywilną operatora, utratę zaufania do usługi oraz ryzyko wtórnego wykorzystania danych w działaniach przestępczych lub wywiadowczych.

Studium przypadku

Wyciek danych lokalizacyjnych pojazdów elektrycznych

W grudniu 2024 r. ujawniono, że dane telematyczne około 800 tys. pojazdów elektrycznych wyprodukowanych przez jeden z koncernów motoryzacyjnych, w tym dokładne dane lokalizacyjne, były przez wiele miesięcy dostępne w niewłaściwie skonfigurowanym środowisku chmurowym spółki, odpowiadającej w grupie za oprogramowanie. Zbiór pozwalał powiązać pozycje pojazdów z danymi właścicieli. Wśród poszkodowanych znaleźli się politycy, przedsiębiorcy i funkcjonariusze. Incydent, wykazał, że pojedynczy błąd konfiguracji w warstwie chmurowej może zniweczyć zabezpieczenia całego ekosystemu pojazdu połączonego. Wnioskiem dla sektora nowej mobilności jest konieczność traktowania minimalizacji danych, regularnych audytów konfiguracji środowisk chmurowych oraz DPIA jako stałych elementów cyklu życia usług, a nie jednorazowych czynności zgodnościowych.

System elektroenergetyczny

Rozwój elektromobilności wiąże system transportowy z systemem elektroenergetycznym w bezprecedensowym zakresie. Infrastruktura ładowania, opisana we wcześniejszym rozdziale przede wszystkim w kontekście urządzenia i usługi, z perspektywy systemu elektroenergetycznego stanowi sterowane cyfrowo obciążenie.

Technologie smart charging i Vehicle-to-Grid pozwalają regulować pobór i oddawanie mocy w czasie rzeczywistym, a agregatorzy oraz mechanizmy odpowiedzi odbioru (DSR) włączają floty pojazdów i stacji w bilansowanie sieci. Sterowanie odbywa się przez łańcuch: pojazd-stacja ładowania-operator punktów ładowania-agregator-operator systemu dystrybucyjnego i przesyłowego. Komunikacja w tym łańcuchu opiera się na protokołach takich jak ISO 15118, OCPP i OpenADR. Powstaje w ten sposób nowa warstwa infrastruktury krytycznej, w której decyzje o rozpływie energii zapadają w systemach informatycznych rozproszonych pomiędzy wiele podmiotów.

Podatność tego obszaru wynika z połączenia trzech cech: masowej skali rozproszonych urządzeń sterowanych zdalnie, silnej zależności od poprawnej implementacji protokołów komunikacyjnych oraz styku technologii informatycznych (IT) z technologiami operacyjnymi (OT) systemu energetycznego. Systemy OT w dystrybucji i przesyle projektowano z myślą o niezawodności a nie o odporności na celowy atak, zaś wiele elementów pozostaje w eksploatacji przez dziesięciolecia. W efekcie warstwa cyfrowego sterowania mocą staje się celem, którego przejęcie oddziałuje bezpośrednio na proces fizyczny. Badania naukowe wskazują, że skoordynowana manipulacja dużą liczbą odbiorników o wysokiej mocy może zaburzać częstotliwość sieci i być wykorzystywana do manipulacji rynkiem energii. Floty pojazdów elektrycznych i stacji szybkiego ładowania mieszczą się w tej klasie odbiorników.

Zagrożenia w tym obszarze obejmują przejęcie systemów operatora punktów ładowania lub agregatora, skoordynowaną zmianę poboru mocy przez flotę stacji i pojazdów, manipulację sygnałami sterującymi ładowaniem, ataki na warstwę komunikacji pojazd-sieć oraz zakłócenie usług bilansujących świadczonych przez zasoby rozproszone. Skutki mogą mieć charakter kaskadowy i wykraczać poza dostępność ładowania: od lokalnych przeciążeń i zadziałania zabezpieczeń, przez naruszenie stabilności fragmentów sieci, po utrudnienie odbudowy zasilania. Nowe unijne zasady dotyczące cyberbezpieczeństwa transgranicznych przepływów energii elektrycznej oraz dyrektywa NIS2, wdrażana w Polsce nowelizacją ustawy o krajowym systemie cyberbezpieczeństwa, obejmują energetykę jako sektor kluczowy, co potwierdza wagę tego ryzyka

Teoretyczny scenariusz incydentu

Atakujący uzyskuje dostęp do platformy zarządzania agregatora łączącego kilka tysięcy punktów ładowania i baterii pojazdów. W godzinach szczytu wysyła skoordynowane polecenia jednoczesnego poboru maksymalnej mocy, a następnie jej gwałtownego zrzutu. Nagła zmiana obciążenia w jednym obszarze dystrybucyjnym prowadzi do lokalnych przeciążeń i zadziałania zabezpieczeń. Skutkiem może być przerwa w zasilaniu odbiorców, unieruchomienie ładowania flot transportu publicznego i logistyki oraz konieczność ręcznego przywracania normalnej pracy sieci. Zakres następstw zależy od udziału sterowanych zdalnie odbiorników w danym obszarze oraz od zabezpieczeń po stronie operatora sieci.

Studium przypadku

Ataki na system elektroenergetyczny Ukrainy (2015, 2016 i 2022)

Najlepiej udokumentowanymi do tej pory, publicznie potwierdzonymi przypadkami przerw w dostawie energii wywołanych celowym działaniem w cyberprzestrzeni pozostają ataki na ukraiński system elektroenergetyczny. W grudniu 2015 r. napastnicy, po wcześniejszym rozpoznaniu i uzyskaniu dostępu do sieci operatorów dystrybucyjnych, zdalnie otworzyli wyłączniki w kilkunastu stacjach, pozbawiając prądu setki tysięcy odbiorców, a jednocześnie utrudnili operatorom reakcję. W grudniu 2016 r. w ramach ataku na stację przesyłową w regionie Kijowa wykorzystano wyspecjalizowane oprogramowanie zdolne bezpośrednio manipulować protokołami sterowania urządzeniami energetycznymi. W październiku 2022 r. atakujący ponownie doprowadzili do przerwy w zasilaniu: zamiast dedykowanego złośliwego oprogramowania wykorzystali natywne funkcje środowiska SCADA do otwarcia wyłączników w stacji, a operację zsynchronizowali z ostrzałem rakietowym infrastruktury energetycznej. Choć celem nie była infrastruktura ładowania, przypadki te pokazują mechanizm istotny dla nowej mobilności: atak z warstwy cyfrowej przekłada się na proces fizyczny w systemie energetycznym, a rosnąca liczba sterowanych zdalnie zasobów rozproszonych, w tym stacji ładowania i pojazdów, poszerza powierzchnię takiego ataku. Wnioskiem dla sektora jest konieczność projektowania integracji ładowania z siecią z założeniem odporności na celowe działanie, segmentacji systemów sterowania oraz zdolności do pracy w trybie awaryjnym niezależnym od warstwy zdalnego sterowania.

Kontekst krajowy

Atak na infrastrukturę sektora energii w Polsce (grudzień 2025)

W Polsce wagę wyzwań związanych z opisywanym ryzykiem potwierdził skoordynowany atak z 29 grudnia 2025 r., opisany w raporcie technicznym CERT Polska ze stycznia 2026 r. Celem było co najmniej 30 farm wiatrowych i fotowoltaicznych, duża elektrociepłownia oraz firma z sektora produkcyjnego. Działania miały charakter destrukcyjny: obejmowały uszkadzanie układowego software urządzeń sterujących (RTU) oraz użycie oprogramowania nieodwracalnie kasującego dane. Do przerw w dostawach energii i ciepła nie doszło, jednak wybór rozproszonych, zdalnie sterowanych źródeł wytwarzania jako celu pokazuje, że powierzchnia ataku opisana w niniejszym rozdziale jest już testowana w praktyce, również w Polsce.

Badania, certyfikacja, homologacja i walidacja cyberbezpieczeństwa

Badania, certyfikacja, homologacja i walidacja cyberbezpieczeństwa stanowią praktyczny pomost między wymaganiami regulacyjnymi a realną zdolnością sprawdzenia odporności technologii nowej mobilności.

Obszar ten obejmuje pojazdy, komponenty, systemy ładowania, oprogramowanie, aktualizacje, narzędzia diagnostyczne oraz procedury eksploatacyjne. Jego znaczenie wynika z faktu, że sama zgodność formalna nie przesądza jeszcze o rzeczywistej odporności systemu na podatności, błędy implementacyjne, nieprawidłowe aktualizacje lub niewłaściwą konfigurację. Dopiero metodyki badawcze, testy odporności, walidacja aktualizacji oraz ocena dokumentacji technicznej pozwalają zweryfikować, czy wymagania cyberbezpieczeństwa zostały skutecznie przełożone na praktykę projektowania, produkcji i eksploatacji rozwiązań nowej mobilności.

Podatność tego obszaru polega na tym, że bez metodyk testowych/badawczych, kompetencji laboratoryjnych i procedur walidacji rynek może polegać wyłącznie na deklaracjach producentów lub zagranicznych centrach oceny. W tym kontekście Polska powinna rozwijać zdolności w zakresie analizy podatności, testów penetracyjnych, oceny architektury E/E, walidacji aktualizacji oprogramowania, badań odporności stacji ładowania, oceny dokumentacji technicznej oraz wsparcia producentów i dostawców w spełnianiu wymagań homologacyjnych i normatywnych.

Teoretyczny scenariusz incydentu

Producent wdraża aktualizację oprogramowania wpływającą na funkcje pojazdu lub infrastruktury ładowania bez wystarczającej walidacji bezpieczeństwa. Aktualizacja powoduje niezamierzone zakłócenie funkcji, ujawnia nową podatność albo wymaga wycofania i ponownego wdrożenia. Skutkiem jest przerwa w dostępności usługi, kosztowna akcja naprawcza, utrata zaufania oraz ryzyko naruszenia wymagań regulacyjnych.

Studium przypadku

Wykrycie podatności i walidacja aktualizacji bezpieczeństwa

W przypadku wykrycia podatności w pojeździe, komponencie lub systemie ładowania kluczowe znaczenie ma zdolność do szybkiego określenia zakresu oddziaływania incydentu, przygotowania poprawki, sprawdzenia jej wpływu na bezpieczeństwo oraz bezpiecznego wdrożenia aktualizacji. Proces ten wymaga współpracy producenta, dostawcy komponentu, operatora systemu, laboratoriów badawczych oraz jednostek technicznych. Jeżeli aktualizacja dotyczy funkcji istotnych dla bezpieczeństwa lub zgodności regulacyjnej, konieczna może być dodatkowa walidacja dokumentacji technicznej i ponowna ocena wpływu zmiany na system.

Systemy sztucznej inteligencji w nowej mobilności

Rozwiązania z obszaru sztucznej inteligencji znajdują zastosowanie w wielu systemach i funkcjach związanych z sektorem nowej mobilności. Modele uczenia maszynowego odpowiadają za percepcję w systemach wspomagania kierowcy i jazdy autonomicznej, monitorowanie stanu kierowcy, optymalizację ładowania i pracy sieci, predykcyjne utrzymanie oraz zarządzanie flotą.

Coraz częściej pojawiają się asystenci głosowi oparte na dużych modelach językowych. W raporcie ENISA i Wspólnego Centrum Badawczego Komisji Europejskiej systemy AI w jeździe autonomicznej opisano jako komponenty działające na podstawie statystycznej analizy dużych zbiorów danych, co odróżnia je od klasycznego oprogramowania opartego na jawnych regułach. Ta właściwość zapewnia niedostępne wcześniej możliwości, a jednocześnie tworzy nową powierzchnię podatności na ataki cybernetyczne. Skalę zjawiska potwierdza raport Upstream z 2026 r., według którego liczba ataków wspieranych przez AI w sektorze motoryzacyjnym w 2025 r. istotnie wzrosła, zarówno po stronie napastników, jak i wektorów wymierzonych w same systemy AI.

Podatność systemów AI wynika z ich zależności od danych i modeli. Ataki adwersaryjne polegają na wprowadzeniu do wejścia niewielkich, często niezauważalnych dla człowieka zakłóceń, które prowadzą do błędnej decyzji modelu, na przykład błędnej klasyfikacji znaku drogowego. Zatruwanie danych treningowych pozwala wprowadzić ukryte błędy już na etapie budowy modelu. Do tego dochodzą kradzież i ekstrakcja modeli, podatności w łańcuchu dostaw modeli gotowych i otwartych oraz manipulacja poleceniami w asystentach opartych na dużych modelach językowych. Raport ENISA i JRC zwraca uwagę, że ryzyka te nakładają się na klasyczne podatności systemów cyfrowych i wymagają uwzględnienia w całym cyklu życia, od danych i treningu, przez walidację, po eksploatację i aktualizacje modelu.

Zagrożenia obejmują błędne decyzje systemów percepcji wywołane celowo, obniżenie skuteczności modeli przez zatrucie danych, przejęcie kontroli nad zachowaniem asystenta pokładowego oraz wykorzystanie AI po stronie atakującego do automatyzacji rozpoznania i ataków. Skutki mogą mieć charakter systemowy, obejmujący wielu użytkowników jednocześnie: modele są powielane w tysiącach pojazdów lub urządzeń tej samej serii, więc jedna skutecznie wykorzystana podatność modelu oddziałuje na całą flotę korzystającą z tego samego rozwiązania. Rośnie w ten sposób ryzyko zdarzeń o zasięgu obejmującym wielu użytkowników jednocześnie, w tym zdarzeń wpływających na bezpieczeństwo funkcjonalne. Odpowiedzią na tę klasę ryzyka jest połączenie sztucznej inteligencji z cyberbezpieczeństwem również po stronie obrony, opisane w literaturze jako AI-driven security: wykrywanie anomalii, automatyzacja reakcji i analiza zagrożeń wspierana modelami.

Wymiar zarządzania ryzykiem wyznacza Rozporządzenie (UE) 2024/1689. Systemy AI wykorzystywane w funkcjach istotnych dla bezpieczeństwa pojazdu mogą zostać zakwalifikowane jako systemy wysokiego ryzyka, co pociąga za sobą wymogi w zakresie zarządzania ryzykiem, jakości danych, dokumentacji, nadzoru człowieka oraz odporności i cyberbezpieczeństwa. Wymogi te stykają się z ramami homologacyjnymi pojazdów oraz z normami inżynierii bezpieczeństwa i cyberbezpieczeństwa. Harmonogram stosowania obowiązków dla systemów wysokiego ryzyka był korygowany na poziomie unijnym, dlatego zakres i termin obowiązywania poszczególnych wymogów należy potwierdzić na dzień publikacji raportu. W szczególności systemy AI wbudowane w produkty regulowane, w tym komponenty bezpieczeństwa pojazdów, podlegają późniejszemu terminowi stosowania (według aktualnego harmonogramu – od 2 sierpnia 2028 r.), zaś samodzielne systemy wysokiego ryzyka z Załącznika III – od 2 grudnia 2027 r.

Teoretyczny scenariusz incydentu

Napastnik uzyskuje wpływ na zbiór danych wykorzystywany do trenowania lub aktualizacji modelu percepcji stosowanego w jednej serii pojazdów. Wprowadzone zatrucie powoduje, że w określonych warunkach model błędnie klasyfikuje wybrane obiekty lub znaki drogowe. Ponieważ ten sam model działa w całej serii, błąd ma charakter powtarzalny i obejmuje wiele pojazdów naraz. Skutkiem może być konieczność wycofania i ponownego trenowania modelu, masowa aktualizacja oprogramowania, czasowe ograniczenie funkcji wspomagania jazdy oraz ryzyko dla bezpieczeństwa funkcjonalnego do czasu usunięcia podatności.

Studium przypadku

Mylenie systemu rozpoznawania znaków drogowych

W raporcie ENISA i JRC omówiono przypadek ataku adwersaryjnego na system rozpoznawania znaków drogowych. Nałożenie na znak przygotowanego zakłócenia, przypominającego naklejkę i niezaburzającego odczytu przez człowieka, doprowadziło do błędnej klasyfikacji znaku przez model. Przykład ten, oparty na wcześniejszych pracach badawczych, ilustruje ogólny mechanizm: model uczenia maszynowego można wprowadzić w błąd przez celowo spreparowane dane wejściowe, bez ingerencji w kod czy sprzęt pojazdu. Wnioskiem dla sektora nowej mobilności jest konieczność walidacji modeli pod kątem odporności na ataki adwersaryjne, testowania w warunkach zbliżonych do rzeczywistej eksploatacji oraz stosowania mechanizmów redundancji i kontroli, ograniczających skutki błędnej decyzji pojedynczego modelu.

2 Bezpieczeństwo narodowe a cyfrowy wymiar nowej mobilności

2

Bezpieczeństwo narodowe a cyfrowy wymiar nowej mobilności

Nowa mobilność i kształtujące ją ramy regulacyjne przestają być wyłącznie domeną bezpieczeństwa ruchu drogowego. Coraz wyraźniej stają się elementem polityki bezpieczeństwa państwa, suwerenności technologicznej oraz konkurencyjności gospodarki.

Chiny, Stany Zjednoczone i Unia Europejska wchodzą tym samym w etap rywalizacji o standardy cyberbezpieczeństwa inteligentnych pojazdów. Przyjmowane regulacje będą odgrywają kluczową rolę zarówno w zapewnieniu ochrony wrażliwych danych, jak i w kształtowaniu pozycji poszczególnych gospodarek na globalnym rynku motoryzacyjnym.

Chiny

Chińska Republika Ludowa (ChRL) zajmuje wiodące miejsce na globalnej mapie rozwoju nowej mobilności. Chiny prowadzą ambitną politykę nie tylko w zakresie innowacji, lecz także regulacji. Dotychczas opracowały jedne z najbardziej zaawansowanych przepisów administracyjnych oraz systemów standaryzacji technicznej dotyczących inteligentnych samochodów.

Zaawansowanie regulacyjne Chin wynika z faktu, że nowa mobilność została od początku powiązana nie tylko z rozwojem rynku motoryzacyjnego, lecz także z budową przewag technologicznych i odpowiedzią na zagrożenia z zakresu cyberbezpieczeństwa i bezpieczeństwa danych. Aparat państwowo-partyjny ChRL postrzega nową mobilność jako sektor strategiczny. Świadczy o tym wpisanie inteligentnych pojazdów oraz inteligentnego transportu do strategicznych dokumentów, tj. „Made in China 2025" oraz XIV planu pięcioletniego ChRL na lata 2021–2025.

Logika regulacyjna ChRL wskazuje, że władze postrzegają inteligentne samochody zarówno jako źródło strategicznych szans, jak i potencjalnych zagrożeń dla bezpieczeństwa państwa. Z perspektywy ChRL przykładem takiej szansy jest rozwijanie wspólnych cywilno-wojskowych projektów badawczych dotyczących inteligentnych pojazdów. Wpisuje się to w realizowaną w ChRL koncepcję fuzji cywilno-wojskowej, w ramach której łączy się sektor technologii cywilnych i wojskowych. Reprezentatywnym przykładem jest system nawigacji satelitarnej BeiDou, wykorzystywany zarówno w cywilnej nawigacji samochodowej, jak i przez Armię Ludowo-Wyzwoleńczą, m.in. naprowadzania amunicji precyzyjnej. Jednocześnie dokumenty państwowe

ChRL wskazują, że rozwojowi inteligentnych pojazdów towarzyszy rosnąca skala zagrożeń, takich jak cyberataki, w tym zdalne przejęcie kontroli nad pojazdem, a także gromadzenie wrażliwych danych geoprzestrzennych, np. informacji o natężeniu ruchu wokół obiektów wojskowych i budynków rządowych, oraz danych osobowych, w tym danych biometrycznych.

Chińskie organy państwowe uznają inteligentne samochody za technologię o charakterze przełomowym, której dynamiczny rozwój wymaga systematycznego dostosowywania ram regulacyjnych – nie jest bowiem możliwe jej uregulowanie w sposób definitywny. Obowiązujące ustawy tworzą podstawę tego systemu, stopniowo uzupełnianą przez regulacje administracyjne i standardy techniczne, które pozwalają na wypracowywanie szczegółowych rozwiązań. Taka konstrukcja umożliwia aparatowi państwowo-partyjnemu relatywnie szybkie reagowanie na zmiany technologiczne zachodzące w sektorze nowej mobilności.

Proces rozwoju tych ram jest koordynowany przez Ministerstwo Przemysłu i Technologii Informacyjnych oraz Państwową Komisję Standaryzacyjną ChRL. W ramach systemu standaryzacji funkcjonuje Państwowa Komisja Techniczna ds. Standaryzacji Motoryzacji, a w jej strukturze — Podkomisja ds. Pojazdów Inteligentnych i Połączonych z Siecią TC114/SC34. Ważną rolę odgrywają również władze lokalne (np. miasta Shenzhen – obszar pilotażowy dla wdrażania i regulowania samochodów autonomicznych w ChRL), które opracowują regionalne standardy techniczne.

Podstawę prawną chińskiego systemu stanowią trzy akty: Ustawa o cyberbezpieczeństwie ChRL z 2017 r., Ustawa o bezpieczeństwie danych z 2021 r. oraz Ustawa o ochronie danych osobowych ChRL z 2021 r. Regulacje te nakładają na producentów szereg obowiązków, obejmujących przede wszystkim przechowywanie kluczowych danych wyłącznie na terytorium Chin. Ich transfer za granicę wymaga zgody Państwowej Administracji ds. Cyberprzestrzeni. Egzekwowanie tego rodzaju wymogów jest co do zasady możliwe głównie w warunkach chińskich, gdzie internet funkcjonuje jako zamknięty i cenzurowany ekosystem, a przepływ danych podlega szeroko zakrojonej kontroli aparatu państwowo-partyjnego. Producenci samochodów inteligentnych są również zobowiązani do wdrażania systemów zarządzania bezpieczeństwem, klasyfikowania danych według ich znaczenia – w tym dla bezpieczeństwa państwa – a także przeprowadzania ocen ryzyka i przekazywania stosownych raportów organom regulacyjnym.

Trajektoria wdrażania chińskich regulacji wskazuje na stopniowe przechodzenie od ogólnych dokumentów strategicznych do coraz bardziej egzekwowalnych instrumentów nadzoru. Narzędziami tymi są przede wszystkim standardy techniczne i system certyfikacji bezpieczeństwa danych inteligentnych pojazdów. Wśród tych pierwszych na szczególną uwagę zasługują dwa rozwiązania. Pierwszym z nich jest wyposażenie inteligentnych samochodów w tryb umożliwiający zatrzymanie gromadzenia danych z otoczenia pojazdu poprzez wyłączenie czujników, kamer, radarów i innych urządzeń rejestrujących. Tryb ten ma być uruchamiany jednym kliknięciem. Jego aktywacja powinna być obowiązkowo sygnalizowana na zewnątrz samochodu, m.in. na potrzeby służb zarządzających obszarami wrażliwymi.

Drugim rozwiązaniem jest zaś klasyfikowanie danych gromadzonych przez inteligentne pojazdy według poziomu ich znaczenia i potencjalnego wpływu na bezpieczeństwo państwa. System obejmuje cztery kategorie – najważniejszą z nich są dane najwyższej wagi, których wyciek mógłby stanowić poważne zagrożenie dla bezpieczeństwa państwa. Zalicza się do nich m.in. mapy obszarów

wrażliwych, informacje o natężeniu ruchu wokół stref wojskowych i instytucji rządowych oraz rozległe zbiory danych osobowych. Oprócz tego od 2024 r. rozwijany jest system certyfikacji bezpieczeństwa danych, prowadzony przez Chińskie Stowarzyszenie Producentów Samochodów oraz Państwowe Centrum Koordynacji Zespołów Technicznych ds. Reagowania na Sytuacje Kryzysowe w Sieci Komputerowej ChRL. Testy obejmują m.in. anonimizację wizerunków twarzy i tablic rejestracyjnych, zakaz bezpośredniego przekazywania danych osobowych za granicę, domyślne niegromadzenie danych z kabiny pojazdu, realizację obowiązków informacyjnych wobec użytkowników oraz ocenę adekwatności jakości danych do funkcji pojazdu.

Certyfikacja bezpieczeństwa danych inteligentnych pojazdów jest formalnie dobrowolna i dostępna zarówno dla producentów chińskich, jak i zagranicznych. Praktyka pokazuje jednak, że może stanowić także nieformalny instrument dostępu do rynku. Reprezentatywnym przykładem jest Tesla. Jest to pierwszy zagraniczny (amerykański) producent, który uzyskał pozytywną ocenę zgodności z chińskimi wymogami bezpieczeństwa danych. Przed jej uzyskaniem pojazdy Tesli podlegały nieformalnym ograniczeniom dotyczącym poruszania się i parkowania w pobliżu obiektów uznawanych za istotne z punktu widzenia bezpieczeństwa państwa. Obejmowały one m.in. instytucje rządowe, obiekty wojskowe i lotniska, a także miejsca organizacji wydarzeń z udziałem najważniejszych przedstawicieli Komunistycznej Partii Chin, w tym Xi Jinpinga. Dopiero uzyskanie certyfikacji bezpieczeństwa danych umożliwiło Tesli swobodniejsze funkcjonowanie na chińskim rynku.

USA

Podejście USA do nowej mobilności opiera się na połączeniu logiki bezpieczeństwa narodowego z pozostawieniem sektorowi prywatnemu wiodącej roli w rozwoju technologii. Waszyngton jako pierwszy uznał, że inteligentne pojazdy – w szczególności ich systemy łączności i automatyzacji jazdy – stanowią źródło zagrożeń wywiadowczych i cybernetycznych.

Główny nurt regulacyjny zmierza więc do wykluczania z rynku rozwiązań i podmiotów powiązanych z państwami uznawanymi w ramach klauzuli bezpieczeństwa narodowego za adwersarzy USA, w szczególności Chin i Rosji.

Znaczenie cyberbezpieczeństwa inteligentnych samochodów w polityce USA potwierdza przyjęcie przez Joe Bidena rygorystycznych regulacji w tym obszarze i utrzymanie ich w mocy nawet po zmianie administracji w Białym Domu. Zakazy te dotyczą oprogramowania systemów łączności i automatyzacji jazdy, a także sprzedaży pojazdów przez producentów kontrolowanych przez Chiny lub Rosję. Mają one wejść w życie stopniowo od roku modelowego 2027 i 2030.

Amerykański system regulacyjny dla nowej mobilności pozostawia jednak Departamentowi Handlu szeroką swobodę w różnicowaniu dostępu przedsiębiorstw do rynku. Obok generalnych ograniczeń przewiduje bowiem możliwość uzyskania indywidualnej autoryzacji wydawanej przez Biuro Przemysłu i Bezpieczeństwa (BIS). Dobrze ilustrują przypadki Volvo i Polestara – obie marki są powiązane kapitałowo z chińskim koncernem Geely, lecz władze USA potraktowały je odmiennie. Po rozmowach dotyczących m.in. stosowanych technologii i bezpieczeństwa danych Volvo uzyskało od BIS indywidualną zgodę na dalszy import i sprzedaż samochodów na rynku amerykańskim.

Miesiąc później analogicznej zgody nie otrzymał jednak Polestar, a oficjalnych powodów decyzji nie ujawniono.

Obowiązujące regulacje skłaniają przedsiębiorstwa do przenoszenia wrażliwych elementów technologicznych i kontroli nad danymi do USA, ale nie muszą prowadzić do całkowitego zerwania powiązań z chińskim przemysłem. Dobrze obrazuje to partnerstwo Waymo z należącą do Geely marką Zeekr przy budowie robotaksówki Waymo Ojai. Strona chińska dostarcza produkowaną w ChRL bazową platformę pojazdu, natomiast Waymo integruje i testuje w zakładzie w Mesa w Arizonie własny system autonomicznej jazdy, w tym sensory i oprogramowanie.

Obecnie w Kongresie trwają prace nad Connected Vehicle Security Act of 2026. Dokument ten miałby nadać rangę ustawową rozwiązaniom przyjętym pod koniec administracji Bidena oraz istotnie rozszerzyć ich zakres. Projekt obejmuje nie tylko Chiny i Rosję, lecz także Iran i Koreę Północną. Od 2027 r. zakazany byłyby import, produkcja, sprzedaż, odsprzedaż i wprowadzanie do obrotu pojazdów pochodzących z tych państw lub w nich zaprojektowanych, a także integrowanie w samochodach objętego ustawą oprogramowania. Od 2030 r. analogiczne restrykcje dotyczyłyby sprzętu systemów łączności. Zakaz miałby obejmować również producentów pojazdów, w których podmioty z wymienionych państw posiadają łącznie ponad 15% udziałów, praw głosu, reprezentacji w organach spółki lub innych form kontroli. To właśnie próg własnościowy budzi najwięcej kontrowersji – mógłby bowiem objąć przedsiębiorstwa spoza państw uznawanych za adwersarzy USA, jeżeli posiadają znaczących chińskich udziałowców (np. Mercedes Benz). Zanim stanie się obowiązującym prawem projekt musi jednak zostać przyjęty przez obie izby Kongresu i podpisany przez prezydenta. Przyjęcie aktu oznaczałoby trwałe wpisanie geopolitycznej selekcji dostępu do rynku w ramy amerykańskiego prawa federalnego i utrudniłoby ich zmianę przez przyszłych prezydentów.

Unia Europejska

Obecny system regulacyjny Unii Europejskiej dla pojazdów został zaprojektowany przede wszystkim z myślą o bezpieczeństwie drogowym, a nie cyfrowym. Wraz z postępującym ucyfrowieniem motoryzacji coraz wyraźniejsza staje się jednak potrzeba dostosowania ram prawnych UE do szans i zagrożeń związanych z nową mobilnością.

W kształtowanie unijnego podejścia do nowej mobilności zaangażowanych jest wiele instytucji reprezentujących odmienne perspektywy regulacyjne i gospodarcze: Dyrekcja Generalna ds. Rynku Wewnętrznego, Przemysłu, Przedsiębiorczości i MŚP (DG GROW), Dyrekcja Generalna ds. Mobilności i Transportu (DG MOVE), Dyrekcja Generalna ds. Handlu i Bezpieczeństwa Gospodarczego (DG TRADE), Dyrekcja Generalna ds. Sieci Komunikacyjnych, Treści i Technologii (DG CNECT), Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), a także Parlament Europejski. Rozproszenie kompetencji odzwierciedla przekrojowy charakter problemu: inteligentny pojazd jest nie tylko środkiem transportu, ale też produktem cyfrowym, a nawet częścią infrastruktury energetycznej. W praktyce wielość zaangażowanych instytucji utrudnia jednak koordynację działań regulacyjnych.

Unijny system regulacji dotyczących cyberbezpieczeństwa i bezpieczeństwa danych w inteligentnych pojazdach ma wciąż charakter fragmentaryczny – nie istnieje jeden kompleksowy akt obejmujący cały cykl ich funkcjonowania. Obowiązki producentów i operatorów są rozproszone między przepisy homologacyjne, międzynarodowe regulaminy techniczne oraz horyzontalne regulacje dotyczące technologii cyfrowych.

Fundamentem unijnego modelu dopuszczania samochodów do obrotu pozostaje procedura homologacji typu pojazdu, określona w obowiązującym od 2020 r. rozporządzeniu (UE) 2018/858. Na jego podstawie właściwy organ krajowy sprawdza, czy dany model pojazdu, system lub komponent spełnia unijne wymagania. Homologacja wydana przez jedno państwo członkowskie jest następnie uznawana w całej Unii. Z jednego strony zapewnia to spójne funkcjonowanie wspólnego rynku, ale z drugiej sprawia, że jakość kontroli przeprowadzonej przez jeden organ krajowy ma konsekwencje dla bezpieczeństwa całego rynku unijnego. System homologacyjny uzupełnia rozporządzenie (UE) 2019/2144, które wprowadza obowiązkowe zaawansowane systemy wspomagania kierowcy oraz tworzy podstawę prawną do określania szczegółowych wymogów homologacyjnych dla pojazdów zautomatyzowanych i w pełni zautomatyzowanych. Włącza ono do unijnego systemu homologacji wymagania wynikające z regulaminów ONZ nr 155, 156 i 157: dot. homologacji pojazdów w zakresie cyberbezpieczeństwa oraz systemu zarządzania cyberbezpieczeństwem, aktualizacji oprogramowania i systemu zarządzania nimi, a także automatycznego systemu utrzymania pasa ruchu.

Nowa mobilność podlega również unijnym regulacjom cyfrowym, które nie zostały stworzone wyłącznie z myślą o sektorze motoryzacyjnym, lecz istotnie wpływają na jego funkcjonowanie. Przykładowo UE dysponuje jednymi z najbardziej rygorystycznych na świecie mechanizmów ochrony danych osobowych. RODO znajduje zatem zastosowanie także do danych gromadzonych i przetwarzanych przez inteligentne samochody (w tym danych lokalizacyjnych i biometrycznych oraz informacji dotyczących kierowców i pasażerów). Na poziomie unijnym nie istnieją jednak analogiczne ramy regulujące gromadzenie i przetwarzanie danych geoprzestrzennych, co w kontekście nowej mobilności stanowi istotną lukę. Inteligentnych pojazdów dotyczy również dyrektywa NIS2, ustanawiająca podstawowe techniczne, operacyjne i organizacyjne obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa. Obejmuje ona podmioty działające m.in. w sektorach produkcji pojazdów, transportu i inteligentnej infrastruktury drogowej, telekomunikacji (w tym sieci 5G i łączności satelitarnej) oraz energetyki. Istotne znaczenie ma również Akt w sprawie danych, który wskazuje pojazdy jako jedną z kluczowych kategorii produktów skomunikowanych oraz reguluje dostęp organów publicznych państw trzecich do danych i zasady ich międzynarodowego przekazywania. Na jego mocy zakazane jest przekazywanie takich danych lub udostępnianie ich organom zagranicznym, jeżeli byłoby to sprzeczne z prawem Unii Europejskiej lub prawem państw członkowskich, z wyjątkiem przypadków objętych odpowiednimi umowami międzynarodowymi. Ponadto mający wejść w życie w pełni w sierpniu 2027 r. Akt w sprawie sztucznej inteligencji wiąże homologację pojazdów z wymaganiami dotyczącymi systemów AI pełniących funkcje związane z bezpieczeństwem (m.in. w zakresie zarządzania ryzykiem, zapewnienia odpowiedniej jakości danych, przejrzystości działania, nadzoru człowieka, a także cyberbezpieczeństwa).

UE coraz trafniej identyfikuje szanse i zagrożenia związane z nową mobilnością. Potwierdza to opublikowana pod koniec stycznia br. ocena ryzyka dotyczącego inteligentnych samochodów, wraz z zestawem narzędzi ICT Supply Chain Toolbox, opracowana przez państwa członkowskie i DG CONNECT. Dokument identyfikuje kluczowe scenariusze ryzyk związanych z nową mobilnością i wskazuje na pilną potrzebę wypełnienia luki regulacyjnej między tradycyjnym systemem homologacji a nowymi zagrożeniami cyfrowymi.

Zagrożenia w zakresie cyberbezpieczeństwa inteligentnych pojazdów mogą być ograniczane w ramach planowanej rewizji Aktu o cyberbezpieczeństwie. Obecna wersja dokumentu obejmuje inteligentne pojazdy, choć zaprezentowane w niej rozwiązania nie dotyczyłyby bezpośrednio samochodów konsumenckich, lecz jedynie podmiotów objętych dyrektywą NIS2. Przełomem w ramach rewizji tego aktu byłoby wprowadzenie rozwiązań pozwalających ograniczać zagrożenia związane z tzw. dostawcami wysokiego ryzyka – ocena takich dostawców uwzględniałaby nie tylko ryzyka techniczne, lecz także otoczenie prawne, organizacyjne i geopolityczne producenta. Nie wyznaczono ostatecznego terminu zakończenia prac nad rewizją aktu, ale jego kształt będzie miał istotny wpływ na kształt nowej mobilności w UE.

Kontekst geopolityczny

Nowa mobilność a zagrożenia wywiadowcze

Rozwój nowej mobilności rodzi szereg zagrożeń wywiadowczych wynikających z możliwości ekspansywnego zbierania wrażliwych danych przez ucyfrowione samochody. Dotyczy to w szczególności:

→ danych geoprzestrzennych (np. danych o infrastrukturze krytycznej, budynkach rządowych, strefach wojskowych),

→ danych osobowych (np. danych biometrycznych kierowcy),

→ analizy dużych zbiorów danych pozwalającej np. na szacowanie natężenia ruchu w pobliżu jednostek wojskowych i wykorzystywanie tych danych jako wskaźników aktywności gospodarczej.

Badania przeprowadzone w ramach norweskiego projektu Lion Cage wskazują, że przepływ danych do i z chińskich samochodów elektrycznych stanowi istotne źródło ryzyka. Z analizy wynika, że około 90% komunikacji wychodzącej z chińskiego samochodu elektrycznego użytkowanego na terenie Norwegii – obejmującej m.in. polecenia głosowe kierowcy oraz dane dotyczące lokalizacji pojazdu – było przesyłane na serwery zlokalizowane w Chinach. Stwarza to wyraźną potrzebę rygorystycznej kontroli ucyfrowionych pojazdów, m.in. pod kątem skanowania infrastruktury krytycznej za pomocą ich sensorów oraz gromadzenia wrażliwych informacji. Szereg państw, w tym m.in. Polska, USA, Izrael, Wielka Brytania i Czechy podjęły już działania mające na celu ochronę stref wojskowych przed gromadzeniem wrażliwych danych przez ucyfrowione pojazdy.

3 Potencjał Polski w łańcuchu wartości cyberbezpieczeństwa

3

Potencjał Polski w łańcuchu wartości cyberbezpieczeństwa

Polska to jeden z największych ośrodków przemysłu motoryzacyjnego w Unii Europejskiej. W 2024 r. z polskich fabryk wyjechało ponad 600 tys. pojazdów, a łączna wartość eksportu krajowego sektora automotive wynosi niemal 33 mld euro. Jednocześnie motoryzacja jest filarem gospodarki Polski. Sektor kreuje ponad 220 tys. miejsc pracy, a jego udział w PKB przekracza 8%.

Postępująca transformacja to dla polskiego przemysłu motoryzacyjnego poważne wyzwanie. Obrazuje to systematyczny spadek wolumenu produkowanych w Polsce samochodów spalinowych: z rekordowych 840 tys. w 2008 r. do zaledwie 101 tys. w roku 2025. Ustępujące technologie są jednak zastępowane nowymi rozwiązaniami, co kreuje nowe przestrzenie w łańcuchach dostaw. W konsekwencji rozwój nowej mobilności to historyczna szansa na wzmocnienie polskiej gospodarki poprzez budowę kompetencji w perspektywicznych obszarach, takich jak pojazdy elektryczne, innowacyjne systemy bateryjne czy cyberbezpieczeństwo.

Na podstawie prognoz, globalne wydatki na rozwiązania z zakresu cyberbezpieczeństwa już do 2029 r. przekroczą 300 mld dolarów. Wzmocnienie krajowych kompetencji umożliwi polskim interesariuszom zdobycie istotnego udziału w tych zasobach kapitałowych.

Polska dysponuje unikalną kombinacją aktywów, które – właściwie ukierunkowane polityką publiczną i strategią sektora prywatnego – mogą przełożyć się na wypracowanie trwałych przewag konkurencyjnych w dziedzinie cyberbezpieczeństwa nowej mobilności. Należy do nich:

Rozwijający się sektor IT i cybersecurity

→ Ponad 600 000 specjalistów IT

→ Centra R&D globalnych liderów technologicznych

Silny sektor automotive

→ Polska jest jednym z największych dostawców podzespołów motoryzacyjnych w Unii Europejskiej – wartość eksportu w tym obszarze wynosi 18 mld EUR

→ Sektor motoryzacyjny odpowiadający za ponad 11% polskiej produkcji przemysłowej

Silne zaplecze akademickie i R&D

→ Renomowane uczelnie techniczne, w tym Politechnika Gdańska, Warszawska, Wrocławska czy AGH

→ NCBR oraz jednostki Sieci Badawczej Łukasiewicz

Strategiczna pozycja geopolityczna

→ Położenie na wschodniej flance UE oraz NATO czyni z Polski naturalne centrum kompetencji dla cyfrowych rozwiązań bezpieczeństwa nowej mobilności

Dynamiczny rozwój nowej mobilności w wymiarze rynkowym i przemysłowym

→ Prognozy szybkiego wzrostu rejestracji samochodów elektrycznych – z ok. 52 tys. szt. w 2025 r. do nawet 188 tys. w roku 2030

→ Znaczny potencjał produkcyjny – silna pozycja w łańcuchu dostaw sektora bateryjnego oraz plany uruchomienia hubu nowej mobilności w Jaworznie

Wzrost potencjału Polski w cyberbezpieczeństwie nowej mobilności powinien zostać zaadresowany poprzez połączenie kompetencji w obszarze IT, automotive, elektromobilności, energetyki, badań, homologacji, certyfikacji i oceny zgodności.

Obecną wartość ekosystemu rozwiązań cyberbezpieczeństwa w Polsce szacuje się na kilkanaście miliardów złotych. Nowa mobilność łączy dwa obszary, w których Polska ma silną pozycję: motoryzację i sektor technologii cyfrowych. Budowa kompetencji na ich styku pozwala tworzyć wyżej marżowe usługi, takie jak badania odporności, audyty, walidacja i ocena zgodności, które można eksportować na rynek europejski.

Polska dysponuje rozbudowanym zapleczem instytucjonalnym w obszarze cyberbezpieczeństwa i sztucznej inteligencji, które można ukierunkować na potrzeby nowej mobilności. Tworzą je jednostki operacyjne krajowego systemu cyberbezpieczeństwa, instytuty badawcze, w tym jednostki Sieci Badawczej Łukasiewicz, oraz silne ośrodki akademickie. Współczesne cyberbezpieczeństwo wymaga łączenia kompetencji z wielu dziedzin: informatyki, motoryzacji, energetyki, prawa i badań stosowanych. Jednostki R&D są naturalnym miejscem takiej integracji, ponieważ dysponują zapleczem laboratoryjnym i zdolnością prowadzenia badań w warunkach zbliżonych do rzeczywistej eksploatacji.

Jedną z przewag Polski może być zdolność do prowadzenia badań i walidacji systemów w warunkach zbliżonych do rzeczywistej eksploatacji. Polska może budować pozycję w europejskim sektorze cyberbezpieczeństwa poprzez wyspecjalizowane usługi testowe, audytowe, homologacyjne i eksperckie dla pojazdów, komponentów, infrastruktury ładowania oraz systemów cyfrowych nowej mobilności. Przykładem instytucji dysponujących potencjałem do wniesienia swoich kompetencji do tego łańcucha jest Łukasiewicz – PIMOT posiadający doświadczenie w badaniach pojazdów, technologii transportowych, elektromobilności, ocenie technicznej i procesach homologacyjnych. W ujęciu systemowym otwiera to możliwość wspierania producentów, dostawców, operatorów infrastruktury i administracji w tworzeniu metodyk badawczych, programów pilotażowych, procedur walidacji, zaplecza laboratoryjnego i rekomendacji regulacyjnych. Taki kierunek wzmacnia bezpieczeństwo państwa, zwiększa odporność przemysłu oraz tworzy nowe obszary specjalizacji eksportowej polskich instytucji R&D.

Położenie Polski na wschodniej flance Unii Europejskiej i NATO wiąże się z największą w Europie ekspozycją na zagrożenia zewnętrzne. Ta sama okoliczność jest jednak źródłem przewagi. Polskie instytucje odpowiedzialne za cyberbezpieczeństwo działają w warunkach stałej presji, co przekłada się na doświadczenie operacyjne trudne do zdobycia w spokojniejszym otoczeniu. Kompetencje wypracowane w obronie infrastruktury krytycznej, w tym energetycznej i transportowej, mogą stać się przedmiotem współpracy i usług oferowanych partnerom europejskim. Budowa krajowego zaplecza badań, walidacji i oceny zgodności zmniejsza zależność od zagranicznych ośrodków certyfikacji i wzmacnia suwerenność technologiczną państwa w obszarze, który łączy bezpieczeństwo, gospodarkę i obronność.

Źródło: Sieć Badawcza Łukasiewicz - Przemysłowy Instytut Motoryzacji

4 Jak przekształcić Polskę w europejski hub cyberbezpieczeństwa nowej mobilności?

4

Jak przekształcić Polskę w europejski hub cyberbezpieczeństwa nowej mobilności?

Rekomendacje dla interesariuszy publicznych, nauki i instytucji R&D

Wdrożenie zachęt sprzyjających lokowaniu w Polsce inwestycji budujących kompetencje w obszarze cyberbezpieczeństwa nowej mobilności

ADRESACI
Administracja centralna, jednostki samorządu terytorialnego, specjalne strefy ekonomiczne, instytucje odpowiedzialne za politykę inwestycyjną i przemysłową, przemysł

GENEZA
Właściwi interesariusze powinni wdrażać zachęty regulacyjne, finansowe oraz systemowe sprzyjające lokowaniu w Polsce inwestycji, które poskutkują wzrostem zdolności produkcyjnych oraz kompetencji R&D w dziedzinie cyberbezpieczeństwa nowej mobilności

EFEKT
Wzmocnienie pozycji Polski w łańcuchu wartości AI i nowej mobilności, zwiększenie suwerenności technologicznej

Stworzenie programu skalowania polskich technologii cyberbezpieczeństwa dla sektora mobilności

ADRESACI
Administracja centralna, instytucje finansujące R&D, przemysł, spółki Skarbu Państwa, fundusze inwestycyjne

GENEZA
Konieczność stworzenia mechanizmu przeprowadzania technologii od badań i demonstratorów do certyfikowanych produktów, pierwszych wdrożeń i skalowania na rynku krajowym oraz rynkach zagranicznych

EFEKT
Wzrost wdrożeń polskich produktów i technologii z obszaru cyberbezpieczeństwa i nowej mobilności przez odbiorców branżowych w Polsce i Europie, rozwój krajowych scale-upów oraz zwiększenie udziału Polski w europejskim łańcuchu wartości sektora motoryzacyjnego

Rozwój w Polsce infrastruktury AI dla przemysłu, mobilności i cyberbezpieczeństwa

ADRESACI
Administracja centralna, jednostki techniczne i laboratoria badawcze, przemysł

GENEZA
Polska powinna inwestować w infrastrukturę umożliwiającą trenowanie, dostrajanie i wdrażanie zaawansowanych modeli AI, stanowiącą jednocześnie zaplecze dla strategicznych zastosowań przemysłowych.

EFEKT
Wzmocnienie pozycji Polski w łańcuchu wartości AI i nowej mobilności, przejście polskich przedsiębiorstw od roli użytkownika gotowych technologii do roli twórcy i integratora zaawansowanych rozwiązań, zwiększenie suwerenności technologicznej

Utworzenie krajowego programu kompetencji w zakresie cyberbezpieczeństwa nowej mobilności

ADRESACI
Administracja centralna, NASK, Sieć Badawcza Łukasiewicz, uczelnie, instytucje R&D, przemysł

GENEZA
Cyberbezpieczeństwo nowej mobilności wymaga połączenia kompetencji automotive, IT, energetyki, regulacji i badań

EFEKT
Integracja kompetencji, rozwój kadr i powstanie rozpoznawalnego ekosystemu eksperckiego

Rozwój krajowych laboratoriów i metodyk badania cyberodporności pojazdów oraz infrastruktury ładowania

ADRESACI
Administracja centralna, instytucje R&D, jednostki techniczne, przemysł

GENEZA
Bez krajowego zaplecza badawczego Polska pozostanie odbiorcą zagranicznych certyfikatów i standardów

EFEKT
Zwiększenie suwerenności technologicznej, wsparcie dla polskich przedsiębiorstw i możliwość świadczenia usług dla rynku europejskiego

Opracowanie krajowych wytycznych dla operatorów infrastruktury ładowania i flot pojazdów elektrycznych

ADRESACI
Administracja centralna, regulatorzy, operatorzy infrastruktury ładowania, operatorzy transportu publicznego i flot komercyjnych

GENEZA
Infrastruktura ładowania staje się elementem o znaczeniu krytycznym dla mobilności i energetyki

EFEKT
Ujednolicenie wymagań, zwiększenie odporności operacyjnej i ograniczenie ryzyka fragmentarycznych praktyk bezpieczeństwa

Uruchomienie krajowego programu badań odporności systemów sztucznej inteligencji stosowanych w mobilności

ADRESACI
Instytucje R&D, jednostki techniczne i laboratoria, administracja centralna, przemysł

GENEZA
Systemy AI w percepcji i sterowaniu wprowadzają nową klasę podatności, w tym ataki adwersaryjne i zatruwanie danych, a AI Act nakłada wymogi odporności na systemy wysokiego ryzyka. Program badań, w tym testów typu red-teaming, uzupełnia rozwijane w kraju zaplecze badań pojazdów i infrastruktury

EFEKT
Krajowa zdolność weryfikacji odporności modeli, wsparcie producentów w spełnianiu wymogów oraz nowa specjalizacja badawcza o potencjale eksportowym

Ustanowienie piaskownicy regulacyjnej (regulatory sandbox) dla integracji ładowania i usług V2G z systemem elektroenergetycznym

ADRESACI
Administracja publiczna, regulatorzy energii, operatorzy systemów, instytucje R&D, przedsiębiorstwa

GENEZA
Technologie V2G i smart charging rozwijają się szybciej niż ramy nadzoru nad ich bezpieczeństwem, a testowanie rozwiązań w warunkach rzeczywistych wymaga kontrolowanego środowiska

EFEKT
Bezpieczne testowanie modeli integracji z siecią, wypracowanie wymagań i dobrych praktyk przed skalowaniem oraz wzmocnienie pozycji polskich podmiotów w tym segmencie rynku

Zobowiązanie producentów samochodów do uzyskania dodatkowej standaryzacji/homologacji bezpieczeństwa danych i cyberbezpieczeństwa na poziomie Unii Europejskiej

ADRESACI
Instytucje Unii Europejskiej

GENEZA
Konieczność ograniczenia ryzyka sprowadzenia UE do roli rynku zbytu lub montowni produktów projektowanych i kontrolowanych w innych regionach świata.

EFEKT
Podniesienie poziomu ochrony na jednolitym rynku, sprzyjające przejmowaniu know-how i zatrzymywaniu większej części wartości dodanej w Europie. Ustanowienie skutecznej bariery pozataryfowej wspierającej rozwój bezpiecznego sektora oprogramowania samochodowego, sensorów i usług cyfrowych.

Skuteczna komunikacja adresowana do konsumentów na temat zagrożeń związanych z cyberbezpieczeństwem i bezpieczeństwem danych nowej mobilności

ADRESACI
Administracja, regulatorzy energii, operatorzy systemów, instytucje B+R, przedsiębiorstwa

GENEZA
Niska świadomość społeczna w dziedzinie zagrożeń związanych z cyberbezpieczeństwem nowej mobilności

EFEKT
Wsparcie odpowiedzialnych decyzji konsumentów zarówno przy wyborze, jak i użytkowaniu pojazdu przy jednoczesnym ograniczeniu ich oporu wobec wprowadzania nowych regulacji na poziomie unijnym i krajowym

Utrzymanie ucyfrowionych pojazdów wśród technologii objętych nowelizacją unijnego Aktu o Cyberbezpieczeństwie

ADRESACI
Instytucje Unii Europejskiej

GENEZA
Rosnące ucyfrowienie pojazdów zwiększa ich znaczenie w odniesieniu do cyberbezpieczeństwa i ochrony danych

EFEKT
Objęcie podmiotów podlegających dyrektywie NIS2 spójnymi na poziomie UE mechanizmami oceny i certyfikacji cyberbezpieczeństwa, ograniczenie ryzyka niekontrolowanego przepływu danych, pozyskiwania nieautoryzowanego, zdalnego dostępu do pojazdów, jak również redukcja podatności oprogramowania i łańcucha dostaw

Wzmocnienie ochrony infrastruktury krytycznej i obiektów o znaczeniu strategicznym przed zagrożeniami wywiadowczymi wynikającymi z wykorzystania ucyfrowionych pojazdów

ADRESACI
Państwa członkowskie UE, instytucje odpowiedzialne za bezpieczeństwo i obronność

GENEZA
Ucyfrowione pojazdy umożliwiają ekspansywne zbieranie wrażliwych danych geoprzestrzennych (m.in. o infrastrukturze krytycznej, strefach wojskowych, budynkach rządowych,) a także osobowych (m.in. danych biometrycznych kierowcy i tras przejazdu) mogących mieć wartość wywiadowczą i wspierać rozpoznanie wrażliwych elementów infrastruktury oraz szacowanie natężenia ruchu np. w pobliżu obiektów wojskowych

EFEKT
Ograniczenie możliwości nieuprawnionego pozyskiwania danych o miejscach lub strefach wrażliwych dla bezpieczeństwa państwa, wzmocnienie odporności państwa na działania wywiadowcze i hybrydowe, zwiększenie bezpieczeństwa infrastruktury krytycznej

Rekomendacje dla dostawców i uczestników rynku nowej mobilności

Wdrożenie podejścia „cybersecurity by design" w pojazdach, komponentach i infrastrukturze ładowania

ADRESACI
Producenci pojazdów, dostawcy komponentów, operatorzy infrastruktury ładowania, dostawcy oprogramowania

GENEZA
Podatności powstają często na etapie projektowania i integracji, a ich usunięcie po wdrożeniu jest kosztowne

EFEKT
Ograniczenie ryzyka incydentów, łatwiejsze spełnienie wymagań regulacyjnych i wzrost zaufania klientów

Regularne testowanie i walidacja cyberbezpieczeństwa pojazdów, komponentów i infrastruktury ładowania

ADRESACI
Producenci, dostawcy, operatorzy infrastruktury ładowania, jednostki techniczne i laboratoria badawcze

GENEZA
Szybki rozwój oprogramowania, aktualizacji OTA, usług chmurowych i komunikacji V2X/V2G wymaga ciągłej weryfikacji odporności

EFEKT
Wcześniejsze wykrywanie podatności, ograniczenie kosztów incydentów i poprawa jakości produktów

Wzmocnienie bezpieczeństwa łańcucha dostaw sektora automotive i elektromobilności

ADRESACI
OEM, dostawcy Tier 1–3, producenci systemów bateryjnych, dostawcy oprogramowania i usług chmurowych

GENEZA
Końcowe bezpieczeństwo produktu zależy od jakości komponentów i procesów u wielu podwykonawców

EFEKT
Zwiększenie odporności przemysłu, lepsza pozycja polskich dostawców w globalnych łańcuchach wartości i ograniczenie ryzyka przerw produkcyjnych

Wdrożenie oceny skutków dla ochrony danych (DPIA) i minimalnych standardów prywatności w platformach mobilności i usługach ładowania

ADRESACI
Operatorzy platform MaaS i współdzielenia pojazdów, operatorzy infrastruktury ładowania, dostawcy aplikacji mobilnych

GENEZA
Usługi nowej mobilności przetwarzają dane lokalizacyjne, płatnicze i behawioralne, a ochrona danych bywa uwzględniana po wdrożeniu, nie na etapie projektu

EFEKT
Ograniczenie ryzyka wycieków, wcześniejsze wykrywanie ryzyk w architekturze usług oraz spójny poziom ochrony prywatności użytkowników na rynku

Uwzględnienie wymagań cyberbezpieczeństwa technologii operacyjnych (OT) w umowach o przyłączenie i świadczenie usług sieciowych

ADRESACI
Operatorzy systemów dystrybucyjnych, operatorzy infrastruktury ładowania, agregatorzy, dostawcy usług bilansujących

GENEZA
Integracja ładowania i usług V2G z siecią tworzy sterowane zdalnie obciążenie o znaczeniu dla stabilności systemu elektroenergetycznego, a wymagania bezpieczeństwa OT nie zawsze są elementem relacji umownych

EFEKT
Ograniczenie ryzyka skoordynowanej manipulacji poborem mocy, jasny podział odpowiedzialności za bezpieczeństwo oraz wzrost odporności lokalnych elementów sieci

Utworzenie sektorowego ośrodka wymiany informacji o zagrożeniach (ISAC) dla nowej mobilności

ADRESACI
Producenci pojazdów i komponentów, operatorzy infrastruktury ładowania, operatorzy flot, dostawcy oprogramowania, instytucje publiczne

GENEZA
Incydenty w sektorze często powtarzają się u różnych podmiotów, a brak zaufanego kanału wymiany informacji opóźnia reakcję

EFEKT
Szybsze wykrywanie i neutralizacja zagrożeń, wspólne standardy zgłaszania incydentów oraz budowa zaufania między uczestnikami rynku

Rekomendacje dla odbiorców produktów i usług nowej mobilności

Wprowadzenie minimalnych wymagań cyberbezpieczeństwa w zakupach flotowych i zamówieniach publicznych

ADRESACI
Administracja centralna, samorządy, operatorzy transportu, przedsiębiorstwa flotowe

GENEZA
Odbiorcy instytucjonalni nabywają coraz więcej pojazdów elektrycznych, usług ładowania i systemów zarządzania flotą, ale kryteria cyberbezpieczeństwa często nie są elementem specyfikacji

EFEKT
Wzrost presji rynkowej na dostawców oraz ograniczenie ryzyka wdrażania rozwiązań niespełniających podstawowych wymagań bezpieczeństwa

Stałe podnoszenie i aktualizowanie poziomu posiadanej wiedzy na temat danych generowanych przez pojazdy i usługi mobilności

ADRESACI
Użytkownicy indywidualni, firmy flotowe, operatorzy usług współdzielenia pojazdów

GENEZA
Pojazdy połączone i aplikacje mobilne przetwarzają dane lokalizacyjne, diagnostyczne, behawioralne i płatnicze

EFEKT
Bardziej świadome zarządzanie zgodami, kontami użytkowników i dostępem do usług cyfrowych

psnm WE DRIVE NEW MOBILITY!

psnm.org