OCHRONA pojazdów drogowych przed CYBERATAKAMI

Morand Fachot

Najważniejsze systemy infrastruktury coraz częściej są celem wyrafinowanych cyberataków. Sesja corocznego sympozjum Future Networked Car – organizowana przez Międzynarodowy Związek Telekomunikacyjny (International Telecommunication Union – ITU) oraz Europejską Komisję Gospodarczą (United Nations Economic Commission for Europe – UNECE) w ramach Geneva Motor Show – dokonała przeglądu środków podejmowanych dla cyberbezpieczeństwa systemów motoryzacyjnych. W wydarzeniu wzięli udział przedstawiciele władz, producenci samochodów oraz osoby zajmujące się opracowywaniem rozwiązań z zakresu cyberbezpieczeństwa w motoryzacji.

Troska o bezpieczeństwo

Instytucje rządowe i władze lokalne są zaniepokojone zagrożeniami związanymi z systemami transportu drogowego.

Darren Handley, Departament Transportu (Department for Transport – DoT), wyjaśnił uczestnikom, że przed przemysłem motoryzacyjnym stoją trzy rodzaje wyzwań:

- kulturalne: cyberbezpieczeństwo jest nowym zjawiskiem dla branży, potrzebuje więc odpowiednich struktur i organizacji;
- techniczne: trudność wynikająca z długiego czasu rozwoju i cyklu życia pojazdów, zarządzania ryzykiem w łańcuchu dostaw i interakcji z osobami trzecimi (trudności jak po wprowadzeniu na rynek urządzeń telematycznych);
- rządowe: nie ma żadnych regulacji, które precyzowałyby, co producenci powinni robić.

Jednak D. Handley zwraca uwagę, że organizacje normalizacyjne takie jak ISO, ITU, Stowarzyszenie Inżynierów Motoryzacji (Society of Automotive Engineers – SAE) oraz IEC i ISO w ramach Wspólnego Komitetu Technicznego ISO/IEC JTC 1 *Information technology*, pracują nad wstępnymi wytycznymi w tym obszarze.

Podejście brytyjskiego Departamentu Transportu ma sprawić, że „sektor transportu w UK będzie bezpieczny i odporny na cyberzagrożenia, a także zdolny do dalszego rozwoju w coraz bardziej połączonym, cyfrowym świecie". DoT chce zapewnić odpowiedni poziom ochrony pojazdów i infrastruktury drogowej z jaką pojazdy się komunikują przed nieautoryzowanym dostępem, przejęciem kontroli czy zakłóceniami.

Według D. Henley'a , DoT będzie wspierać to podejście poprzez:

- rozumienie zagrożeń dla cyberbezpieczeństwa i wrażliwość sektora transportu;
- zmniejszanie ryzyka wystąpienia cyberataku i podejmowanie odpowiednich działań, by chronić kluczowe zasoby;
- szybkie i efektywne reagowanie na incydenty cybernetyczne;
- promocję zmiany kulturowej, zwiększenie świadomości i budowę potencjału cybernetycznego.

Podejmowane w tej materii działania obejmują:

- promocję – dzięki inicjatywom takim jak wymiana informacji motoryzacyjnych prowadzona przez brytyjskie Centrum Bezpieczeństwa Cybernetycznego (National Cyber Security Centre (NCSC)) oraz Centre for the Protection of National Infrastructure (CPNI) w lutym 2017 r.; promocja zasad cyberbezpieczeństwa połączonych pojazdów autonomicznych (connected autonomous vehicles – CAV) w kwietniu 2017 r.;
- łagodzenie – poprzez współpracę w zakresie bezpieczeństwa cybernetycznego dla połączonych korytarzy* z partnerami z UE; przewodnictwo Grupy zadaniowej ds. bezpieczeństwa internetowego w ramach światowego forum UNECE w sprawie harmonizacji przepisów dotyczących pojazdów (projekt dokumentu 2018);
- reagowanie – zapewnienie mechanizmów raportowania i reagowania na incydenty poprzez system NCSC/CPNI Cyber Incident Response (CIR) (2017 r.).

Perspektywa jednostek badawczych i certyfikujących

Dirk Schlesinger, Dyrektor ds. Technologii w TÜV SÜD, (międzynarodowa firma świadcząca usługi w zakresie badań, kontroli, audytów i certyfikacji), podkreślił, jakie, wyzwania stoją przed branżą: „samochodem jutra jest komputer na kółkach, tylko bardziej skomplikowany". D. Schlesinger wspomniał o systemie Windows 10, który zawiera 27 – 50 milionów linii kodu, włączając w to płytę główną, kartę graficzną i aplikacje takie jak Office. Zauważył też, że Windows 10 nie ma żadnych czujników, a wszystko pozostaje w jednym miejscu. Dla porównania: supersamochód Ford GT ma 50 różnych czujników w zestawach 28 mikroprocesorów, 6 sieci CAN (communication area network), 3 000 różnych sygnałów dostarczających ekwiwalent 100 GB danych na godzinę (100 GB/h).

Wyzwaniem jest zebranie wszystkich sygnałów i ich skomunikowanie, mając przy tym pewność, że „gdy jeden czujnik zawiedzie to nie padnie cały system". Zauważa też, że samochód ma 10 milionów linii kodu „do zastosowań w sytuacjach krytycznych", czyli o 3 miliony więcej niż Boeing 787 i o 8 milionów więcej niż myśliwiec F-22, a „restart podczas jazdy jest wykluczony".

„Zawsze zakładaj, że jesteś w niebezpiecznej sieci, gdzie jesteś narażony na wiele ataków z różnych źródeł", uważa D. Schlesinger. Źródłem ataku mogą być wg niego „pokładowe" systemy audio, aplikacje na smartfony, przechwycenie komunikacji, (np. przy zdalnym otwieraniu drzwi, czujnikach ciśnienia opon oraz bezpośrednim dostępie do sieci przez tylną kamerę) lub zerwanie lusterka. Niedługo źródłem zagrożeń może być infrastruktura IT sprzedawcy lub zakładu naprawczego, dane od producentów oryginalnego wyposażenia albo inne elementy cyfrowego łańcucha dostaw.

Jak podkreślił D. Schlesinger, ochrona oprogramowania i kontrola jakości są coraz istotniejsze, jednak istniejące normy nie są wystarczające. Ostrzegał, że poleganie wyłącznie na bramach sieciowych i programach antywirusowych nie rozwiązuje wszystkich problemów, a całościowe spojrzenie na cyberbezpieczeństwo powinno uwzględniać technologię informatyczną i operacyjną (IT and Operational Technology – OT) podobną do tej w automatyce przemysłowej.

W poszukiwaniu rozwiązań informatycznych

Arnaud Taddei, Dyrektor ds. Architektury Systemów Bezpieczeństwa i główny technolog w Symantec, zaprezentował podejście firmy polegające na wyposażaniu samochodów w kompleksowe systemy bezpieczeństwa. To podejście zostało krótko opisane w Białej Księdze.

Według firmy Symantec „technologia istnieje po to, aby rozwiązywać wiele problemów związanych z bezpieczeństwem; trudności związane z wdrażaniem takiej technologii w samochodach są znacznie większe niż podobne działania w tradycyjnych systemach informatycznych. W nich większość problemów może zostać rozwiązana dzięki szybkiej instalacji, aktualizacji, zmianie konfiguracji" lub przy wykorzystaniu bardziej radykalnych środków mających na celu walkę z wyrafinowanymi zagrożeniami. Ale „samochody nie działają w ten sposób", ponieważ nie otrzymują „tygodniowych, codziennych i bieżących aktualizacji zabezpieczeń".

Firma Symantec zaleca „skalowalne podejście do wbudowanego systemu zabezpieczeń". Wymaga ono dyscypliny i współpracy w stosowaniu następujących podstawowych zasad bezpieczeństwa:

- ochrona całej komunikacji (całej łączności);
- ochrona każdego czujnika, siłownika, mikrokontrolera (MCU) i mikroprocesora;
- bezpieczne i efektywne zarządzanie całym pojazdem za pomocą OTA***;
- łagodzenie zaawansowanych zagrożeń.

Branża motoryzacyjna stoi w obliczu poważnych wyzwań, jak zauważa Symantec - aby bezpiecznie wprowadzać nowe technologie, potrzeba jest długiego czasu na przeprowadzanie certyfikacji. Ale sytuacja jest pilna, zaniedbanie tej kwestii może spowodować wzrost liczby ofiar śmiertelnych, podobnie jak zbyt szybkie zmiany w technologii.

Rozwiązanie tego „dużego i złożonego problemu wymaga zrozumienia i starań zarówno ze strony firm motoryzacyjnych, jak i firm zajmujących się bezpieczeństwem IT i OT. Projektowanie samochodów, które są bezpieczne od początku do końca, będzie wymagało czasu, a oba przemysły muszą zacząć rozwiązywać kwestie związane z bezpieczeństwem na każdym poziomie motoryzacyjnego łańcucha wartości".

Ochrona samochodów przed zagrożeniami cybernetycznymi wymaga dyscypliny i współpracy w stosowaniu podstawowych zasad bezpieczeństwa na każdym poziomie.

Symantec wskazuje „cztery podstawy" takiego działania:

- ochrona łączności: w szczególności modemów wykorzystywanych w ramach platform IVI (in-vehicle infotainment) lub w diagnostyce pokładowej pojazdu (on-board diagnostics – OBD);
- ochrona każdego modułu: czujników, siłowników i wszystkiego z MCU;
- zarządzanie z pomocą OTA: z chmury do każdego samochodu;
- łagodzenie zaawansowanych zagrożeń: analiza w samochodzie i w chmurze.

„Długoterminowe, kompleksowe bezpieczeństwo wymaga zbudowania bezpieczeństwa w każdej warstwie samochodu. Dzisiejsze samochody mają wiele warstw. (...). Zabezpieczenie całego „stosu" od góry do dołu w pełni i kompleksowo potrwa wiele lat, biorąc pod uwagę złożoność relacji z rozproszonymi dostawcami", zauważa Symantec, który oferuje zestaw technologii, mających sprostać tym wyzwaniom.

Bezpieczne pojazdy połączone

Yoram Berholtz, Dyrektor ds. Rozwoju Biznesowego w firmie Argus (firma zajmująca się bezpieczeństwem cybernetycznym w motoryzacji), która zapewnia bezpieczeństwo sieciowe całego pojazdu dzięki wykrywaniu ataków, podejrzanych działań i zmian standardowych zachowań w sieci pojazdu. Pojazdowa Ochrona Sieci firmy Argus, dzięki scentralizowanemu ośrodkowi sterowania, bada całą sieć komunikacyjną pojazdu i powstrzymuje pojawiające się w niej zagrożenia.

Według Y. Berholtza, w przyszłym roku na drogach będzie się poruszać 100 milionów samochodów.