Autonaprawa

www.e-autonaprawa.pl

Adres redakcji:
ul. Parkowa 25
51-616 Wrocław
tel. 71 715 77 95
faks 71 348 81 50
autonaprawa@technotransfer.pl
www.technotransfer.pl
Numer rachunku bankowego:
03 1140 2004 0000 3102 5467 9483

Redaktor naczelny:
Jan Wajdzik
j.wajdzik@technotransfer.pl

Redaktor prowadzący:
Marcin Bieńkowski
m.bienkowski@technotransfer.pl

Sekretarz redakcji:
Bogusława Krzczanowicz
b.krzczanowicz@technotransfer.pl

Serwis e-autonaprawa.pl:
Adam Rudziński
a.rudzinski@technotransfer.pl

Stali współpracownicy:
Andrzej Kowalewski, KrzaQ,
Hubert Kwarta, Zenon Majkut,
Leszek A. Stricker, Tomasz Szulc

Marketing i reklama:
Małgorzata Salamaga-Borysenko
tel. 71 733 67 56
m.salamaga@technotransfer.pl

Prenumerata:
tel. 71 715 77 95
prenumerata@technotransfer.pl

Opracowanie graficzne i skład:
Taurus CD
tel. 71 715 77 98

Wydawca:
Wydawnictwo Technotransfer

Druk i oprawa:
AMW Wrocław

Zdjęcia na okładce:
archiwum, ZF Aftermarket

FOT. ARCHIWUM

Cyberbezpieczeństwo

*Wydawać by się mogło, że cyberbezpieczeństwo i przemysł samochodowy to dwa odległe od siebie zagadnienia. A jednak nie. 25 czerwca br. UNECE (*United Nations Economic Commission for Europe*), czyli Europejska Komisja Gospodarcza będąca jedną z komisji regionalnych Organizacji Narodów Zjednoczonych, opublikowała wytyczne dotyczące cyberbezpieczeństwa związanego z samochodami i przemysłem motoryzacyjnym.*

Dwie nowe regulacje ONZ dotyczące bezpieczeństwa cybernetycznego i aktualizacji oprogramowania mają za zadanie stworzyć mechanizmy ochrony przed cyberzagrożeniami dotyczącymi coraz bardziej zdygitalizowanych pojazdów, ustanawiając jasne wymagania dotyczące cyfrowych procesów i ich audytu dla producentów samochodów, a pośrednio – również dla warsztatów samochodowych dokonujących napraw pojazdów i aktualizacji ich oprogramowania. Są to pierwsze w historii zharmonizowane i wiążące normy dotyczące sfery działalności przemysłu motoryzacyjnego.

Dwie regulacje ONZ, przyjęte przez Światowe Forum EKG ONZ ds. Harmonizacji przepisów dotyczących pojazdów, wymagają wdrożenia przepisów i procedur bezpieczeństwa w czterech obszarach. Pierwsze trzy dotyczą przede wszystkim producentów samych pojazdów i zarządzania flotą. Są to odpowiednio obszary obejmujące zarządzanie cyberzagrożeniami związanymi bezpośrednio z pojazdami, cyfrowe zabezpieczenia całego projektu samochodu oraz jego elementów składowych, co ograniczyć ma w założeniu cyberzagrożenia wzdłuż łańcucha wartości oraz wykrywanie i reagowanie na zdarzenia naruszające cyberbezpieczeństwo w całej flocie.

Ostatnim, czwartym obszarem, obejmującym już warsztaty samochodowe, jest zapewnienie bezpiecznych aktualizacji oprogramowania i bezpieczeństwa pojazdu przed zagrożeniami związanymi z upgradem i wymianą danych „w locie”. Chodzi tu o wprowadzenie mechanizmów cyberbezpieczeństwa i powiązanych z nimi regulacji dla tak zwanych aktualizacji Over-the-Air (OTA) *w oprogramowaniu pokładowym pojazdu.*

Wprowadzane przepisy będą miały zastosowanie zarówno do samochodów osobowych i dostawczych, jak i ciężarowych czy autobusów. Wejdą w one życie w styczniu 2021 r. W Unii Europejskiej nowe rozporządzenie w sprawie cybernetycznego bezpieczeństwa zacznie obowiązywać od lipca 2022 r. i dotyczyć będzie wszystkich wymienionych typów pojazdów samochodów wyprodukowanych od lipca 2024 r. Co ważne, również Korea Południowa i Japonia zobowiązały się do wprowadzenia w życie nowych regulacji.

Dlaczego jest to tak istotne? Pomijam już tu aspekt bezpieczeństwa związanego z coraz szerszym stosowaniem w najbliższej przyszłości pojazdów autonomicznych, które mogą być narażone na ataki hakerów i cyberterorystów. Otóż obecnie samochody zawierają do 150 elektronicznych jednostek sterujących i około 100 milionów linii kodu oprogramowania. Jest to czterokrotnie więcej niż w wypadku myśliwca F16. Według prognoz do 2030 roku liczba linii kodu wzrośnie do 300 milionów. Najmniejszy błąd podczas aktualizacji oprogramowania może po prostu kosztować czyjeś życie.

Marcin Bieńkowski

Marcin Bieńkowski