Samo izvorni tekstovi UNECE-a imaju pravni učinak prema međunarodnom javnom pravu. Status i dan stupanja na snagu ovog Pravilnika treba provjeriti u najnovijem izdanju dokumenta UN/ECE TRANS/WP.29/343, koji je dostupan na: https://unece.org/status-1958-agreement-and-annexed-regulations

Pravilnik UN-a br. 155 – Jedinstvene odredbe o homologaciji vozila s obzirom na kibersigurnost i sustav za upravljanje kibersigurnošću [2025/5]

Obuhvaća sav važeći tekst do:

dopune 3. izvorne verzije Pravilnika – datum stupanja na snagu: 10. siječnja 2025.

Ovaj je dokument isključivo informativne prirode. Vjerodostojni i pravno obvezujući tekstovi su:

— ECE/TRANS/WP.29/2020/79 (kako je izmijenjen dokumentima ECE/TRANS/WP.29/2020/94 i ECE/TRANS/WP.29/2020/97)

— ECE/TRANS/WP.29/2022/54

— ECE/TRANS/WP.29/2023/70 i

— ECE/TRANS/WP.29/2024/55

SADRŽAJ

Pravilnik

1. Područje primjene
2. Definicije
3. Zahtjev za homologaciju
4. Oznake
5. Homologacija
6. Certifikat o sukladnosti sustava za upravljanje kibersigurnošću
7. Specifikacije
8. Preinake tipa vozila i proširenje homologacije
9. Sukladnost proizvodnje
10. Sankcije za nesukladnost proizvodnje
11. Trajno obustavljena proizvodnja
12. Imena i adrese tehničkih službi odgovornih za provođenje homologacijskih ispitivanja te imena i adrese homologacijskih tijela

Prilozi

1. Opisni dokument
2. Izjava
3. Izgled homologacijskih oznaka
4. Predložak certifikata o sukladnosti sustava za upravljanje kibersigurnošću
5. Popis prijetnji i odgovarajućih protumjera

1. Područje primjene

1.1. Ovaj se Pravilnik primjenjuje na vozila kategorija L, M, N i O s obzirom na kibersigurnost ako imaju barem jednu elektroničku upravljačku jedinicu.

1.2. Ovim se Pravilnikom ne dovode u pitanje drugi pravilnici UN-a, regionalno zakonodavstvo ni nacionalno zakonodavstvo kojima je uređeno kako ovlaštene strane pristupaju vozilu i njegovim podacima, funkcijama i resursima te uvjeti takvog pristupa. Njime se ne dovodi u pitanje ni primjena nacionalnog i regionalnog zakonodavstva u području privatnosti i zaštite fizičkih osoba s obzirom na obradu njihovih osobnih podataka.

1.3. Ovim se Pravilnikom ne dovode u pitanje drugi pravilnici UN-a, regionalno zakonodavstvo ni nacionalno zakonodavstvo kojima je uređeno kako se razvijaju i ugrađuju/integriraju u sustav fizički i digitalni zamjenski dijelovi i zamjenski sastavni dijelovi s obzirom na kibersigurnost.

2. Definicije

Za potrebe ovog Pravilnika primjenjuju se sljedeće definicije:

2.1. „tip vozila” znači vozila koja se ne razlikuju barem prema sljedećim bitnim svojstvima:

(a) proizvođačeva oznaka tipa vozila;

(b) bitne karakteristike električke/elektroničke arhitekture i vanjskih sučelja s obzirom na kibersigurnost;

2.2. „kibersigurnost” znači stanje u kojem su cestovna vozila i njihove funkcije zaštićeni od kiberprijetnji električnim i elektroničkim sastavnim dijelovima;

2.3. „sustav za upravljanje kibersigurnošću” ili „CSMS” znači na riziku utemeljen sustavan pristup kojim se definiraju organizacijski postupci, odgovornosti i upravljanje namijenjeni za obradu rizika povezanih s kiberprijetnjama vozilima i za zaštitu vozila od kibernapada;

2.4. „sustav” znači skup sastavnih dijelova i/ili podsustava kojim su ostvarene određene funkcije;

2.5. „faza razvoja” znači razdoblje prije homologacije tipa vozila;

2.6. „faza proizvodnje” znači razdoblje tijekom kojeg se određeni tip vozila proizvodi;

2.7. „faza nakon proizvodnje” znači razdoblje od prestanka proizvodnje tipa vozila do kraja životnog vijeka svih vozila tog tipa. Tijekom ove faze vozila tog tipa su u uporabi, ali se više ne proizvode. Ova se faza završava kad u uporabi više nema vozila tog tipa;

2.8. „protumjera” znači mjera koja smanjuje rizik;

2.9. „rizik” znači potencijal određene prijetnje za iskorištavanje slabih točaka vozila, a time i uzrokovanja štete organizaciji ili pojedincu;

2.10. „procjena rizika” znači cijeli postupak pronalaženja, prepoznavanja i opisivanja rizika (utvrđivanje rizika) radi razumijevanja prirode rizika i određivanja njegova stupnja (analiza rizika) te primjena kriterija rizika na rezultate analize rizika kako bi se odredilo jesu li rizik i/ili njegovi razmjeri prihvatljivi ili podnošljivi (evaluacija rizika);

2.11. „upravljanje rizikom” znači koordinirane aktivnosti za usmjeravanje i kontrolu organizacije s obzirom na rizik;

2.12. „prijetnja” znači potencijalni uzrok neželjenog događaja čija posljedica može biti šteta sustavu, organizaciji ili pojedincu;

2.13. „slaba točka” znači slabost elementa ili protumjere zbog koje je taj element odnosno protumjera izložen najmanje jednoj prijetnji.

3. Zahtjev za homologaciju

3.1. Zahtjev za homologaciju tipa vozila s obzirom na kibersigurnost podnosi proizvođač vozila ili njegov ovlašteni zastupnik.

3.2. Zahtjevu se prilažu dokumenti u nastavku u tri primjerka i sljedeće pojedinosti:

3.2.1. opis tipa vozila s obzirom na elemente iz Priloga 1. ovom Pravilniku;

3.2.2. ako se pokaže da su podaci zaštićeni pravima intelektualnog vlasništva ili da predstavljaju specifično znanje i iskustvo proizvođača ili njegovih dobavljača, proizvođač odnosno njegovi dobavljači dužni su staviti na raspolaganje dovoljno podataka za ispravno provođenje provjera propisanih u ovom Pravilniku. Svi se takvi podaci smatraju povjerljivima;

3.2.3. certifikat o sukladnosti CSMS-a u skladu sa stavkom 6. ovog Pravilnika.

3.3. Dokumentacija se dijeli na dva dijela:

(a) službena opisna dokumentacija za homologaciju, koja sadržava stavke iz Priloga 1., koja se dostavlja homologacijskom tijelu ili njegovoj tehničkoj službi u trenutku podnošenja zahtjeva za homologaciju. Homologacijskom tijelu, ili njegovoj tehnički službi, ta je opisna dokumentacija osnovna referenca za homologacijski postupak. Homologacijsko tijelo, ili njegova tehnička služba, dužno se pobrinuti da opisna dokumentacija bude dostupna najmanje deset godina od trenutka trajnog obustavljanja proizvodnje tipa vozila;

(b) dodatni materijali bitni za zahtjeve ovog Pravilnika koje proizvođač može zadržati, ali koji se daju na uvid u trenutku homologacije. Proizvođač se dužan pobrinuti da svi materijali dani na uvid u trenutku homologacije budu dostupni najmanje deset godina od trenutka trajnog obustavljanja proizvodnje tipa vozila.

4. Oznake

4.1. Na svako se vozilo koje je sukladno s tipom vozila homologiranim na temelju ovog Pravilnika pričvršćuje, na vidljivom i lako dostupnom mjestu naznačenom na homologacijskom obrascu, međunarodna homologacijska oznaka koja se sastoji od:

4.1.1. kružnice oko slova „E” iza kojeg slijedi razlikovni broj države koja je dodijelila homologaciju;

4.1.2. desno od kružnice propisane u stavku 4.1.1., broja ovog Pravilnika iza kojeg slijede slovo „R”, crtica i homologacijski broj.

4.2. Ako je vozilo sukladno s tipom vozila homologiranim na temelju najmanje jednog drugog pravilnika priloženog Sporazumu u zemlji koja je dodijelila homologaciju na temelju ovog Pravilnika, simbol propisan stavkom 4.1.1. ovog Pravilnika ne treba ponavljati; u tom se slučaju brojevi pravilnika, homologacijski brojevi i dodatni simboli svih pravilnika na temelju kojih je homologacija dodijeljena u zemlji koja je dodijelila homologaciju na temelju ovog Pravilnika navode u okomitim stupcima desno od simbola opisanog u stavku 4.1.1.

4.3. Homologacijska oznaka mora biti lako čitljiva i neizbrisiva.

4.4. Homologacijska oznaka postavlja se blizu pločice s podacima o vozilu koju je pričvrstio proizvođač ili na nju.

4.5. U Prilogu 3. ovom Pravilniku prikazani su primjeri homologacijskih oznaka.

5. Homologacija

5.1. Homologacijska tijela dodjeljuju, kako je primjenjivo, homologaciju s obzirom na kibersigurnost samo tipovima vozila koji ispunjavaju zahtjeve ovog Pravilnika.

5.1.1. Homologacijsko tijelo, ili njegova tehnička služba, dužno je u dokumentaciji provjeriti da je proizvođač vozila poduzeo potrebne mjere relevantne za tip vozila radi:

(a) prikupljanja i provjeravanja podataka, koji se traže na temelju ovog Pravilnika, u cijelom lancu opskrbe kako bi se dokazalo da su rizici povezani s dobavljačima utvrđeni i stavljeni pod kontrolu;

(b) dokumentiranja procjene rizika (provedene tijekom faze razvoja ili naknadno) te ispitivanja rezultata i protumjera primijenjenih na tipu vozila, uključujući konstrukcijske podatke na kojima se temelji procjena rizika;

(c) ugradnje odgovarajućih kibersigurnosnih mjera u konstrukciju tipa vozila;

(d) otkrivanja mogućih kibersigurnosnih napada i odgovaranja na njih;

(e) bilježenja podataka kako bi se pomoglo u otkrivanju kibernapada i posjedovanja funkcionalnosti obrade podataka radi analize pokušanih i uspješnih kibernapada.

5.1.2. Homologacijsko tijelo, ili njegova tehnička služba, dužno je ispitivanjem uzorka tipa vozila provjeriti da je proizvođač vozila ugradio kibersigurnosne mjere navedene u dokumentaciji. Na temelju uzoraka homologacijsko tijelo ili tehnička služba provodi ispitivanja samostalno ili u suradnji s proizvođačem vozila. Iako je fokus provjere uzoraka na rizicima koji su u procjeni rizika ocijenjeni visokima, ta provjera nije ograničena samo na te rizike.

5.1.3. Homologacijsko tijelo, ili njegova tehnička služba, dužno je odbiti homologaciju s obzirom na kibersigurnost ako proizvođač vozila nije ispunio neki od zahtjeva iz stavka 7.3., konkretno:

(a) ako proizvođač vozila nije proveo temeljitu procjenu rizika iz stavka 7.3.3., što uključuje i ako nije uzeo u obzir sve rizike povezane s prijetnjama iz dijela A Priloga 5.;

(b) ako proizvođač vozila nije zaštitio tip vozila od rizika utvrđenih u procjeni rizika koju je sam izradio ili ako nije ugradio razmjerne protumjere, kako je propisano u stavku 7.;

(c) ako proizvođač vozila nije uspostavio odgovarajuće i razmjerne mjere za osiguravanje namjenskih okruženja u tipu vozila (prema potrebi) za pohranu i izvršavanje softvera, usluga, aplikacija i podataka koji se dodaju nakon prodaje;

(d) ako proizvođač vozila nije prije homologacije proveo odgovarajuće i dostatno ispitivanje da potvrdi djelotvornost ugrađenih sigurnosnih mjera.

5.1.4. Homologacijsko tijelo koje provodi homologacijska ispitivanja dužno je odbiti homologaciju s obzirom na kibersigurnost ako homologacijsko tijelo odnosno njegova tehnička služba od proizvođača vozila ne dobije dostatne podatke za procjenu kibersigurnosti tipa vozila.

5.2. Obavijest o dodjeljivanju, proširenju ili odbijanju homologacije tipa vozila homologiranog na temelju ovog Pravilnika dostavlja se ugovornim strankama Sporazuma iz 1958. koje primjenjuju ovaj Pravilnik putem obrasca u skladu s predloškom iz Priloga 2. ovom Pravilniku.

5.3. Homologacijsko tijelo ne smije dodijeliti homologaciju prije nego što provjeri da je proizvođač uspostavio zadovoljavajuće mjere i postupke za valjano upravljanje kibersigurnosnim svojstvima obuhvaćenima ovim Pravilnikom.

5.3.1. Homologacijsko tijelo i njegove tehničke službe dužni su se uz kriterije s Popisa 2. Sporazuma iz 1958. pobrinuti:

(a) da raspolažu stručnim osobljem s odgovarajućim kibersigurnosnim vještinama i poznavanjem procjena rizika specifičnih za automobilski sektor; ([1])

(b) da uvedu postupke za ujednačenu evaluaciju na temelju ovog Pravilnika.

5.3.2. Svaka ugovorna stranka koja primjenjuje ovaj Pravilnik putem svojeg homologacijskog tijela obavješćuje homologacijska tijela ostalih ugovornih stranaka koje primjenjuju ovaj Pravilnik o metodi i kriterijima kojima se to homologacijsko tijelo služi za procjenu primjerenosti mjera poduzetih na temelju ovog Pravilnika, a osobito stavaka 5.1., 7.2. i 7.3.

Te se informacije dijele (a) samo jednom, prije prve dodjele homologacije na temelju ovog Pravilnika, i (b) svaki put kad se metoda ili kriteriji procjene ažuriraju.

Te se informacije trebaju dijeliti radi prikupljanja i analize najboljih primjera iz prakse te zato da sva homologacijska tijela koja primjenjuju ovaj Pravilnik budu dosljedna u njegovoj primjeni.

5.3.3. Informacije iz stavka 5.3.2. unose se na engleskom jeziku u sigurnu internetsku bazu podataka „DETA” ([2]), koju je uspostavila Gospodarska komisija Ujedinjenih naroda za Europu, pravovremeno, a najkasnije 14 dana prije dodjele homologacije na temelju tih metoda i kriterija procjene. Te informacije moraju biti dovoljne za razumijevanje minimalne učinkovitosti koju je homologacijsko tijelo postavilo za svaki specifični zahtjev iz stavka 5.3.2. te postupaka i mjera koje to tijelo primjenjuje da bi provjerilo da je ta minimalna učinkovitost postignuta ([3]).

5.3.4. Homologacijska tijela koja primaju informacije iz stavka 5.3.2. mogu u roku od 14 dana od primanja obavijesti unijeti u DETA-u komentare namijenjene homologacijskom tijelu koje je unijelo obavijest.

5.3.5. Ako homologacijsko tijelo koje dodjeljuje homologaciju ne može uzeti u obzir komentare primljene u skladu sa stavkom 5.3.4., homologacijska tijela koja su poslala komentare i homologacijsko tijelo koje dodjeljuje homologaciju dužna su tražiti dodatno objašnjenje u skladu s Popisom 6. Sporazuma iz 1958. Odgovarajuća pomoćna radna skupina ([4]) Svjetskog foruma za usklađivanje pravilnika o vozilima (WP.29) za ovaj Pravilnik dogovara zajedničko tumačenje metoda i kriterija procjene ([5]). To se zajedničko tumačenje mora primijeniti te su sva homologacijska tijela dužna izdavati homologacije na temelju ovog Pravilnika u skladu s tim zajedničkim tumačenjem.

([1]) Npr. ISO 26262-2018, ISO/PAS 21448, ISO/SAE 21434.
([2]) https://www.unece.org/trans/main/wp29/datasharing.html.
([3]) Smjernice za detaljne podatke (npr. metoda, kriteriji, učinkovitost) koje treba unijeti i format tih podataka navode se u dokumentu za tumačenje koji Radna skupina za kibersigurnost i pitanja odašiljanja radiovalovima priprema za sedmi sastanak GRVA-e.
([4]) Radna skupina za automatizirana/autonomna i povezana vozila (GRVA).
([5]) To se tumačenje mora unijeti u dokument za tumačenje na koji se upućuje u bilješki uz stavak 5.3.3.

5.3.6. Svako homologacijsko tijelo koje dodijeli homologaciju na temelju ovog Pravilnika dužno je o dodijeljenoj homologaciji obavijestiti ostala homologacijska tijela. U roku od 14 dana od dana dodjele homologacije homologacijsko tijelo u DETA-u unosi homologaciju i dopunsku dokumentaciju na engleskom jeziku. ([6])

5.3.7. Ugovorne stranke mogu proučiti dodijeljene homologacije na temelju informacija unesenih u skladu sa stavkom 5.3.6. Ako ugovorne stranke donesu različite zaključke, to se rješava u skladu s člankom 10. i Popisom 6. Sporazuma iz 1958. Ugovorne stranke također obavješćuju odgovarajuću pomoćnu radnu skupinu Svjetskog foruma za usklađivanje pravilnika o vozilima (WP.29) o različitim tumačenjima u smislu Popisa 6. Sporazuma iz 1958. Odgovarajuća radna skupina pomaže u rješavanju pitanja različitih zaključaka te se prema potrebi može savjetovati s WP.29.

5.4. Za potrebe stavka 7.2. ovog Pravilnika proizvođač se dužan pobrinuti da su kibersigurnosna svojstva obuhvaćena ovim Pravilnikom ugrađena.

6. Certifikat o sukladnosti sustava za upravljanje kibersigurnošću

6.1. Ugovorne stranke imenuju homologacijsko tijelo za procjenu proizvođača i izdavanje certifikata o sukladnosti CSMS-a.

6.2. Zahtjev za certifikat o sukladnosti sustava za upravljanje kibersigurnošću podnosi proizvođač vozila ili njegov ovlašteni zastupnik.

6.3. Zahtjevu se prilažu dokumenti u nastavku u tri primjerka i sljedeće pojedinosti:

6.3.1. dokumenti s opisom sustava za upravljanje kibersigurnošću;

6.3.2. potpisana izjava u skladu s predloškom iz Dodatka 1. Prilogu 1.

6.4. U okviru procjene proizvođač izjavljuje, koristeći izjavu u skladu s predloškom iz Dodatka 1. Prilogu 1., i mora dokazati homologacijskom tijelu ili njegovoj tehničkoj službi da je uspostavio potrebne postupke za ispunjavanje svih zahtjeva za kibersigurnost u skladu s ovim Pravilnikom.

6.5. Nakon što je zaprimljena potpisana proizvođačeva izjava u skladu s predloškom iz Dodatka 1. Prilogu 1. i ako je ishod procjene pozitivan, proizvođaču se dodjeljuje certifikat koji se zove certifikat o sukladnosti CSMS-a, kako je opisan u Prilogu 4. ovom Pravilniku (dalje u tekstu „certifikat o sukladnosti CSMS-a”).

6.6. Homologacijsko tijelo ili njegova tehnička služba za certifikat o sukladnosti CSMS-a koristi predložak iz Priloga 4. ovom Pravilniku.

6.7. Ako nije prethodno povučen, certifikat o sukladnosti CSMS-a vrijedi najdulje tri godine od datuma izdavanja.

6.8. Homologacijsko tijelo koje je dodijelilo certifikat o sukladnosti CSMS-a može u bilo kojem trenutku provjeriti da su zahtjevi za valjanost certifikata i dalje ispunjeni. Ako zahtjevi utvrđeni u ovom Pravilniku nisu ispunjeni, homologacijsko tijelo povlači certifikat o sukladnosti CSMS-a.

([6]) Na sedmom sastanku GRVA-a pripremit će se dodatne informacije o minimalnim zahtjevima za opisnu dokumentaciju.

6.9. Proizvođač obavješćuje homologacijsko tijelo ili njegovu tehničku službu o svakoj promjeni koja će utjecati na valjanost certifikata o sukladnosti CSMS-a. Nakon savjetovanja s proizvođačem homologacijsko tijelo ili njegova tehnička služba odlučuje jesu li potrebne nove provjere.

6.10. Zahtjev za novi certifikat o sukladnosti CSMS-a ili produljenje postojećeg certifikata o sukladnosti CSMS-a proizvođač je dužan podnijeti pravovremeno tako da homologacijsko tijelo može dovršiti procjenu prije isteka valjanosti certifikata o sukladnosti CSMS-a. Ako je ishod procjene pozitivan, homologacijsko tijelo izdaje novi certifikat o sukladnosti CSMS-a ili produljuje valjanost postojećeg certifikata za novo razdoblje od tri godine. Homologacijsko tijelo provjerava da CSMS i dalje ispunjava zahtjeve ovog Pravilnika. Homologacijsko tijelo izdaje novi certifikat ako su njemu odnosno njegovoj tehničkoj službi prijavljene promjene, a ishod procjene tih promjena bio je pozitivan.

6.11. Istek ili povlačenje proizvođačeva certifikata o sukladnosti CSMS-a smatra se, kad je riječ o tipovima vozila na koje se odnosi taj CSMS, kao preinaka homologacije, kako je navedeno u stavku 8., što može značiti povlačenje homologacije ako uvjeti za njezinu dodjelu više nisu ispunjeni.

7. Specifikacije

7.1. Opće specifikacije

7.1.1. Zahtjevi ovog Pravilnika ne ograničavaju odredbe ni zahtjeve drugih pravilnika UN-a.

7.2. Zahtjevi za sustav za upravljanje kibersigurnošću

7.2.1. Za potrebe ocjenjivanja homologacijsko tijelo ili njegova tehnička služba provjerava da je proizvođač vozila uspostavio sustav za upravljanje kibersigurnošću te da je taj sustav sukladan s ovim Pravilnikom.

7.2.2. Sustav za upravljanje kibersigurnošću obuhvaća sljedeće.

7.2.2.1. Proizvođač vozila dužan je dokazati homologacijskom tijelu ili njegovoj tehničkoj službi da se sustav za upravljanje kibersigurnošću primjenjuje na sljedeće faze:

(a) fazu razvoja;

(b) fazu proizvodnje;

(c) fazu nakon proizvodnje.

7.2.2.2. Proizvođač vozila dužan je dokazati da se postupcima u njegovu sustavu za upravljanje kibersigurnošću jamči da je sigurnost uzeta u obzir na primjeren način, što uključuje uzimanje u obzir rizika i protumjera iz Priloga 5. To obuhvaća:

(a) postupke za upravljanje kibersigurnošću u proizvođačevoj organizaciji;

(b) postupke za utvrđivanje rizika za tipove vozila. U tim se postupcima moraju uzeti u obzir prijetnje iz dijela A. Priloga 5. i druge relevantne prijetnje;

(c) postupke za ocjenjivanje, kategorizaciju i obradu utvrđenih rizika;

(d) postupke za provjeru da se utvrđenim rizicima upravlja na odgovarajući način;

(e) postupke za ispitivanje kibersigurnosti tipa vozila;

(f) postupke za osiguravanje ažurnosti procjene rizika;

(g) postupke za praćenje i otkrivanje kibernapada, kiberprijetnji i slabih točaka na tipovima vozila, postupke za odgovaranje na te kibernapade, kiberprijetnje i slabe točke te postupke za procjenu jesu li ugrađene kibersigurnosne mjere još djelotvorne s obzirom na novoutvrđene kiberprijetnje i slabosti;

(h) postupke za prikupljanje odgovarajućih podataka radi analize pokušanih i uspješnih kibernapada.

7.2.2.3. Proizvođač vozila dužan je dokazati da se postupcima u njegovu sustavu za upravljanje kibersigurnošću postiže da su, u skladu s kategorizacijom iz stavka 7.2.2.2. podstavaka (c) i (g), u razumnom roku poduzete protumjere u slučaju kiberprijetnji i slabih točaka na koje je proizvođač vozila dužan reagirati.

7.2.2.4. Proizvođač vozila dužan je dokazati da se postupcima u njegovu sustavu za upravljanje kibersigurnošću kontinuirano vrši praćenje iz stavka 7.2.2.2. podstavka (g). To:

(a) obuhvaća praćenje vozila nakon prve registracije;

(b) obuhvaća sposobnost analiziranja i otkrivanja kiberprijetnji, slabih točaka i kibernapada na temelju podataka i zapisa iz vozila. Ta sposobnost mora biti u skladu sa stavkom 1.3. i pravom na privatnost vlasnika i vozača vozila, a osobito s obzirom na privolu.

7.2.2.5. Proizvođač vozila dužan je dokazati kako s obzirom na zahtjeve iz stavka 7.2.2.2. njegov sustav za upravljanje kibersigurnošću drži pod kontrolom potencijalne ovisnosti među dobavljačima, pružateljima usluga ili proizvođačevim podorganizacijama.

7.3. Zahtjevi za tipove vozila

7.3.1. Proizvođač mora imati valjan certifikat o sukladnosti sustava za upravljanje kibersigurnošću koji odgovara tipu vozila koji se homologira. Međutim, kad je riječ o homologacijama vozila kategorija M, N i O prvobitno dodijeljenima prije 1. srpnja 2024. i homologacijama vozila kategorije L prvobitno dodijeljenima prije 1. srpnja 2029. i svim njihovim proširenjima, ako proizvođač vozila može dokazati da se tip vozila ne bi mogao projektirati u skladu s CSMS-om, proizvođač vozila dokazuje da je kibersigurnost primjereno uzeta u obzir u fazi razvoja tog tipa vozila.

7.3.2. Da bi se vozilo homologiralo, proizvođač vozila dužan je utvrditi i staviti pod kontrolu rizike povezane s dobavljačima.

7.3.3. Proizvođač vozila dužan je identificirati kritične elemente tipa vozila i provodi temeljitu procjenu rizika za taj tip vozila pa obrađuje ili kontrolira utvrđene rizike na primjeren način. U procjeni rizika uzima u obzir pojedinačne elemente tipa vozila i njihove interakcije. U procjeni rizika razmatra i interakcije sa svim vanjskim sustavima. U procjeni rizika proizvođač vozila uzima u obzir rizike povezane sa svim prijetnjama iz dijela A Priloga 5. i sve ostale relevantne rizike.

7.3.4. Proizvođač vozila dužan je zaštititi tip vozila od rizika utvrđenih u procjeni rizika koju je izradio. Radi zaštite tipa vozila ugrađuje razmjerne protumjere. Ugrađene protumjere moraju obuhvaćati sve protumjere iz dijelova B i C Priloga 5. relevantne za utvrđene rizike. Međutim, ako neka protumjera iz dijela B ili C Priloga 5. nije relevantna ili nije dovoljna za utvrđeni rizik, proizvođač vozila dužan se pobrinuti za ugradnju druge odgovarajuće protumjere.

Posebno, kad je riječ o homologacijama vozila kategorija M, N i O prvobitno dodijeljenima prije 1. srpnja 2024. i homologacijama vozila kategorije L prvobitno dodijeljenima prije 1. srpnja 2029. i svim njihovim proširenjima, proizvođač vozila dužan se pobrinuti da je ugrađena druga odgovarajuća protumjera ako neka protumjera iz dijela B ili C Priloga 5. nije tehnički izvediva. Proizvođač je dužan homologacijskom tijelu dati odgovarajuću procjenu tehničke izvedivosti.

7.3.5. Proizvođač vozila dužan je uspostaviti odgovarajuće i razmjerne sigurnosne mjere za namjenska okruženja u tipu vozila (ako takva okruženja postoje u vozilu) za pohranu i izvršavanje softvera, usluga, aplikacija i podataka koji se dodaju nakon prodaje.

7.3.6. Proizvođač vozila dužan je prije homologacije provesti odgovarajuće i dostatno ispitivanje da potvrdi djelotvornost ugrađenih sigurnosnih mjera.

7.3.7. Proizvođač vozila dužan je u tip vozila ugraditi mjere:

(a) za otkrivanje i sprečavanje kibernapada na vozila tog tipa vozila;

(b) za potporu proizvođačeve sposobnosti praćenja radi otkrivanja prijetnji, slabih točaka i kibernapada relevantnih za tip vozila;

(c) za funkcionalnost obrade podataka radi analize pokušanih i uspješnih kibernapada.

7.3.8. Kriptografski moduli koji se koriste za potrebe ovog Pravilnika moraju biti u skladu s prihvaćenim normama. Ako korišteni kriptografski moduli nisu u skladu s prihvaćenim normama, proizvođač vozila dužan je obrazložiti njihovu uporabu.

7.4. Izvješćivanje

7.4.1. Proizvođač vozila najmanje jednom godišnje, ili češće ako je važno, izvješćuje homologacijsko tijelo ili tehničku službu o ishodima aktivnosti praćenja, kako su definirane u stavku 7.2.2.2. podstavku (g), što obuhvaća relevantne informacije o novim kibernapadima. Proizvođač vozila također izvješćuje homologacijsko tijelo ili tehničku službu o tome da su kibersigurnosne mjere ugrađene u njegove tipove vozila i dalje djelotvorne i potvrđuje tu djelotvornost te ih izvješćuje o svim dodatnim poduzetim mjerama.

7.4.2. Homologacijsko tijelo ili tehnička služba provjerava dostavljene informacije i prema potrebi traži da proizvođač vozila ispravi utvrđene nedjelotvornosti.

Ako izvješćivanje ili odgovori nisu dostatni, homologacijsko tijelo može odlučiti povući certifikat o sukladnosti CSMS-a u skladu sa stavkom 6.8.

8. Preinake tipa vozila i proširenje homologacije

8.1. Homologacijsko tijelo koje je homologiralo tip vozila mora se obavijestiti o svakoj preinaci tog tipa vozila koja utječe na tehničku sposobnost s obzirom na kibersigurnost i/ili na dokumentaciju propisane ovim Pravilnikom. Homologacijsko tijelo tada može:

8.1.1. smatrati da učinjene preinake još uvijek ispunjavaju zahtjeve i da odgovaraju dokumentaciji postojeće homologacije; ili

8.1.2. provesti potrebnu dodatnu procjenu u skladu sa stavkom 5. i prema potrebi tražiti dodatno ispitno izvješće od tehničke službe odgovorne za provođenje ispitivanja.

8.1.3. Obavijest o dodjeljivanju, proširenju ili odbijanju homologacije, uz navođenje preinaka, dostavlja se putem obrasca u skladu s predloškom iz Priloga 2. ovom Pravilniku. Homologacijsko tijelo koje izda proširenje homologacije dodjeljuje serijski broj tom proširenju te je o tome dužno obavijestiti ostale stranke Sporazuma iz 1958. koje primjenjuju ovaj Pravilnik izjavom u skladu s predloškom iz Priloga 2. ovom Pravilniku.

9. Sukladnost proizvodnje

9.1. Postupci za provjeru sukladnosti proizvodnje moraju biti u skladu s onima iz Popisa 1. Sporazuma iz 1958. (E/ECE/TRANS/505/Rev.3) i ispunjavati sljedeće zahtjeve:

9.1.1. nositelj homologacije dužan se pobrinuti da su rezultati provjera sukladnosti proizvodnje zabilježeni i da su priloženi dokumenti dostupni tijekom razdoblja dogovorenog s homologacijskim tijelom ili njegovom tehničkom službom. To razdoblje ne smije biti dulje od 10 godina od trenutka trajnog obustavljanja proizvodnje;

9.1.2. homologacijsko tijelo koje je dodijelilo homologaciju može u bilo kojem trenutku provjeriti metode za provjeru sukladnosti proizvodnje koje se primjenjuju u svakom proizvodnom pogonu. Te se provjere obično provode jednom u tri godine.

10. Sankcije za nesukladnost proizvodnje

10.1. Homologacija dodijeljena tipu vozila na temelju ovog Pravilnika može se povući ako nisu ispunjeni zahtjevi ovog Pravilnika ili ako uzorci vozila ne ispunjavaju zahtjeve ovog Pravilnika.

10.2. Ako homologacijsko tijelo povuče homologaciju koju je prethodno dodijelilo, dužno je o tome odmah obavijestiti druge ugovorne stranke koje primjenjuju ovaj Pravilnik izjavom u skladu s predloškom iz Priloga 2. ovom Pravilniku.

11. Trajno obustavljena proizvodnja

11.1. Ako nositelj homologacije potpuno obustavi proizvodnju tipa vozila homologiranog na temelju ovog Pravilnika, dužan je o tome obavijestiti homologacijsko tijelo koje je dodijelilo homologaciju. Nakon primanja te obavijesti to tijelo o tome obavještava druge stranke Sporazuma koje primjenjuju ovaj Pravilnik kopijom izjave o homologaciji na čijem je kraju bilješka „PROIZVODNJA OBUSTAVLJENA”, napisana velikim slovima, potpisana i datirana.

12. Imena i adrese tehničkih službi odgovornih za provođenje homologacijskih ispitivanja te imena i adrese homologacijskih tijela

12.1. Ugovorne stranke Sporazuma koje primjenjuju ovaj Pravilnik prijavljuju Tajništvu Ujedinjenih naroda imena i adrese tehničkih službi odgovornih za provođenje homologacijskih ispitivanja te homologacijskih tijela koja dodjeljuju homologacije i kojima treba dostaviti obrasce za potvrdu dodjeljivanja, proširenja, odbijanja ili povlačenja homologacije koji su izdani u drugim državama.

PRILOG 1.

Opisni dokument

Sljedeći se podaci, ako su primjenjivi, dostavljaju u tri primjerka s popisom sadržaja. Svi se crteži dostavljaju u prikladnom mjerilu na formatu A4 ili u mapi tog formata i moraju biti dovoljno detaljni. Fotografije, ako ih ima, moraju biti dovoljno detaljne.

1. Marka (trgovačko ime proizvođača):.....

2. Tip i opći trgovački opisi:.....

3. Podaci za identifikaciju tipa, ako su označeni na vozilu:.....

4. Mjesto te oznake:.....

5. Kategorije vozila:.....

6. Ime i adresa proizvođača/proizvođačeva zastupnika:.....

7. Imena i adrese proizvodnih pogona:.....

8. Fotografije i/ili crteži reprezentativnog vozila:.....

9. Kibersigurnost

9.1. Opće konstrukcijske karakteristike tipa vozila, uključujući:

(a) sustave vozila bitne za kibersigurnost tipa vozila

(b) sastavne dijelove tih sustava koji su bitni za kibersigurnost

(c) interakciju tih sustava s drugim sustavima vozila i vanjskim sučeljima

9.2. Shema tipa vozila

9.3. Broj certifikata o sukladnosti sustava za upravljanje kibersigurnošću:.....

9.4. Dokumenti, koji se odnose na tip vozila koji se homologira, s opisom ishoda procjene rizika i utvrđenih rizika:.....

9.5. Dokumenti, koji se odnose na tip vozila koji se homologira, s opisom protumjera ugrađenih na popisane sustave ili u tip vozila i načina kako utječu na navedene rizike:.....

9.6. Dokumenti, koji se odnose na tip vozila koji se homologira, s opisom zaštita namjenskih okruženja za softver, usluge, aplikacije i podatke koji se dodaju nakon prodaje:.....

9.7. Dokumenti, koji se odnose na tip vozila koji se homologira, s opisom ispitivanja korištenih za provjeru kibersigurnosti tipa vozila i njegovih sustava i s rezultatima tih ispitivanja:.....

9.8. Opis kako je lanac opskrbe uzet u obzir s obzirom na kibersigurnost:.....

Prilog 1. – Dodatak 1.

Predložak proizvođačeve izjave o sukladnosti sustava za upravljanje kibersigurnošću

Proizvođačeva izjava o sukladnosti sa zahtjevima za sustav za upravljanje kibersigurnošću

Ime proizvođača: ……

Adresa proizvođača: ……

…… .(*ime proizvođača*)

potvrđuje da su postupci potrebni za ispunjavanje zahtjeva za sustav za upravljanje kibersigurnošću, utvrđeni u stavku 7.2. Pravilnika UN-a br. 155, uspostavljeni i da se održavaju.

Sastavljeno u: …… (*mjesto*)

Datum:……

Ime potpisnika: ……

Funkcija potpisnika: ……

(pečat i potpis proizvođačeva zastupnika)

PRILOG 2.

Izjava

(najveći format: A4 (210 × 297 mm))



koju je izdalo: ime tijela
……
……
……

o: (2) dodjeli homologacije
proširenju homologacije
povlačenju homologacije s učinkom od dd/mm/gggg
odbijanju homologacije
trajno obustavljenoj proizvodnji

tipa vozila na temelju Pravilnika UN-a br. 155

Homologacijski broj: ……

Broj proširenja: ……

Obrazloženje proširenja:……

1. Marka (trgovačko ime proizvođača):……

2. Tip i opći trgovački opisi:……

3. Podaci za identifikaciju tipa, ako su označeni na vozilu:……

3.1. Mjesto te oznake:……

4. Kategorije vozila: ……

5. Ime i adresa proizvođača/proizvođačeva zastupnika:……

6. Imena i adrese proizvodnih pogona: ……

7. Broj certifikata o sukladnosti sustava za upravljanje kibersigurnošću:……

8. Tehnička služba odgovorna za provođenje homologacijskih ispitivanja: ……

9. Datum ispitnog izvješća:……

10. Broj ispitnog izvješća: ……

11. Napomene: (ako ih ima) ……

12. Mjesto:……

(1) Razlikovni broj države koja je dodijelila/proširila/odbila/povukla homologaciju (vidjeti odredbe o homologaciji u Pravilniku).
(2) Prekrižiti suvišno.

13. Datum: .....

14. Potpis: .....

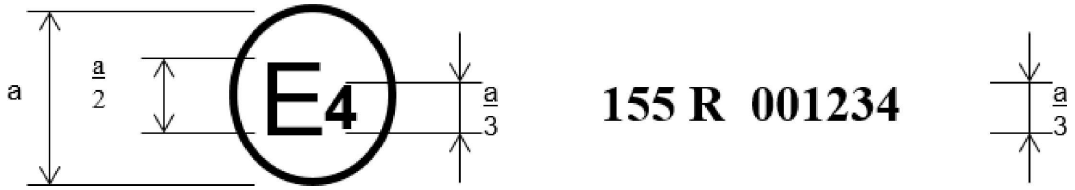
15. Priloženo je kazalo informacijskog paketa podnesenog homologacijskom tijelu, koji se može dobiti na zahtjev.

PRILOG 3.

Izgled homologacijskih oznaka

PREDLOŽAK A

(vidjeti stavak 4.2. ovog Pravilnika)



a = 8 mm (najmanje)

Ova homologacijska oznaka pričvršćena na vozilo označava da je taj tip cestovnog vozila homologiran u Nizozemskoj (E 4) na temelju pravilnika br. 155 pod homologacijskim brojem 001234. Prve dvije znamenke homologacijskog broja označavaju da je homologacija dodijeljena u skladu sa zahtjevima iz ovog Pravilnika u izvornoj verziji (00).

PRILOG 4.

PREDLOŽAK CERTIFIKATA O SUKLADNOSTI SUSTAVA ZA UPRAVLJANJE KIBERSIGURNOŠĆU

Certifikat o sukladnosti sustava za upravljanje kibersigurnošću

s Pravilnikom UN-a br. 155

Broj certifikata [*referentni broj*]

[……. *homologacijsko tijelo*]

potvrđuje da je

proizvođač: ……

adresa proizvođača: ……

sukladan s odredbama stavka 7.2. Pravilnika br. 155.

Provjere su provedene (datum): ……

od (ime i adresa homologacijskog tijela ili tehničke službe): ……

Broj izvješća: ……

Certifikat važi do: […… *datum*]

Sastavljeno u: […… *mjesto*]

[……*datum*]

[……*potpis*]

Prilozi: proizvođačev opis sustava za upravljanje kibersigurnošću

PRILOG 5.

Popis prijetnji i odgovarajućih protumjera

1. Ovaj se Prilog sastoji od tri dijela. U dijelu A ovog Priloga opisane su referentne prijetnje, slabe točke i metode napada. U dijelu B ovog Priloga opisane su protumjere prijetnjama protiv tipova vozila. U dijelu C ovog Priloga opisane su protumjere prijetnjama protiv područja izvan vozila, npr. *back-end* informatičkoj infrastrukturi.

2. Proizvođači vozila dužni su u procjeni rizika i u odlučivanju o protumjerama koje moraju ugraditi uzeti u obzir dijelove A, B i C.

3. U dijelu A indeksirane su slabe točke, podijeljene u glavne skupine, s odgovarajućim primjerima. Tim se indeksiranjem u tablicama u dijelovima B i C svaki napad/slaba točka povezuje s popisom odgovarajućih protumjera.

4. U analizi prijetnji uzimaju se u obzir i moguće posljedice napada. To može poslužiti da bi se utvrdila težina rizika i da se utvrde dodatni rizici. Među mogućim posljedicama napada mogu biti:

   (a) ugrožen siguran rad vozila;

   (b) prekinut rad funkcija vozila;

   (c) izmijenjen softver s utjecajem na radni učinak;

   (d) izmijenjen softver, ali bez posljedica na rad;

   (e) povreda cjelovitosti podataka;

   (f) povreda povjerljivosti podataka;

   (g) gubitak raspoloživosti podataka;

   (h) drugo, među ostalim kriminal.

DIO A

Slabe točke i metode napada povezane s prijetnjama

Prijetnje i povezane slabe točke ili metode napada razvrstane su u glavne skupine i opisane u tablici A1.

Tablica A1

Popis slabih točaka ili metoda napada povezanih s prijetnjama

Glavna podjela i potpodjela prijetnji/slabih točaka s opisom			Primjer slabe točke ili metode napada	
4.3.1. Prijetnje koje se odnose na *back-end* poslužitelje povezane s vozilima u uporabi	1.	*Back-end* poslužitelji iskorišteni za napad na vozilo ili krađu podataka	1.1.	Zlouporaba prava osoblja (napad iznutra)
			1.2.	Neovlašten pristup poslužitelju s interneta (putem stražnjih ulaza, neispravljenih slabih točaka softvera, napada putem SQL-a ili na druge načine)
			1.3.	Neovlašten fizički pristup poslužitelju (npr. priključivanjem USB memorije u poslužitelj ili čitanjem sadržaja nekog drugog medija)
	2.	Ometanje usluga *back-end* poslužitelja koje utječe na rad vozila	2.1.	Napad na back-end poslužitelj zbog kojeg potonji ne može raditi, npr. zbog napada ne može komunicirati s vozilima i pružati usluge na koje se vozila oslanjaju

Glavna podjela i potpodjela prijetnji/slabih točaka s opisom			Primjer slabe točke ili metode napada	
	3.	Izgubljeni ili ugroženi podaci povezani s vozilima smješteni na *back-end* poslužiteljima („povreda podataka”)	3.1.	Zlouporaba prava osoblja (napad iznutra)
			3.2.	Gubitak informacija u oblaku; osjetljivi podaci mogu biti izgubljeni zbog napada ili slučajnih nesreća ako su pohranjeni kod treće strane pružatelja usluga u oblaku
			3.3.	Neovlašten pristup poslužitelju s interneta (putem stražnjih ulaza, neispravljenih slabih točaka softvera, napada putem SQL-a ili drugih načina)
			3.4.	Neovlašten fizički pristup poslužitelju (npr. priključivanjem USB memorije u poslužitelj ili čitanjem sadržaja nekog drugog medija)
			3.5.	Povreda podataka u obliku nenamjeravanog dijeljenja podataka (npr. administratorske pogreške)
4.3.2. Prijetnje vozilima preko njihovih komunikacijskih kanala	4.	Lažiranje poruka ili podataka koje vozilo prima	4.1.	Lažiranje poruka (npr. V2X poruke za kooperativnu informiranost ili poruke za koordinaciju manevra, poruke GNSS-a itd.) imitiranjem
			4.2.	Sybilin napad (lažiranje drugih vozila tako da se čini da na cesti postoji mnogo vozila)
	5.	Komunikacijski kanali iskorišteni za neovlašteno manipuliranje, brisanje ili druge izmjene koda/podataka u vozilima	5.1.	Moguće je ubaciti kod putem komunikacijskih kanala, npr. nedopušteno modificirani softver u binarnom obliku može biti ubačen u komunikacijski protok
			5.2.	Moguće je manipulirati kodom/podacima u vozilu putem komunikacijskih kanala
			5.3.	Moguće je prebrisati kod/podatke u vozilu putem komunikacijskih kanala
			5.4.	Moguće je izbrisati kod/podatke u vozilu putem komunikacijskih kanala
			5.5.	Moguće je unijeti kod/podatke u vozilo putem komunikacijskih kanala (pisanje podataka ili koda)
	6.	Moguće je dopustiti prihvaćanje nevjerodostojnih/ nepouzdanih poruka putem komunikacijskih kanala ili je moguće iskoristiti slabe točke komunikacijskih kanala za napad lažiranjem sesija/ ponavljanjem sesija	6.1.	Prihvaćanje informacija iz nepouzdanog ili nevjerodostojnog izvora
			6.2.	Napad putem posrednika (*man in the middle*)/ otimanje sesije
			6.3.	Napad ponavljanjem sesije, npr. napad na komunikacijsku pristupnu točku, znači napad koji omogućava napadaču da softver elektroničke upravljačke jedinice ili integrirani softver pristupne točke zamijeni starijom verzijom softvera
	7.	Moguće je otkrivanje informacija, na primjer, prisluškivanjem komunikacije ili dopuštanjem neovlaštenog pristupa osjetljivim datotekama i mapama	7.1.	Presretanje informacija/interferencijske emisije/ praćenje komunikacija
			7.2.	Dobivanje neovlaštenog pristupa osjetljivim datotekama i mapama

Glavna podjela i potpodjela prijetnji/slabih točaka s opisom			Primjer slabe točke ili metode napada	
	8.	Napadi uskraćivanjem usluga putem komunikacijskih kanala radi ometanja funkcija vozila	8.1.	Slanje velike količine neispravnih podataka informatičkom sustavu vozila tako da ga se onemogući u uobičajenom pružanju usluga
			8.2.	Crna rupa, vrsta napada u kojoj napadač blokira poruke poslane vozilima kako bi prekinuo komunikaciju među vozilima
	9.	Neovlašteni korisnik može dobiti povlašteni pristup sustavima vozila	9.1.	Neovlašteni korisnik može dobiti povlašteni pristup, npr. root pristup
	10.	Virusi skriveni u komunikacijskim medijima mogu zaraziti sustave vozila	10.-1.	Virus skriven u komunikacijskim medijima ulazi u sustave vozila
	11.	Poruke koje vozilo primi (npr. X2V ili dijagnostičke poruke) ili koje se prenose unutar vozila sadržavaju zlonamjerni sadržaj	11.-1.	Zlonamjerne unutarnje poruke (npr. CAN)
			11.-2.	Zlonamjerne V2X poruke, npr. poruke infrastruktura-vozilo ili vozilo-vozilo (npr. CAM, DENM)
			11.-3.	Zlonamjerne dijagnostičke poruke
			11.-4.	Zlonamjerne poruke vlasničke vrste (poruke koje obično dolaze od OEM-a ili dobavljača sastavnog dijela/sustava/funkcije)
4.3.3. Prijetnje procesima ažuriranja softvera u vozilima	12.	Zlouporabljeni ili ugroženi procesi ažuriranja softvera	12.-1.	Ugroženi bežični procesi ažuriranja softvera; ovo obuhvaća lažni softver i integrirani softver za ažuriranje sustava
			12.-2.	Ugroženi lokalni/fizički procesi ažuriranja softvera; ovo obuhvaća lažni softver i integrirani softver za ažuriranje sustava
			12.-3.	Softver je nedopušteno izmijenjen prije procesa ažuriranja (tj. softver je pokvaren), iako je sam proces valjan
			12.-4.	Moguće je nevaljano ažuriranje softvera zbog ugroženih kriptografskih ključeva dobavljača
	13.	Moguće je blokirati legitimna ažuriranja softvera	13.-1.	Napad uskraćivanjem usluga na poslužitelj ili mrežu radi sprečavanja slanja kritičnih ažuriranja softvera i/ili aktiviranja svojstava za određene korisnike
4.3.4. Prijetnje vozilima zbog nenamjernih ljudskih radnji zbog kojih je izvođenje kibernapada lakše	15.	Legitimni akteri mogu učiniti nešto čime nenamjerno olakšavaju izvođenje kibernapada	15.-1.	Nevina je žrtva (npr. vlasnik, operater ili serviser) prevarena da poduzme radnju kojom se nenamjerno učitava zlonamjerni softver ili omogućava napad
			15.-2.	Ne primjenjuju se definirani sigurnosni postupci

Glavna podjela i potpodjela prijetnji/slabih točaka s opisom			Primjer slabe točke ili metode napada	
4.3.5. Prijetnje vozilima preko njihovih vanjskih veza i priključaka	16.	Manipulacije komunikacijom funkcija vozila omogućavaju kibernapad, što može uključivati telematiku; sustavi s dopuštenim daljinskim upravljanjem; sustavi koji koriste kratkodometnu bežičnu komunikaciju	16.-1.	Manipulacija funkcijama konstruiranima za daljinsko upravljanje sustavima, kao što su bežični ključ, imobilizator i infrastruktura za punjenje
			16.-2.	Manipulacija telematikom vozila (npr. manipuliranje izmjerenom temperaturom osjetljive robe, daljinsko otključavanje teretnih vrata)
			16.-3.	Interferencija s kratkodometnim bežičnim sustavima ili senzorima
	17.	Softver treće strane u sustavu, npr. aplikacije za zabavu, korištene kao vektor za napad na sustave vozila	17.-1.	Pokvarene aplikacije ili aplikacije sa slabim sigurnosnim mjerama korištene kao metoda za napad na sustave vozila
	18.	Uređaji priključeni na vanjska sučelja, npr. USB ili priključak OBD-a, korišteni kao sredstvo za napad na sustave vozila	18.-1.	Vanjska sučelja, kao što je USB priključak ili drugi, korištena kao mjesto napada, npr. ubacivanjem koda
			18.-2.	Mediji zaraženi virusom uneseni u sustav vozila
			18.-3.	Dijagnostički pristup (npr. hardverski ključevi u priključku OBD-a) korišteni za olakšavanje napada, npr. za manipulaciju parametrima vozila (izravno ili neizravno)
4.3.6. Prijetnje podacima/kodu vozila	19.	Izvlačenje podataka/koda iz vozila	19.-1.	Izvlačenje softvera, vlasničkog ili zaštićenog autorskim pravom, iz sustava vozila (piratiziranje proizvoda)
			19.-2.	Neovlašteni pristup podacima koji se odnose na privatnost vlasnika, kao što su podaci o osobnom identitetu, podaci o bankovnom računu, podaci iz adresara, podaci o lokaciji, elektronički identifikator vozila itd.
			19.-3.	Vađenje kriptografskih ključeva
	20.	Manipulacija podataka/koda u vozilu	20.-1.	Nezakonite/neovlaštene promjene elektroničkog identifikatora vozila
			20.-2.	Prevara s identitetom; na primjer, ako korisnik želi prikazati drugi identitet kad komunicira sa sustavima za naplatu cestarine i proizvođačevom *back-end* infrastrukturom
			20.-3.	Radnje za zaobilaženje sustava za praćenje (npr. hakiranje/nedopušteni zahvati/blokiranje poruka kao što su podaci ODR Trackera ili broj pokretanja)
			20.-4.	Manipuliranje podacima radi krivotvorenja podataka o vožnji vozila (npr. kilometraža, brzina vožnje, smjer vožnje itd.)
			20.-5.	Neovlaštene promjene podataka dijagnostičkog sustava
	21.	Brisanje podataka/koda	21.-1.	Neovlašteno brisanje zapisa događaja u sustavu ili manipulacija tim zapisima
	22.	Unošenje zlonamjernog softvera	22.-2.	Unošenje zlonamjernog softvera ili aktivnost zlonamjernog softvera

Glavna podjela i potpodjela prijetnji/slabih točaka s opisom			Primjer slabe točke ili metode napada	
	23.	Unošenje novog softvera ili prebrisivanje postojećeg softvera	23.-1.	Lažiranje softvera upravljačkog ili informacijskog sustava vozila
	24.	Ometanje sustava ili prekid rada	24.-1.	Uskraćivanje usluga može se uzrokovati na unutarnjoj mreži tako da se CAN sabirnica preplavi ili da se izazovu pogreške ECU-a visokom stopom slanja poruka
	25.	Manipulacija parametrima vozila	25.-1.	Neovlašteni pristup radi krivotvorenja konfiguracijskih parametara ključnih funkcija vozila, npr. podaci za kočenje, prag aktivacije zračnog jastuka itd.
			25.-2.	Neovlašteni pristup radi krivotvorenja parametara punjenja, npr. napon punjenja, snaga punjenja, temperatura baterije itd.
4.3.7. Potencijalne slabe točke koje se mogu iskoristiti ako nisu dovoljno zaštićene ili ojačane	26.	Kriptografske tehnologije mogu biti ugrožene ili je moguće da nisu primijenjene u dovoljnoj mjeri	26.-1.	Napadač može razbiti šifru zbog kombinacije kratkih ključeva za šifriranje i dugog valjanja ključeva
			26.-2.	Nedovoljno korištenje kriptografskih algoritama za zaštitu osjetljivih sustava
			26.-3.	Korištenje već ili uskoro zastarjelih kriptografskih algoritama
	27.	Dijelovi ili materijali mogu biti ugroženi radi omogućavanja napada na vozila	27.-1.	Hardver ili softver s konstrukcijskim rješenjima zbog kojih je napad moguć ili koji ne ispunjava konstrukcijske kriterije za zaustavljanje napada
	28.	Moguće su slabe točke zbog softverskog ili hardverskog razvoja	28.-1.	Pogreške u softveru. Prisutnost pogrešaka u softveru može biti osnova potencijalno iskoristivih slabih točaka. To osobito vrijedi ako softver nije testiran kako bi se provjerilo da nije prisutan poznat loš kod/pogreške i kako bi se smanjio rizik od nepoznatog lošeg koda/pogrešaka.
			28.-2.	Moguće je da korištenje elemenata zaostalih iz razvoja (npr. priključak za debugiranje, JTAG-ov priključak, mikroprocesori, razvojni certifikati, programerske šifre...) omogući pristup ECU-ima ili napadačima da više ovlasti
	29.	Slabe točke zbog projekta mreže	29.-1.	Otvoreni suvišni internetski portovi putem kojih je moguć pristup mrežnim sustavima
			29.-2.	Zaobilaženje razdvajanja mreže radi stjecanja kontrole. konkretan primjer je korištenje nezaštićenih pristupnih točaka (npr. pristupnih točaka kamion-prikolica) radi zaobilaženja zaštita i ostvarivanja pristupa drugim dijelovima mreže u svrhu zlonamjernih radnji, npr. slanja arbitrarnih poruka na CAN sabirnici
	31.	Moguć je nenamjerni prijenos podataka	31.-1.	Povreda podataka; osobni podaci mogu procuriti kad se promijeni korisnik automobila (npr. automobil je prodan ili služi kao vozilo za najam s novim najmoprimcima)

Glavna podjela i potpodjela prijetnji/slabih točaka s opisom			Primjer slabe točke ili metode napada	
	32.	Fizičko manipuliranje sustavima može omogućiti napad	32.-1.	Manipulacija elektronikom, npr. u vozilo je ugrađen neovlašteni hardver kojim je omogućen „napad putem posrednika” Zamjena ovlaštene elektronike (npr. senzora) neovlaštenim hardverom Manipulacija podacima prikupljenima senzorom (npr. korištenje magneta da se utječe na senzor Hallova efekta povezan s mjenjačem)

DIO B

Protumjere za prijetnje vozilima

1. Protumjere za prijetnje vrste „Komunikacijski kanali vozila”

Protumjere za prijetnje vrste „Komunikacijski kanali vozila” navedene su u tablici B1.

Tablica B1

Protumjera za prijetnje vrste „Komunikacijski kanali vozila”

Upućivanje na tablicu A1	Prijetnje vrste „Komunikacijski kanali vozila”	Upućivanje	Protumjera
4.1.	Lažiranje poruka (npr. V2X poruke za kooperativnu informiranost ili poruke za koordinaciju manevra, poruke GNSS-a itd.) imitiranjem	M10	Vozilo mora provjeravati vjerodostojnost i cjelovitost primljenih poruka.
4.2.	Sybilin napad (lažiranje drugih vozila tako da se čini da na cesti postoji mnogo vozila)	M11	Moraju se uvesti sigurnosne mjere za pohranu kriptografskih ključeva (npr. hardverski sigurnosni moduli).
5.1.	Moguće je ubaciti kod u kod/podatke u vozilu putem komunikacijskih kanala, npr. nedopušteno modificirani softver u binarnom obliku može biti ubačen u komunikacijski protok	M10 M6	Vozilo mora provjeravati vjerodostojnost i cjelovitost primljenih poruka. Kako bi se rizik u sustavima smanjio na najmanju moguću mjeru, sigurnosni aspekti moraju biti ugrađeni u njih pri projektiranju.
5.2.	Moguće je manipulirati kodom/podacima u vozilu putem komunikacijskih kanala	M7	Da bi se zaštitili podaci/kod sustava, moraju se primijeniti tehnike i koncepti kontrole pristupa.
5.3.	Moguće je prebrisati kod/podatke u vozilu putem komunikacijskih kanala		
5.4. 21.1.	Moguće je izbrisati kod/podatke u vozilu putem komunikacijskih kanala		
5.5.	Moguće je unijeti kod/podatke u sustave vozila putem komunikacijskih kanala (pisanje podataka ili koda)		

Upućivanje na tablicu A1	Prijetnje vrste „Komunikacijski kanali vozila”	Upućivanje	Protumjera
6.1.	Prihvaćanje informacija iz nepouzdanog ili nevjerodostojnog izvora	M10	Vozilo mora provjeravati vjerodostojnost i cjelovitost primljenih poruka.
6.2.	Napad putem posrednika (*man in the middle*)/otimanje sesije	M10	Vozilo mora provjeravati vjerodostojnost i cjelovitost primljenih poruka.
6.3.	Napad ponavljanjem sesije, npr. napad na komunikacijsku pristupnu točku, znači napad koji omogućava napadaču da softver elektroničke upravljačke jedinice ili integrirani softver pristupne točke zamijeni starijom verzijom softvera		
7.1.	Presretanje informacija/interferencijske emisije/praćenje komunikacija	M12	Povjerljivi podaci koji se šalju vozilu ili iz vozila moraju biti zaštićeni.
7.2.	Dobivanje neovlaštenog pristupa osjetljivim datotekama i mapama	M8	Koncept sustava i kontrole pristupa ne bi trebali neovlaštenom osoblju dopustiti pristup osobnim ili sistemskim ključnim podacima. Za primjer sigurnosnih kontrola vidjeti OWASP.
8.1.	Slanje velike količine neispravnih podataka informatičkom sustavu vozila tako da ga se onemogući u uobičajenom pružanju usluga	M13	Moraju se ugraditi mjere za otkrivanje napada uskraćivanjem usluge i vraćanje u ispravno stanje.
8.2.	Crna rupa, vrsta napada u kojoj se prekida komunikacija među vozilima blokiranjem prijenosa poruka drugim vozilima	M13	Moraju se ugraditi mjere za otkrivanje napada uskraćivanjem usluge i vraćanje u ispravno stanje.
9.1.	Neovlašteni korisnik može dobiti povlašteni pristup, npr. root pristup	M9	Moraju se ugraditi mjere za sprečavanje i otkrivanje neovlaštenog pristupa.
10.1.	Virus skriven u komunikacijskim medijima ulazi u sustave vozila	M14	Moraju se razmotriti mjere za zaštitu sustava od skrivenih virusa/zlonamjernog softvera.
11.1.	Zlonamjerne unutarnje poruke (npr. CAN)	M15	Moraju se razmotriti mjere za otkrivanje zlonamjernih unutarnjih poruka ili aktivnosti.
11.2.	Zlonamjerne V2X poruke, npr. poruke infrastruktura-vozilo ili vozilo-vozilo (npr. CAM, DENM)	M10	Vozilo mora provjeravati vjerodostojnost i cjelovitost primljenih poruka.
11.3.	Zlonamjerne dijagnostičke poruke		
11.4.	Zlonamjerne poruke vlasničke vrste (poruke koje obično dolaze od OEM-a ili dobavljača sastavnog dijela/sustava/funkcije)		

2. Protumjere za prijetnje vrste „Proces ažuriranja”

Protumjere za prijetnje vrste „Proces ažuriranja” navedene su u tablici B2.

Tablica B2

Protumjere za prijetnje vrste „Proces ažuriranja”

Upućivanje na tablicu A1	Prijetnje vrste „Proces ažuriranja”	Upućivanje	Protumjera
12.1.	Ugroženi bežični procesi ažuriranja softvera; ovo obuhvaća lažni softver i integrirani softver za ažuriranje sustava	M16	Za proces ažuriranja moraju se upotrebljavati sigurni postupci.
12.2.	Ugroženi lokalni/fizički procesi ažuriranja softvera; ovo obuhvaća lažni softver i integrirani softver za ažuriranje sustava		
12.3.	Softver je nedopušteno izmijenjen prije procesa ažuriranja (tj. softver je pokvaren), iako je sam proces valjan		
12.4.	Moguće je nevaljano ažuriranje softvera zbog ugroženih kriptografskih ključeva dobavljača	M11	Za pohranu kriptografskih ključeva moraju postojati sigurnosne kontrole.
13.1.	Napad uskraćivanjem usluga na poslužitelj ili mrežu radi sprečavanja slanja kritičnih ažuriranja softvera i/ili aktiviranja svojstava za određene korisnike	M3	U *back-end* sustavima moraju postojati sigurnosne kontrole. Ako su *back-end* poslužitelji od ključne važnosti za pružanje usluga, moraju postojati mjere za vraćanje u ispravno stanje u slučaju kvara sustava. Za primjer sigurnosnih kontrola vidjeti OWASP.

3. Protumjere za prijetnje vrste „Nenamjerne ljudske radnje zbog kojih je izvođenje kibernapada lakše”

Protumjere za prijetnje vrste „Nenamjerne ljudske radnje zbog kojih je izvođenje kibernapada lakše” navedene su u tablici B3.

Tablica B3

Protumjere za prijetnje vrste „Nenamjerne ljudske radnje zbog kojih je izvođenje kibernapada lakše”

Upućivanje na tablicu A1	Protumjere za prijetnje vrste „Nenamjerne ljudske radnje”	Upućivanje	Protumjera
15.1.	Nevina je žrtva (npr. vlasnik, operater ili serviser) prevarena da poduzme radnju kojom se nenamjerno učitava zlonamjerni softver ili omogućava napad	M18	Moraju se uvesti mjere za definiranje i kontrolu korisničkih uloga i pristupnih ovlasti, koje se moraju temeljiti na načelu dodjeljivanja samo nužnih prava na pristup.

Upućivanje na tablicu A1	Protumjere za prijetnje vrste „Nenamjerne ljudske radnje”	Upućivanje	Protumjera
15.2.	Ne primjenjuju se definirani sigurnosni postupci	M19	Organizacije su se dužne pobrinuti da se sigurnosni postupci definiraju i primjenjuju, što uključuje evidentiranje radnji i pristupa povezanih s upravljanjem sigurnosnim funkcijama.

4. Protumjere za prijetnje vrste „Vanjske veze i priključke”

Protumjere za prijetnje vrste „Vanjske veze i priključke” navedene su u tablici B4.

Tablica B4

Protumjere za prijetnje vrste „Vanjske veze i priključke”

Upućivanje na tablicu A1	Prijetnje vrste „Vanjske veze i priključke”	Upućivanje	Protumjera
16.1.	Manipulacija funkcijama konstruiranima za daljinsko upravljanje sustavima vozila, kao što su bežični ključ, imobilizator i infrastruktura za punjenje	M20	U sustavima s daljinskim pristupom moraju postojati sigurnosne kontrole.
16.2.	Manipulacija telematikom vozila (npr. manipuliranje izmjerenom temperaturom osjetljive robe, daljinsko otključavanje teretnih vrata)		
16.3.	Interferencija s kratkodometnim bežičnim sustavima ili senzorima		
17.1.	Pokvarene aplikacije ili aplikacije sa slabim sigurnosnim mjerama korištene kao metoda za napad na sustave vozila	M21	Softver mora biti sigurnosno ocijenjen, autentificiran i zaštićene cjelovitosti. Moraju se primjenjivati sigurnosne kontrole radi smanjivanja rizika od softvera treće strane koji je namijenjen za izvršavanje u vozilu ili za koji se može predvidjeti da će se izvršavati u njemu.
18.1.	Vanjska sučelja, npr. USB ili drugi priključci, korištena kao mjesto napada, npr. ubacivanjem koda	M22	Na vanjskim sučeljima moraju postojati sigurnosne kontrole.
18.2.	Mediji zaraženi virusima uneseni u sustav vozila		
18.3.	Dijagnostički pristup (npr. hardverski ključevi u priključku OBD-a) korišteni za olakšavanje napada, npr. za manipulaciju parametrima vozila (izravno ili neizravno)	M22	Na vanjskim sučeljima moraju postojati sigurnosne kontrole.

5. Protumjere za prijetnje vrste „Potencijalni ciljevi ili motivi za napad”

Protumjere za prijetnje vrste „Potencijalni ciljevi ili motivi za napad” navedene su u tablici B5.

Tablica B5

Protumjere za prijetnje vrste „Potencijalni ciljevi ili motivi za napad”

Upućivanje na tablicu A1	Prijetnje vrste „Potencijalni ciljevi ili motivi za napad”	Upućivanje	Protumjera
19.1.	Izvlačenje softvera, vlasničkog ili zaštićenog autorskim pravom, iz sustava vozila (piratiziranje proizvoda / ukradeni softver)	M7	Da bi se zaštitili podaci/kod sustava, moraju se primijeniti tehnike i koncepti kontrole pristupa. Za primjer sigurnosnih kontrola vidjeti OWASP.
19.2.	Neovlašteni pristup podacima koji se odnose na privatnost vlasnika, kao što su podaci o osobnom identitetu, podaci o bankovnom računu, podaci iz adresara, podaci o lokaciji, elektronički identifikator vozila itd.	M8	Koncept sustava i kontrole pristupa ne bi trebali neovlaštenom osoblju dopustiti pristup osobnim ili sistemskim ključnim podacima. Za primjere sigurnosnih kontrola vidjeti OWASP.
19.3.	Vađenje kriptografskih ključeva	M11	Moraju se uvesti sigurnosne mjere za pohranu kriptografskih ključeva, npr. sigurnosni moduli.
20.1.	Nezakonite/neovlaštene promjene elektroničkog identifikatora vozila	M7	Da bi se zaštitili podaci/kod sustava, moraju se primijeniti tehnike i koncepti kontrole pristupa. Za primjer sigurnosnih kontrola vidjeti OWASP.
20.2.	Prevara s identitetom; na primjer, ako korisnik želi prikazati drugi identitet kad komunicira sa sustavima za naplatu cestarine i proizvođačevom *back-end* infrastrukturom		
20.3.	Radnje za zaobilaženje sustava za praćenje (npr. hakiranje/nedopušteni zahvati/ blokiranje poruka kao što su podaci ODR Trackera ili broj pokretanja)	M7	Da bi se zaštitili podaci/kod sustava, moraju se primijeniti tehnike i koncepti kontrole pristupa. Za primjer sigurnosnih kontrola vidjeti OWASP. Protumjera za napade u obliku manipulacije podacima koji su usmjereni na senzore ili emitirane podatke može biti uspoređivanje podataka iz različitih izvora.
20.4.	Manipuliranje podacima radi krivotvorenja podataka o vožnji vozila (npr. kilometraža, brzina vožnje, smjer vožnje itd.)		
20.5.	Neovlaštene promjene podataka dijagnostičkog sustava		
21.1.	Neovlašteno brisanje zapisa događaja u sustavu ili manipulacija tim zapisima	M7	Da bi se zaštitili podaci/kod sustava, moraju se primijeniti tehnike i koncepti kontrole pristupa. Za primjer sigurnosnih kontrola vidjeti OWASP.
22.2.	Unošenje zlonamjernog softvera ili aktivnost zlonamjernog softvera	M7	Da bi se zaštitili podaci/kod sustava, moraju se primijeniti tehnike i koncepti kontrole pristupa. Za primjer sigurnosnih kontrola vidjeti OWASP.
23.1.	Lažiranje softvera upravljačkog ili informacijskog sustava vozila		

Upućivanje na tablicu A1	Prijetnje vrste „Potencijalni ciljevi ili motivi za napad”	Upućivanje	Protumjera
24.1.	Uskraćivanje usluga može se na unutarnjoj mreži uzrokovati tako da se CAN sabirnica preplavi ili da se izazovu pogreške ECU-a visokom stopom slanja poruka	M13	Moraju se ugraditi mjere za otkrivanje napada uskraćivanjem usluge i vraćanje u ispravno stanje.
25.1.	Neovlašteni pristup radi krivotvorenja konfiguracijskih parametara ključnih funkcija vozila, npr. podaci za kočenje, prag aktivacije zračnog jastuka itd.	M7	Da bi se zaštitili podaci/kod sustava, moraju se primijeniti tehnike i koncepti kontrole pristupa. Za primjer sigurnosnih kontrola vidjeti OWASP.
25.2.	Neovlašteni pristup radi krivotvorenja parametara punjenja, npr. napon punjenja, snaga punjenja, temperatura baterije itd.		

6. Protumjere za prijetnje vrste „Potencijalne slabe točke koje se mogu iskoristiti ako nisu dovoljno zaštićene ili ojačane”

Protumjere za prijetnje vrste „Potencijalne slabe točke koje se mogu iskoristiti ako nisu dovoljno zaštićene ili ojačane” navedene su u tablici B6.

Tablica B6

Protumjere za prijetnje vrste „Potencijalne slabe točke koje se mogu iskoristiti ako nisu dovoljno zaštićene ili ojačane”

Upućivanje na tablicu A1	Prijetnje vrste „Potencijalne slabe točke koje se mogu iskoristiti ako nisu dovoljno zaštićene ili ojačane”	Upućivanje	Protumjera
26.1.	Napadač može razbiti šifru zbog kombinacije kratkih ključeva za šifriranje i dugog valjanja ključeva	M23	U softverskom i hardverskom razvoju moraju se primjenjivati najbolji primjeri iz prakse u području kibersigurnosti.
26.2.	Nedovoljno korištenje kriptografskih algoritama za zaštitu osjetljivih sustava		
26.3.	Korištenje zastarjelih kriptografskih algoritama		
27.1.	Hardver ili softver s konstrukcijskim rješenjima zbog kojih je napad moguć ili koji ne ispunjava konstrukcijske kriterije za zaustavljanje napada	M23	U softverskom i hardverskom razvoju moraju se primjenjivati najbolji primjeri iz prakse u području kibersigurnosti.
28.1.	Prisutnost pogrešaka u softveru može biti osnova potencijalno iskoristivih slabih točaka. To osobito vrijedi ako softver nije testiran kako bi se provjerilo da nije prisutan poznat loš kod/pogreške i kako bi se smanjio rizik od nepoznatog lošeg koda/pogrešaka.	M23	U softverskom i hardverskom razvoju moraju se primjenjivati najbolji primjeri iz prakse u području kibersigurnosti. Ispitivanje kibersigurnosti mora biti dovoljno opsežno.

Upućivanje na tablicu A1	Prijetnje vrste „Potencijalne slabe točke koje se mogu iskoristiti ako nisu dovoljno zaštićene ili ojačane”	Upućivanje	Protumjera
28.2.	Moguće je da korištenje elemenata zaostalih iz razvoja (npr. priključak za debugiranje, JTAG-ov priključak, mikroprocesori, razvojni certifikati, programerske šifre...) napadaču omogući pristup ECU-ima ili da više ovlasti		
29.1.	Otvoreni suvišni internetski portovi putem kojih je moguć pristup mrežnim sustavima		
29.2.	Zaobilaženje razdvajanja mreže radi stjecanja kontrole. Konkretan primjer je korištenje nezaštićenih pristupnih točaka (npr. pristupnih točaka kamion-prikolica) radi zaobilaženja zaštita i ostvarivanja pristupa drugim dijelovima mreže u svrhu zlonamjernih radnji, npr. slanja arbitrarnih poruka na CAN sabirnici	M23	U softverskom i hardverskom razvoju moraju se primjenjivati najbolji primjeri iz prakse u području kibersigurnosti. U koncipiranju sustava i integraciji sustava moraju se primjenjivati najbolji primjeri iz prakse u području kibersigurnosti.

7. Protumjere za prijetnje vrste „Gubitak podataka iz vozila/povreda podataka iz vozila”

Protumjere za prijetnje vrste „Gubitak podataka iz vozila/povreda podataka iz vozila” navedene su u tablici B7.

Tablica B7

Protumjere za prijetnje vrste „Gubitak podataka iz vozila/povreda podataka iz vozila”

Upućivanje na tablicu A1	Prijetnje vrste „Gubitak podataka iz vozila/povreda podataka iz vozila”	Upućivanje	Protumjera
31.1.	Povreda podataka; može doći do povrede osobnih podataka kad se promijeni korisnik automobila (npr. automobil je prodan ili služi kao vozilo za najam s novim najmoprimcima)	M24	U pohrani osobnih podataka moraju se primjenjivati najbolji primjeri iz prakse radi zaštite cjelovitosti i povjerljivosti podataka.

8. Protumjere za prijetnje vrste „Fizičko manipuliranje sustavima radi omogućavanja napada”

Protumjere za prijetnje vrste „Fizičko manipuliranje sustavima radi omogućavanja napada” navedene su u tablici B8.

Tablica B8

Protumjere za prijetnje vrste „Fizičko manipuliranje sustavima radi omogućavanja napada”

Upućivanje na tablicu A1	Prijetnje vrste „Fizičko manipuliranje sustavima radi omogućavanja napada”	Upućivanje	Protumjera
32.1.	Manipulacija hardverom OEM-a, npr. u vozilo je ugrađen neovlašteni hardver kojim je omogućen „napad putem posrednika”	M9	Moraju se ugraditi mjere za sprečavanje i otkrivanje neovlaštenog pristupa.

DIO C

Protumjere za prijetnje izvan vozila

1. Protumjere za prijetnje vrste „*Back-end* poslužitelji”

Protumjere za prijetnje vrste „*Back-end* poslužitelji” navedene su u tablici C1.

Tablica C1

Protumjere za prijetnje vrste „*Back-end* poslužitelji”

Upućivanje na tablicu A1	Protumjere za prijetnje vrste „Back-end poslužitelji”	Upućivanje	Protumjera
1.1. & 3.1.	Zlouporaba prava osoblja (napad iznutra)	M1	U *back-end* sustavima moraju se primjenjivati sigurnosne kontrole radi svođenja rizika od unutarnjeg napada na najmanju moguću mjeru.
1.2. & 3.3.	Neovlašten pristup poslužitelju s interneta (putem stražnjih ulaza, neispravljenih slabih točaka softvera, napada putem SQL-a ili drugih načina)	M2	U *back-end* sustavima moraju se primjenjivati sigurnosne kontrole radi svođenja neovlaštenog pristupa na najmanju moguću mjeru. Za primjer sigurnosnih kontrola vidjeti OWASP.
1.3. & 3.4.	Neovlašten fizički pristup poslužitelju (npr. priključivanjem USB memorije u poslužitelj ili čitanjem sadržaja nekog drugog medija)	M8	Koncept sustava i kontrole pristupa ne bi trebali neovlaštenom osoblju dopustiti pristup osobnim ili sistemskim ključnim podacima.
2.1.	Napad na back-end poslužitelj zbog kojeg potonji ne može raditi, npr. zbog napada ne može komunicirati s vozilima i pružati usluge na koje se vozila oslanjaju	M3	U *back-end* sustavima moraju postojati sigurnosne kontrole. Ako su *back-end* poslužitelji od ključne važnosti za pružanje usluga, moraju postojati mjere za vraćanje u ispravno stanje u slučaju kvara sustava. Za primjer sigurnosnih kontrola vidjeti OWASP.
3.2.	Gubitak informacija u oblaku; osjetljivi podaci mogu biti izgubljeni zbog napada ili slučajnih nesreća ako su pohranjeni kod treće strane pružatelja usluga u oblaku	M4	Moraju se primjenjivati sigurnosne kontrole radi svođenja rizika povezanog s računalstvom u oblaku na najmanju moguću mjeru. Za primjer sigurnosnih kontrola vidjeti OWASP-ove i NCSC-ove smjernice za računalstvo u oblaku.
3.5.	Povreda podataka u obliku nenamjeravanog dijeljenja podataka (npr. administratorske pogreške, čuvanje podataka na poslužiteljima u servisima)	M5	U back-end sustavima moraju se primjenjivati sigurnosne kontrole radi sprečavanja povreda podataka. Za primjer sigurnosnih kontrola vidjeti OWASP.

2. Protumjere za prijetnje vrste „Nenamjerne ljudske radnje”

Protumjere za prijetnje vrste „Nenamjerne ljudske radnje” navedene su u tablici C2.

Tablica C2

Protumjere za prijetnje vrste „Nenamjerne ljudske radnje”

Upućivanje na tablicu A1	Protumjere za prijetnje vrste „Nenamjerne ljudske radnje”	Upućivanje	Protumjera
15.1.	Nevina je žrtva (npr. vlasnik, operater ili serviser) prevarena da poduzme radnju kojom se nenamjerno učitava zlonamjerni softver ili omogućava napad	M18	Moraju se uvesti mjere za definiranje i kontrolu korisničkih uloga i pristupnih ovlasti, koje se moraju temeljiti na načelu dodjeljivanja samo nužnih prava na pristup.
15.2.	Ne primjenjuju se definirani sigurnosni postupci	M19	Organizacije su se dužne pobrinuti da se sigurnosni postupci definiraju i primjenjuju, što uključuje evidentiranje radnji i pristupa povezanih s upravljanjem sigurnosnim funkcijama.

3. Protumjere za prijetnje vrste „Fizički gubitak podataka”

Protumjere za prijetnje vrste „Fizički gubitak podataka” navedene su u tablici C3.

Tablica C3

Protumjere za prijetnje vrste „Fizički gubitak podataka”

Upućivanje na tablicu A1	Prijetnje vrste „Fizički gubitak podataka”	Upućivanje	Protumjera
30.1.	Oštećenja koja je uzrokovala treća strana; osjetljivi podaci mogu biti izgubljeni ili ugroženi zbog fizičkog oštećenja u slučaju prometne nesreće ili krađe	M24	U pohrani osobnih podataka moraju se primjenjivati najbolji primjeri iz prakse radi zaštite cjelovitosti i povjerljivosti podataka. Za primjer sigurnosnih kontrola vidjeti ISO/SC27/WG5.
30.2.	Gubitak zbog neusklađenosti u DRM-u (upravljanje digitalnim pravima); moguće je da se korisnikovi podaci izbrišu zbog problema s DRM-om		
30.3.	Moguće je da se osjetljivi podaci izgube ili njihova cjelovitost naruši zbog habanja informatičkih sastavnih dijelova, što može uzrokovati daljnje posljedice (npr. u slučaju izmjene ključeva)		