Právny účinok podľa medzinárodného práva verejného majú iba originálne texty EHK OSN. Status tohto predpisu a dátum nadobudnutia jeho platnosti je potrebné overiť v poslednom znení dokumentu EHK OSN o statuse TRANS/WP.29/343, ktorý je k dispozícii na internetovej stránke: http://www.unece.org/trans/main/wp29/wp29wgs/wp29gen/wp29fdocstts.html

# Predpis OSN č. 155 – Jednotné ustanovenia na účely typového schvaľovania vozidiel vzhľadom na kybernetickú bezpečnosť a systém riadenia kybernetickej bezpečnosti [2021/387]

Dátum nadobudnutia platnosti: 22. januára 2021

Tento dokument slúži výhradne ako dokumentačný nástroj. Autentickými a právne záväznými sú texty:

— ECE/TRANS/WP.29/2020/79,

— ECE/TRANS/WP.29/2020/94 a

— ECE/TRANS/WP.29/2020/97.

OBSAH

PREDPIS

1. Rozsah pôsobnosti
2. Vymedzenie pojmov
3. Žiadosť o typové schválenie
4. Označenia
5. Typové schválenie
6. Osvedčenie o zhode systému riadenia kybernetickej bezpečnosti
7. Špecifikácie
8. Zmena typu vozidla a rozšírenie typového schválenia
9. Zhoda výroby
10. Sankcie v prípade nezhody výroby
11. Definitívne zastavenie výroby
12. Názvy a adresy technických služieb zodpovedných za vykonávanie schvaľovacích skúšok a názvy a adresy schvaľovacích úradov

PRÍLOHY

1 Informačný dokument

2 Oznámenie

3 Usporiadanie značky typového schválenia

4 Vzor osvedčenia o zhode systému riadenia kybernetickej bezpečnosti

5 Zoznam hrozieb a príslušných zmierňujúcich opatrení

## 1. ROZSAH PÔSOBNOSTI

1.1. Tento predpis sa vzťahuje na vozidlá kategórie M a N vzhľadom na kybernetickú bezpečnosť.

Tento predpis sa vzťahuje aj na vozidlá kategórie O, pokiaľ sú vybavené aspoň jednou elektronickou riadiacou jednotkou.

1.2. Tento predpis sa vzťahuje aj na vozidlá kategórie $L_6$ a $L_7$, ak sú vybavené funkciami automatizovanej jazdy úrovne 3 alebo vyššej, ako sa stanovuje v Referenčnom dokumente s vymedzeniami pojmu automatizovanej jazdy v rámci pracovnej skupiny WP.29 a so všeobecnými zásadami na vypracovanie predpisu OSN o automatizovaných vozidlách (ECE/TRANS/WP.29/1140).

1.3. Týmto predpisom nie sú dotknuté ostatné predpisy OSN, regionálne ani vnútroštátne právne predpisy, ktorými sa upravuje prístup oprávnených strán k vozidlu, jeho údajom, funkciám a zdrojom a podmienky takéhoto prístupu. Nie je ním dotknuté ani uplatňovanie vnútroštátnych a regionálnych právnych predpisov o ochrane súkromia a fyzických osôb v súvislosti so spracovaním ich osobných údajov.

1.4. Týmto predpisom nie sú dotknuté ostatné predpisy OSN, vnútroštátne ani regionálne právne predpisy, ktorými sa upravuje vývoj a montáž/systémová integrácia náhradných dielov a komponentov, fyzických a digitálnych, vzhľadom na kybernetickú bezpečnosť.

2. VYMEDZENIE POJMOV

Na účely tohto predpisu sa uplatňuje toto vymedzenie pojmov:

2.1. „Typ vozidla“ sú vozidlá, ktoré sa nelíšia minimálne v týchto podstatných aspektoch:

a) určenie typu vozidla výrobcom;

b) podstatné aspekty elektrickej/elektronickej architektúry a externých rozhraní z hľadiska kybernetickej bezpečnosti.

2.2. „Kybernetická bezpečnosť“ je stav, pri ktorom sú cestné vozidlá a ich funkcie chránené pred kybernetickými hrozbami pre elektrické alebo elektronické komponenty.

2.3. „Systém riadenia kybernetickej bezpečnosti (CSMS)“ je systematický prístup založený na rizikách, ktorým sa vymedzujú organizačné procesy, povinnosti a riadenie na riešenie rizík spojených s kybernetickými hrozbami pre vozidlá a na ochranu vozidiel pred kybernetickými útokmi.

2.4. „Systém“ je súbor komponentov a/alebo podsystémov, ktorý plní určitú funkciu alebo funkcie.

2.5. „Vývojová fáza“ je obdobie pred typovým schválením typu vozidla.

2.6. „Výrobná fáza“ označuje dĺžku trvania výroby typu vozidla.

2.7. „Povýrobná fáza“ je obdobie, počas ktorého sa typ vozidla už nevyrába až do konca životnosti všetkých vozidiel daného typu. Vozidlá, medzi ktoré sa začleňuje špecifický typ vozidla, budú počas tejto fázy prevádzkyschopné, nebudú sa však už vyrábať. Táto fáza sa skončí vtedy, keď už nie sú žiadne prevádzkyschopné vozidlá špecifického typu vozidla.

2.8. „Zmierňujúce opatrenie“ je opatrenie, ktorým sa znižuje riziko.

2.9. „Riziko“ je možnosť, že daná hrozba bude schopná zneužiť zraniteľnosti vozidla, čím vznikne škoda organizácii alebo jednotlivcovi.

2.10. „Posudzovanie rizika“ je súhrnný proces zisťovania, rozpoznávania a opisu rizík (identifikácia rizika) s cieľom porozumieť povahe rizika a stanoviť jeho úroveň (analýza rizika) a porovnania výsledkov analýzy rizika s kritériami rizika s cieľom určiť, či je riziko a/alebo jeho závažnosť prijateľná alebo prípustná (hodnotenie rizika).

2.11. „Riadenie rizika“ sú koordinované činnosti na usmernenie a riadenie organizácie s ohľadom na riziko.

2.12. „Hrozba“ je možná príčina neželanej udalosti, ktorá môže mať za následok vznik ujmy systému, organizácii alebo jednotlivcovi.

2.13. „Zraniteľnosť“ je slabá stránka prostriedku alebo zmierňujúceho opatrenia, ktorú môže zneužiť jedna alebo viacero hrozieb.

3. ŽIADOSŤ O TYPOVÉ SCHVÁLENIE

3.1. Žiadosť o typové schválenie typu vozidla vzhľadom na kybernetickú bezpečnosť predkladá výrobca vozidla alebo jeho riadne splnomocnený zástupca.

3.2. K žiadosti musia byť v troch vyhotoveniach priložené ďalej uvedené dokumenty s týmito údajmi:

3.2.1. Opis typu vozidla vzhľadom na položky uvedené v prílohe 1 k tomuto predpisu.

3.2.2. V prípadoch, keď sa na informácie vzťahuje právo duševného vlastníctva alebo sú osobitným know-how výrobcu alebo jeho dodávateľov, poskytne výrobca alebo jeho dodávatelia dostatočné informácie, ktoré umožnia riadne uskutočnenie kontrol uvedených v tomto predpise. S takýmito informáciami sa zaobchádza ako s dôvernými.

3.2.3. Osvedčenie o zhode systému riadenia kybernetickej bezpečnosti podľa bodu 6 tohto predpisu.

3.3. Dokumentácia musí byť dostupná v dvoch častiach:

a) oficiálny dokumentačný súbor na typové schválenie, ktorý obsahuje materiál uvedený v prílohe 1, ktorý sa poskytne schvaľovaciemu úradu alebo jeho technickej službe v čase predloženia žiadosti o typového schválenie. Tento dokumentačný súbor použije schvaľovací úrad alebo jeho technická služba ako základnú referenciu pre postup schvaľovania. Schvaľovací úrad alebo jeho technická služba zabezpečí, aby tento dokumentačný súbor ostal dostupný aspoň 10 rokov od definitívneho zastavenia výroby typu vozidla;

b) výrobca si môže ponechať dodatočné materiály týkajúce sa požiadaviek tohto predpisu, v čase typového schválenia ich však musí sprístupniť na kontrolu. Výrobca zabezpečí, aby všetky materiály sprístupnené na kontrolu počas typového schvaľovania ostali prístupné aspoň počas obdobia 10 rokov, ktoré sa začína dátumom definitívneho zastavenia výroby typu vozidla.

4. OZNAČENIE

4.1. Na každé vozidlo zodpovedajúce typu vozidla schválenému podľa tohto predpisu sa zreteľne a na ľahko dostupnom mieste špecifikovanom v schvaľovacom formulári upevní medzinárodná značka typového schválenia, ktorá pozostáva z:

4.1.1. písmena „E“ v kružnici, za ktorým nasleduje rozlišovacie číslo krajiny, ktorá typové schválenie udelila;

4.1.2. čísla tohto predpisu, za ktorým nasleduje písmeno „R“, pomlčka a schvaľovacie číslo schválenia vpravo od kružnice opísanej v bode 4.1.1.

4.2. Ak vozidlo zodpovedá typu vozidla schválenému podľa jedného alebo viacerých ďalších predpisov pripojených k uvedenej dohode v krajine, ktorá udelila schválenie podľa tohto predpisu, symbol uvedený v bode 4.1.1 sa nemusí opakovať; v takom prípade sa číslo predpisu a schvaľovacie číslo, ako aj doplnkové symboly všetkých predpisov, na základe ktorých bolo schválenie udelené v krajine, ktorá udelila schválenie podľa tohto predpisu, umiestňujú do vertikálnych stĺpcov vpravo od symbolu uvedeného v bode 4.1.1.

4.3. Značka typového schválenia musí byť ľahko čitateľná a nezmazateľná.

4.4. Značka typového schválenia sa umiestni v blízkosti štítku s údajmi o vozidle pripevneného výrobcom alebo na ňom.

4.5. Príklady usporiadania značky typového schválenia sú uvedené v prílohe 3 k tomuto predpisu.

5. TYPOVÉ SCHVÁLENIE

5.1. Schvaľovacie úrady podľa potreby udeľujú typové schválenie vzhľadom na kybernetickú bezpečnosť iba tým typom vozidiel, ktoré spĺňajú požiadavky tohto predpisu.

5.1.1. Schvaľovací úrad alebo technická služba prostredníctvom kontrol dokumentov overia, že výrobca vozidla prijal potrebné opatrenia relevantné pre typ vozidla s cieľom:

a) prostredníctvom dodávateľského reťazca zhromaždiť a overiť informácie požadované podľa tohto predpisu, a tak preukázať, že riziká spojené s dodávateľmi boli zistené a že sú pod kontrolou;

b) zdokumentovať posúdenie rizík (ktoré sa uskutočnilo vo vývojovej fáze alebo spätne), výsledky skúšok a zmierňujúce opatrenia použité na daný typ vozidla vrátane konštrukčných informácií podporujúcich posudzovanie rizika;

c) implementovať primerané opatrenia v oblasti kybernetickej bezpečnosti v konštrukcii typu vozidla;

d) odhaľovať a reagovať na možné kybernetické útoky;

e) zaznamenávať údaje na podporu odhaľovania kybernetických útokov a zabezpečenia schopnosti v oblasti forenznej analýzy údajov s cieľom umožniť analýzu úspešných kybernetických útokov alebo pokusov o ne.

5.1.2. Schvaľovací úrad alebo technická služba prostredníctvom skúšky vozidla daného typu overia, že výrobca vozidla implementoval opatrenia v oblasti kybernetickej bezpečnosti, ktoré úrad alebo služba zdokumentovali. Skúšky vykoná schvaľovací úrad alebo technická služba, a to buď samostatne, alebo v spolupráci s výrobcom vozidla, prostredníctvom odberu vzoriek. Odber vzoriek sa okrem iného zameria na riziká, ktoré boli počas posudzovania rizík vyhodnotené ako vysoké.

5.1.3. Schvaľovací úrad alebo technická služba odmietnu udeliť typové schválenie vzhľadom na kybernetickú bezpečnosť v prípade, keď výrobca vozidla nesplnil jednu alebo viaceré požiadavky uvedené v bode 7.3, predovšetkým:

a) výrobca vozidla nevykonal úplné posúdenie rizika uvedené v bode 7.3.3, a to aj v prípade, keď výrobca nezohľadnil všetky riziká súvisiace s hrozbami uvedenými v časti A prílohy 5;

b) výrobca vozidla nezabezpečil typ vozidla proti rizikám identifikovaným pri posudzovaní rizika, ktoré uskutočnil výrobca vozidla, alebo neimplementoval primerané zmierňujúce opatrenia v súlade s bodom 7;

c) výrobca vozidla nezaviedol vhodné a primerané opatrenia, aby zabezpečil vyhradené prostredia v type vozidla (ak existuje) na ukladanie a spúšťanie popredajného softvéru, služieb, aplikácií alebo údajov;

d) výrobca vozidla pred udelením typového schválenia neimplementoval vhodné a dostatočné skúšky na overenie účinnosti zavádzaných bezpečnostných opatrení.

5.1.4. Schvaľovací úrad, ktorý vykonáva posudzovanie, takisto odmietne udeliť typové schválenie vzhľadom na kybernetickú bezpečnosť, ak schvaľovací úrad alebo technická služba nedostali od výrobcu vozidla dostatočné informácie na posúdenie kybernetickej bezpečnosti typu vozidla.

5.2. Oznámenie o typovom schválení, jeho rozšírení alebo zamietnutí podľa tohto predpisu sa oznámi stranám dohody z roku 1958, ktoré uplatňujú tento predpis, prostredníctvom formulára zodpovedajúceho vzoru uvedenému v prílohe 2 k tomuto predpisu.

5.3. Schvaľovacie úrady neudelia žiadne typové schválenie bez toho, aby overili, že výrobca zaviedol vyhovujúce opatrenia a postupy na primerané riadenie aspektov kybernetickej bezpečnosti uvedených v tomto predpise.

5.3.1. Schvaľovací úrad a jeho technické služby musia okrem kritérií stanovených v dodatku 2 k dohode z roku 1958 zabezpečiť, aby:

a) mali kvalifikovaný personál s primeranými zručnosťami v oblasti kybernetickej bezpečnosti a s osobitnými znalosťami súvisiacimi s posudzovaním rizika automobilov ([1]);

b) implementovali postupy týkajúce sa jednotného hodnotenia podľa tohto predpisu.

([1]) Napr. ISO 26262-2018, ISO/PAS 21448, ISO/SAE 21434.

5.3.2. Každá zmluvná strana, ktorá uplatňuje tento predpis, prostredníctvom svojho schvaľovacieho úradu upovedomí a informuje ostatné schvaľovacie úrady zmluvných strán uplatňujúcich tento predpis OSN o postupe a kritériách prijatých ako základ, podľa ktorého oznamujúci úrad posudzuje vhodnosť opatrení prijatých v súlade s týmto predpisom, a najmä s bodmi 5.1, 7.2 a 7.3.

Výmena informácií bude prebiehať a) iba pred prvým udelením typového schválenia v súlade s týmto predpisom a b) zakaždým, keď sa aktualizuje postup alebo kritériá posudzovania.

Tieto informácie sú určené na výmenu na účely zhromažďovania a analýzy najlepších postupov a s cieľom zabezpečiť konvergentné uplatňovanie tohto predpisu všetkými schvaľovacími úradmi uplatňujúcimi tento predpis.

5.3.3. Informácie uvedené v bode 5.3.2 sa nahrajú v anglickom jazyku do zabezpečenej internetovej databázy DETA ([2]) zriadenej Európskou hospodárskou komisiou OSN v náležitom čase a najneskôr 14 dní pred prvým udelením typového schválenia podľa dotknutých postupov a kritérií posudzovania. Informácie musia byť dostatočné na pochopenie toho, aké minimálne úrovne výkonnosti schvaľovací úrad prijal ku každej osobitnej požiadavke uvedenej v bode 5.3.2, ako aj toho, aké postupy a opatrenia uplatňuje, aby overil dodržanie týchto minimálnych úrovní výkonnosti ([3]).

5.3.4. Schvaľovacie úrady, ktoré dostanú informácie uvedené v bode 5.3.2, môžu pripomienky predložiť oznamujúcemu schvaľovaciemu úradu tak, že ich nahrajú do databázy DETA do 14 dní od dátumu oznámenia.

5.3.5. Ak udeľujúci schvaľovací úrad nemôže zohľadniť pripomienky, ktoré dostal podľa bodu 5.3.4, schvaľovacie úrady, ktoré pripomienky poslali, a udeľujúci schvaľovací úrad požiadajú o ďalšie objasnenie v súlade s dodatkom 6 k dohode z roku 1958. Príslušná podporná pracovná skupina ([4]) Svetového fóra pre harmonizáciu predpisov o vozidlách (WP.29) zodpovedná za tento predpis dohodne spoločný výklad postupov a kritérií posudzovania ([5]). Uplatňuje sa uvedený spoločný výklad a všetky schvaľovacie úrady budú vydávať typové schválenia podľa tohto predpisu v súlade s týmto výkladom.

5.3.6. Každý schvaľovací úrad, ktorý udeľuje typové schválenie podľa tohto predpisu, ostatným schvaľovacím úradom oznámi udelené typové schválenie. Schvaľovací úrad typové schválenie spoločne s doplňujúcou dokumentáciou nahrá v anglickom jazyku do databázy DETA ([6]), a to do 14 dní od dátumu udelenia typového schválenia.

5.3.7. Zmluvné strany môžu skúmať schválenia udelené na základe informácií nahratých v súlade s bodom 5.3.6. V prípade rozdielnych názorov zmluvných strán sa rozpory urovnajú v súlade s článkom 10 dohody z roku 1958 a s dodatkom 6 k tejto dohode. Zmluvné strany takisto o rozdielnych výkladoch v zmysle dodatku 6 k dohode z roku 1958 informujú príslušnú podpornú pracovnú skupinu Svetového fóra pre harmonizáciu predpisov o vozidlách (WP.29). Príslušná pracovná skupina podporí riešenie rozdielnych názorov a v prípade potreby sa vo veci môže poradiť s pracovnou skupinou WP.29.

5.4. Na účely bodu 7.2 tohto predpisu výrobca zabezpečí implementovanie aspektov kybernetickej bezpečnosti opísaných v tomto predpise.

---

([2]) https://www.unece.org/trans/main/wp29/datasharing.html.

([3]) Usmernenia týkajúce sa podrobných informácií (napr. o postupe, kritériách, úrovni výkonnosti), ktoré sa majú nahrať do databázy, a ich formátu sa poskytnú prostredníctvom vysvetľujúceho dokumentu, ktorý na siedme zasadnutie pracovnej skupiny pre automatizované/autonómne a prepojené vozidlá (GRVA) pripravuje osobitná skupina pre otázky kybernetickej bezpečnosti a šírenia údajov vzduchom.

([4]) Pracovná skupina pre automatizované/autonómne a prepojené vozidlá (GRVA).

([5]) Tento výklad sa zohľadní vo vysvetľujúcom dokumente uvedenom v poznámke pod čiarou k bodu 5.3.3.

([6]) Ďalšie informácie o minimálnych požiadavkách na dokumentačný súbor vypracuje pracovná skupina pre automatizované/autonómne a prepojené vozidlá (GRVA) na svojom siedmom zasadnutí.

6. OSVEDČENIE O ZHODE SYSTÉMU RIADENIA KYBERNETICKEJ BEZPEČNOSTI

6.1. Zmluvné strany vymenujú schvaľovací úrad, ktorý bude vykonávať posudzovanie výrobcu a vydá osvedčenie o zhode systému riadenia kybernetickej bezpečnosti.

6.2. Žiadosť o osvedčenie o zhode systému riadenia kybernetickej bezpečnosti predkladá výrobca vozidla alebo jeho riadne splnomocnený zástupca.

6.3. K žiadosti musia byť v troch vyhotoveniach priložené ďalej uvedené dokumenty s týmito údajmi:

6.3.1. dokumenty s opisom systému riadenia kybernetickej bezpečnosti;

6.3.2. podpísané vyhlásenie podľa vzoru vymedzeného v doplnku 1 k prílohe 1.

6.4. V rámci posudzovania výrobca vystaví vyhlásenie podľa vzoru vymedzeného v doplnku 1 k prílohe 1 a k spokojnosti schvaľovacieho úradu alebo jeho technickej služby preukáže, že má potrebné postupy na splnenie všetkých požiadaviek na kybernetickú bezpečnosť v súlade s týmto predpisom.

6.5. Po úspešnom ukončení posudzovania a doručení podpísaného vyhlásenia výrobcu vypracovaného podľa vzoru vymedzeného v doplnku 1 k prílohe 1 sa výrobcovi udelí osvedčenie s názvom Osvedčenie o zhode systému riadenia kybernetickej bezpečnosti podľa opisu v prílohe 4 k tomuto predpisu (ďalej len „osvedčenie o zhode systému riadenia kybernetickej bezpečnosti“).

6.6. Schvaľovací úrad alebo jeho technická služba na osvedčenie o zhode systému riadenia kybernetickej bezpečnosti použije vzor uvedený prílohe 4 k tomuto predpisu.

6.7. Pokiaľ nebolo odňaté, osvedčenie o zhode systému riadenia kybernetickej bezpečnosti platí najviac tri roky od dátumu doručenia osvedčenia.

6.8. Schvaľovací úrad, ktorý udelil osvedčenie o zhode systému riadenia kybernetickej bezpečnosti, môže kedykoľvek overiť, či sú požiadavky, ktoré sa naň vzťahujú, stále splnené. Ak už nie sú splnené požiadavky stanovené v tomto predpise, schvaľovací úrad osvedčenie o zhode systému riadenia kybernetickej bezpečnosti odníme.

6.9. Výrobca informuje schvaľovací úrad alebo jeho technickú službu o všetkých zmenách, ktoré majú vplyv na relevantnosť osvedčenia o zhode systému riadenia kybernetickej bezpečnosti. Schvaľovací úrad alebo jeho technická služba na základe konzultácie s výrobcom rozhodne, či sú potrebné nové kontroly.

6.10. V primeranom čase, aby schvaľovací úrad mohol dokončiť svoje posudzovanie pred uplynutím platnosti osvedčenia o zhode systému riadenia kybernetickej bezpečnosti, výrobca požiada o nové osvedčenie o zhode systému riadenia kybernetickej bezpečnosti alebo o predĺženie platnosti existujúceho osvedčenia. Schvaľovací úrad na základe kladného posúdenia vystaví nové osvedčenie o zhode systému riadenia kybernetickej bezpečnosti alebo predĺži jeho platnosť o ďalšie tri roky. Schvaľovací úrad overí, či systém riadenia kybernetickej bezpečnosti naďalej spĺňa požiadavky tohto predpisu. Schvaľovací úrad vystaví nové osvedčenie v prípadoch, keď bol schvaľovací úrad alebo jeho technická služba upozornený na zmeny a posúdenie týchto zmien bolo priaznivé.

6.11. Uplynutie platnosti výrobcovho osvedčenia o zhode systému riadenia kybernetickej bezpečnosti alebo jeho odňatie sa s ohľadom na typy vozidiel, pre ktoré je dotknutý systém riadenia kybernetickej bezpečnosti relevantný, považuje za zmenu typového schválenia, ako sa uvádza v bode 8, čo môže predstavovať aj odňatie typového schválenia v prípade, ak už nie sú splnené podmienky na udelenie schválenia.

7. ŠPECIFIKÁCIE

7.1. Všeobecné špecifikácie

7.1.1. Požiadavky tohto predpisu nesmú obmedzovať ustanovenia ani požiadavky ostatných predpisov OSN.

7.2. Požiadavky na systém riadenia kybernetickej bezpečnosti

7.2.1. Schvaľovací úrad alebo jeho technická služba na účely posúdenia overí, či výrobca vozidla zaviedol systém riadenia kybernetickej bezpečnosti, a skontroluje jeho súlad s týmto predpisom.

7.2.2. Systém riadenia kybernetickej bezpečnosti sa týka týchto aspektov:

7.2.2.1. Výrobca vozidla schvaľovaciemu úradu alebo technickej službe preukáže, že jeho systém riadenia kybernetickej bezpečnosti sa vzťahuje na tieto fázy:

a) vývojová fáza;

b) výrobná fáza;

c) povýrobná fáza.

7.2.2.2. Výrobca vozidla preukáže, že postupy používané v jeho systéme riadenia kybernetickej bezpečnosti zaisťujú primerané zohľadnenie bezpečnosti vrátane rizík a zmierňujúcich opatrení uvedených v prílohe 5. To zahŕňa:

a) postupy používané v organizácii výrobcu na riadenie kybernetickej bezpečnosti;

b) postupy používané na identifikáciu rizík pre typy vozidiel. V rámci týchto postupov sa zohľadnia hrozby uvedené v časti A prílohy 5 a ďalšie relevantné hrozby;

c) postupy používané na posudzovanie, kategorizáciu a riešenie identifikovaných rizík;

d) postupy, ktoré boli zavedené na overovanie primeraného riadenia identifikovaných rizík;

e) postupy používané na skúšky kybernetickej bezpečnosti typu vozidla;

f) postupy používané na zabezpečenie aktuálnosti posudzovania rizika;

g) postupy používané na monitorovanie kybernetických útokov, kybernetických hrozieb a zraniteľností v rámci typov vozidiel, ich odhaľovanie a reagovanie na ne a postupy používané na posúdenie, či implementované opatrenia v oblasti kybernetickej bezpečnosti sú so zreteľom na nové identifikované kybernetické hrozby a zraniteľnosti ešte účinné;

h) postupy používané na poskytovanie relevantných údajov na podporu analýzy úspešných kybernetických útokov alebo pokusov o ne.

7.2.2.3. Výrobca vozidla preukáže, že postupy používané v jeho systéme riadenia kybernetickej bezpečnosti zabezpečujú, že na základe kategorizácie uvedenej v bode 7.2.2.2 písm. c) a g) sa v primeranom časovom rámci zmiernia kybernetické hrozby a zraniteľnosti, ktoré si vyžadujú reakciu výrobcu vozidla.

7.2.2.4. Výrobca vozidla preukáže, že postupy používané v jeho systéme riadenia kybernetickej bezpečnosti zabezpečujú nepretržité monitorovanie uvedené v bode 7.2.2.2 písm. g). Tieto postupy:

a) zahŕňajú monitorovanie vozidiel po prvej evidencii;

b) zahŕňajú schopnosť odhaľovať kybernetické hrozby, zraniteľnosti a kybernetické útoky z údajov o vozidle a z denníka vozidla a analyzovať ich. Pri tejto schopnosti musia byť dodržané ustanovenia v bode 1.3 a právo na súkromie vlastníkov alebo vodičov automobilov, najmä pokiaľ ide o súhlas.

7.2.2.5. Výrobca vozidla musí preukázať, ako jeho systém riadenia kybernetickej bezpečnosti zvláda možné závislosti od zmluvných dodávateľov, poskytovateľov služieb alebo organizácií podriadených výrobcovi, pokiaľ ide o požiadavky bodu 7.2.2.2.

7.3. Požiadavky na typy vozidiel

7.3.1. Výrobca musí mať platné osvedčenie o zhode systému riadenia kybernetickej bezpečnosti relevantné pre schvaľovaný typ vozidla.

Ak však v prípade typových schválení udelených do 1. júla 2024 výrobca môže preukázať, že typ vozidla nemohol byť navrhnutý v súlade so systémom riadenia kybernetickej bezpečnosti, potom musí preukázať, že kybernetická bezpečnosť bola náležite zohľadnená vo vývojovej fáze dotknutého typu vozidla.

7.3.2. Výrobca vozidla v prípade schvaľovaného typu vozidla identifikuje riziká spojené s dodávateľmi a riadi ich.

7.3.3. Výrobca vozidla identifikuje kritické prvky typu vozidla a uskutoční vyčerpávajúce posúdenie rizika pre daný typ vozidla a identifikované riziká bude riešiť/riadiť primeraným spôsobom. V posúdení rizika sa zohľadnia jednotlivé prvky typu vozidla a ich vzájomné pôsobenie. Okrem toho sa v ňom zohľadní vzájomné pôsobenie so všetkými externými systémami. Pri posudzovaní rizík výrobca vozidla zohľadní riziká súvisiace so všetkými hrozbami uvedenými v časti A prílohy 5, ako aj všetky ostaté relevantné riziká.

7.3.4. Výrobca vozidla musí zabezpečiť typ vozidla proti rizikám identifikovaným pri posudzovaní rizika, ktoré uskutočnil výrobca vozidla. Na účely ochrany typu vozidla sa implementujú primerané zmierňujúce opatrenia. Implementované zmierňujúce opatrenia zahŕňajú všetky zmierňujúce opatrenia uvedené v častiach B a C prílohy 5, ktoré sú relevantné z hľadiska identifikovaných rizík. Ak však zmierňujúce opatrenie uvedené v časti B alebo C prílohy 5 nie je relevantné alebo dostatočné vzhľadom na identifikované riziko, výrobca vozidla zabezpečí implementovanie iného vhodného zmierňujúceho opatrenia.

Konkrétne v prípade typových schválení udelených do 1. júla 2024 výrobca vozidla zabezpečí, aby sa implementovalo iné vhodné zmierňujúce opatrenie, ak zmierňujúce opatrenie uvedené v časti B alebo C prílohy 5 nie je technicky realizovateľné. Príslušné posúdenie technickej uskutočniteľnosti výrobca poskytne schvaľovaciemu úradu.

7.3.5. Výrobca vozidla zavedie vhodné a primerané opatrenia, aby zabezpečil vyhradené prostredia v type vozidla (ak existuje) na ukladanie a spúšťanie popredajného softvéru, služieb, aplikácií alebo údajov.

7.3.6. Výrobca vozidla pred udelením typového schválenia vykoná vhodné a dostatočné skúšky na overenie účinnosti implementovaných bezpečnostných opatrení.

7.3.7. Výrobca vozidla implementuje opatrenia pre daný typ vozidla s cieľom:

a) odhaľovať kybernetické útoky proti vozidlám daného typu vozidla a predchádzať im;

b) podporiť monitorovaciu schopnosť výrobcu vozidla, pokiaľ ide o odhaľovanie hrozieb, zraniteľností a kybernetických útokov relevantných pre daný typ vozidla;

c) zabezpečiť schopnosti v oblasti forenznej analýzy údajov s cieľom umožniť analýzu úspešných kybernetických útokov alebo pokusov o ne.

7.3.8. Kryptografické moduly používané na účely tohto predpisu musia byť v súlade so spoločnými normami. V prípade, ak použité kryptografické moduly nie sú v súlade so spoločnými normami, výrobca vozidla musí odôvodniť ich použitie.

7.4. Ustanovenia týkajúce sa podávania správ

7.4.1. Výrobca vozidla aspoň raz ročne alebo v prípade potreby častejšie predloží schvaľovaciemu úradu alebo technickej službe správu o výsledku svojho monitorovania, ako sa uvádza v bode 7.2.2.2 písm. g), ktorá bude obsahovať relevantné informácie o nových kybernetických útokoch. Výrobca vozidla takisto schvaľovaciemu úradu alebo technickej službe predloží správu o tom, že zmierňujúce opatrenia v oblasti kybernetickej bezpečnosti implementované v prípade jeho typov vozidiel sú stále účinné, a o všetkých dodatočných opatreniach, ktoré výrobca prijal.

7.4.2. Schvaľovací úrad alebo technická služba overí poskytnuté informácie a v prípade potreby požiada výrobcu vozidla o nápravu akejkoľvek zistenej neúčinnosti.

V prípade, ak schvaľovací úrad považuje správu alebo reakciu za nedostatočnú, môže rozhodnúť o stiahnutí systému riadenia kybernetickej bezpečnosti v súlade s bodom 6.8.

8. ZMENA TYPU VOZIDLA A ROZŠÍRENIE TYPOVÉHO SCHVÁLENIA

8.1. Každá zmena typu vozidla ovplyvňujúca jeho technické vlastnosti z hľadiska kybernetickej bezpečnosti a/alebo dokumentácie vyžadovanej podľa tohto predpisu sa musí oznámiť schvaľovaciemu úrad, ktorý schválil typ vozidla. Schvaľovací úrad potom môže buď:

8.1.1. dospieť k názoru, že uskutočnené zmeny sú stále v súlade s požiadavkami existujúceho typového schválenia a dokumentáciou k nemu; alebo

8.1.2. pristúpiť k nevyhnutnému doplnkovému posudzovaniu podľa bodu 5 a v prípade potreby vyžadovať ďalší skúšobný protokol od technickej služby, ktorá je zodpovedná za vykonávanie skúšok.

8.1.3. Potvrdenie, rozšírenie alebo zamietnutie typového schválenia, v ktorom sú špecifikované zmeny, sa musí oznámiť prostredníctvom formulára oznámenia zodpovedajúceho vzoru uvedenému v prílohe 2 k tomuto predpisu. Schvaľovací úrad, ktorý vydáva rozšírenie schválenia, pridelí tomuto rozšíreniu poradové číslo a oznámi ho ostatným stranám dohody z roku 1958, ktoré uplatňujú tento predpis, prostredníctvom formulára oznámenia zodpovedajúceho vzoru uvedenému v prílohe 2 k tomuto predpisu.

9. ZHODA VÝROBY

9.1. Postupy na zabezpečenie zhody výroby musia byť v súlade s postupmi stanovenými v dodatku 1 k dohode z roku 1958 (E/ECE/TRANS/505/Rev.3), pričom musia byť splnené tieto požiadavky:

9.1.1. držiteľ typového schválenia musí zabezpečiť, aby boli zaznamenané výsledky skúšok zhody výroby a aby priložené dokumenty boli k dispozícii počas obdobia stanoveného po dohode so schvaľovacím úradom alebo technickou službou. Toto obdobie nesmie presiahnuť 10 rokov od dátumu definitívneho zastavenia výroby;

9.1.2. schvaľovací úrad, ktorý typové schválenie udelil, môže kedykoľvek overiť postupy kontroly zhody používané v jednotlivých výrobných závodoch. Tieto overovania sa zvyčajne vykonávajú každé tri roky.

10. SANKCIE V PRÍPADE NEZHODY VÝROBY

10.1. Typové schválenie udelené typu vozidla podľa tohto predpisu môže byť odňaté, ak nie sú splnené požiadavky uložené v tomto predpise alebo ak vozidlá zo vzorky nespĺňajú požiadavky tohto predpisu.

10.2. Ak schvaľovací úrad odníme typové schválenie, ktoré predtým udelil, bezodkladne to oznámi zmluvným stranám, ktoré uplatňujú tento predpis, a to prostredníctvom formulára oznámenia zodpovedajúceho vzoru uvedenému v prílohe 2 k tomuto predpisu.

11. DEFINITÍVNE ZASTAVENIE VÝROBY

11.1. Ak držiteľ typového schválenia úplne zastaví výrobu typu vozidla schváleného podľa tohto predpisu, informuje o tom úrad, ktorý typové schválenie udelil. Po prijatí príslušného oznámenia uvedený úrad o tom informuje ostatné zmluvné strany dohody, ktoré uplatňujú tento predpis, prostredníctvom kópie schvaľovacieho formulára, na konci ktorého je veľkými písmenami uvedená poznámka „VÝROBA ZASTAVENÁ“ spolu s podpisom a dátumom.

12. NÁZVY A ADRESY TECHNICKÝCH SLUŽIEB ZODPOVEDNÝCH ZA VYKONÁVANIE SCHVAĽOVACÍCH SKÚŠOK A NÁZVY A ADRESY SCHVAĽOVACÍCH ÚRADOV

12.1. Zmluvné strany dohody, ktoré uplatňujú tento predpis, oznámia sekretariátu Organizácie Spojených národov názvy a adresy technických služieb zodpovedných za vykonávanie schvaľovacích skúšok, ako aj názvy a adresy schvaľovacích úradov, ktoré schválenia udeľujú a ktorým sa majú zasielať formuláre potvrdzujúce udelenie, rozšírenie, zamietnutie alebo odňatie typového schválenia vydaného v iných krajinách.

*PRÍLOHA 1*

**Informačný dokument**

V prípade potreby sa nasledujúce údaje poskytnú v troch vyhotoveniach spolu so súpisom obsahu. Všetky výkresy sa dodávajú vo vhodnej mierke vo formáte A4 alebo poskladané na tento formát a sú dostatočne podrobné. Prípadné fotografie musia byť dostatočne podrobné.

1. Značka (obchodný názov výrobcu): .....

2. Typ a všeobecné obchodné označenie: .....

3. Prostriedky identifikácie typu, ak sú vyznačené na vozidle: .....

4. Umiestnenie tohto označenia: .....

5. Kategória vozidla: .....

6. Názov a adresa výrobcu/názov a adresa zástupcu výrobcu: .....

7. Názov a adresa montážnych závodov: .....

8. Fotografie a/alebo výkresy reprezentatívneho vozidla: .....

9. Kybernetická bezpečnosť

9.1. Všeobecné konštrukčné charakteristiky typu vozidla vrátane:

a) systémov vozidla, ktoré sú relevantné pre kybernetickú bezpečnosť typu vozidla;

b) komponentov systémov, ktoré sú relevantné pre kybernetickú bezpečnosť;

c) vzájomného pôsobenia týchto systémov s ostatnými systémami v rámci typu vozidla a externých rozhraní.

9.2. Schematické znázornenie typu vozidla

9.3. Číslo osvedčenia o zhode systému riadenia kybernetickej bezpečnosti: .....

9.4. Dokumenty pre typ vozidla, ktorý sa má schváliť, v ktorých sa opisujú výsledky posúdenia rizika a identifikované riziká: .....

9.5. Dokumenty pre typ vozidla, ktorý sa má schváliť, v ktorých sa opisujú zmierňujúce opatrenia implementované v súvislosti s uvedenými systémami alebo typom vozidla a spôsob, akým riešia uvedené riziká: .....

9.6. Dokumenty pre typ vozidla, ktorý sa má schváliť, v ktorých sa opisuje ochrana vyhradených prostredí pre popredajný softvér, služby, aplikácie alebo údaje: .....

9.7. Dokumenty pre typ vozidla, ktorý sa má schváliť, v ktorých sa opisuje, aké skúšky sa použili na overenie kybernetickej bezpečnosti typu vozidla a jeho systémov a výsledky týchto skúšok: .....

9.8. Opis ohľadov týkajúcich sa dodávateľského reťazca v súvislosti s kybernetickou bezpečnosťou: .....

*Doplnok 1k prílohe I*

**Vzor vyhlásenia výrobcu o zhode systému riadenia kybernetickej bezpečnosti**

Vyhlásenie výrobcu o zhode s požiadavkami na systém riadenia kybernetickej bezpečnosti

Názov výrobcu: .....

Adresa výrobcu: .....

..... (*názov výrobcu*) týmto potvrdzuje, že boli zavedené potrebné procesy na splnenie požiadaviek na systém riadenia kybernetickej bezpečnosti stanovených v bode 7.2 predpisu OSN č. 155 a že sa budú dodržiavať. ..... ..... .....

Miesto vyhotovenia: ..... (*miesto*)

Dátum: .....

Meno podpisovateľa: .....

Funkcia podpisovateľa: .....

.....

(*pečiatka a podpis zástupcu výrobcu*)

*PRÍLOHA 2*

**Oznámenie**

[Maximálny formát: A4 (210 × 297 mm)]


Vydal: Názov schvaľovacieho úradu:
.....
.....
.....

týkajúce sa (2) udelenia typového schválenia
rozšírenia typového schválenia
odňatia typového schválenia s účinnosťou od dd. mm. rrrr
zamietnutia typového schválenia
definitívneho zastavenia výroby

typu vozidla podľa predpisu OSN č. 155

Typové schválenie č.: .....

Rozšírenie č.: .....

Dôvod rozšírenia: .....

1. Značka (obchodný názov výrobcu): .....

2. Typ a všeobecné obchodné označenie: .....

3. Prostriedky identifikácie typu, ak sú vyznačené na vozidle: .....

3.1. Umiestnenie tohto označenia: .....

4. Kategória vozidla: .....

5. Názov a adresa výrobcu/meno a adresa zástupcu výrobcu: .....

6. Názov a adresa výrobného závodu: .....

7. Číslo osvedčenia o zhode systému riadenia kybernetickej bezpečnosti: .....

8. Technická služba zodpovedná za vykonávanie skúšok: .....

9. Dátum skúšobného protokolu: .....

10. Číslo skúšobného protokolu: .....

11. Poznámky: (ak sú) .....

12. Miesto: .....

13. Dátum: .....

14. Podpis: .....

15. Priložený je súpis informačného zväzku uchovávaného schvaľovacím úradom, ktorý je možné získať na požiadanie:

---

([1]) Rozlišovacie číslo krajiny, ktorá typové schválenie udelila/rozšírila/zamietla/odňala (pozri ustanovenia o typovom schválení v predpise).

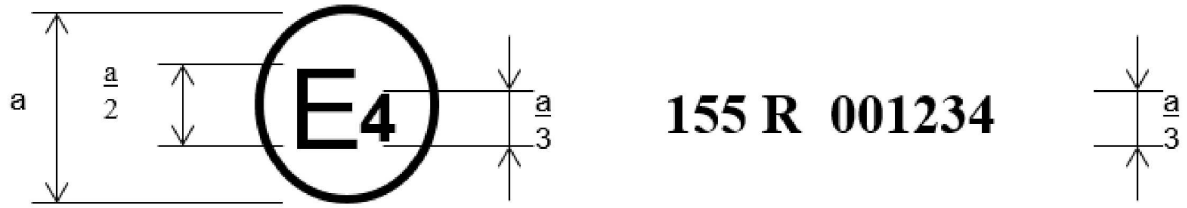
([2]) Nehodiace sa prečiarknite.

*PRÍLOHA 3*

**Usporiadanie značky typového schválenia**

Vzor A

(pozri bod 4.2 tohto predpisu)




a = min. 8 mm

Z uvedenej značky typového schválenia upevnenej na vozidlo vyplýva, že príslušný typ cestného vozidla bol schválený v Holandsku (E 4) podľa predpisu č. 155 a pod schvaľovacím číslom 001234. Prvé dve číslice schvaľovacieho čísla označujú, že typové schválenie bolo udelené v súlade s požiadavkami tohto predpisu v jeho pôvodnom znení (00).

*PRÍLOHA 4*

**Vzor osvedčenia o zhode systému riadenia kybernetickej bezpečnosti**

Osvedčenie o zhode systému riadenia kybernetickej bezpečnosti

s predpisom OSN č. 155

Číslo osvedčenia [*referenčné číslo*]

[……. *schvaľovací úrad*]

osvedčuje, že

Výrobca: ……

Adresa výrobcu: ……

spĺňa ustanovenia bodu 7.2 predpisu č. 155.

Kontroly vykonal dňa: ……

(názov a adresa schvaľovacieho úradu alebo technickej služby): ……

Číslo správy: ……

Osvedčenie je platné do [……*dátum*]

V [……*miesto*]

Dňa [……*dátum*]

[……*podpis*]

Prílohy: opis systému riadenia kybernetickej bezpečnosti výrobcom.

*PRÍLOHA 5*

**Zoznam hrozieb a príslušných zmierňujúcich opatrení**

1. Táto príloha sa skladá z troch častí. Časť A tejto prílohy obsahuje opis východísk pre hrozby, zraniteľnosti a spôsoby útoku. Časť B tejto prílohy obsahuje opis opatrení na zmiernenie hrozieb, ktoré sú určené pre typy vozidiel. Časť C tejto prílohy obsahuje opis opatrení na zmiernenie hrozieb, ktoré sú určené pre oblasti mimo vozidiel, napr. pre infraštruktúru IT.

2. Časť A, časť B a časť C sa zohľadňujú na účely posúdenia rizika a zmierňujúcich opatrení, ktoré majú implementovať výrobcovia vozidla.

3. Zraniteľnosti na vysokej úrovni a jej zodpovedajúcim príkladom je pridelené indexové číslo v časti A. Ten istý spôsob označovania sa používa aj v tabuľkách v častiach B a C s cieľom prepojiť každý útok/zraniteľnosť so zoznamom zodpovedajúcich zmierňujúcich opatrení.

4. V analýze hrozieb sa zohľadnia aj možné následky útoku, ktoré môžu pomôcť pri zisťovaní závažnosti rizika a pri identifikácii ďalších rizík. Medzi možné následky útoku môže patriť:

   a) narušená bezpečná prevádzka vozidla;

   b) zastavenie funkcií vozidla;

   c) úprava softvéru, zmena výkonnosti;

   d) upravený softvér, ale bez vplyvu na prevádzku;

   e) narušenie integrity údajov;

   f) narušenie dôvernosti údajov;

   g) strata dostupnosti údajov;

   h) iné vrátane trestnej činnosti.

Časť A. Zraniteľnosť alebo spôsob útoku v súvislosti s hrozbami

1. Vysoké úrovne opisov hrozieb a súvisiaca zraniteľnosť alebo spôsob útoku sa uvádzajú v tabuľke A1.

*Tabuľka A1*

**Zoznam zraniteľností alebo spôsobov útoku v súvislosti s hrozbami**

| Vysoké úrovne a podúrovne opisov zraniteľnosti/hrozby | | | Príklad zraniteľnosti alebo spôsobu útoku | |
|---|---|---|---|---|
| 4.3.1. Hrozby týkajúce sa serverov back-end v súvislosti s vozidlami v prevádzke | 1. | Servery back-end používané ako nástroje útoku na vozidlo alebo na extrakciu údajov | 1.1. | Zneužitie oprávnení zamestnancami (útok zvnútra) |
| | | | 1.2. | Neoprávnený internetový prístup na server (umožnený napríklad prostredníctvom zadných vrátok, neopravených zraniteľností softvéru operačného systému, napadnutia databázy SQL alebo iných prostriedkov) |
| | | | 1.3. | Neoprávnený fyzický prístup k serveru (ktorý sa uskutočnil napríklad pripojením USB kľúčov alebo iných médií k serveru) |
| | 2. | Prerušenie služieb servera back-end, čo má vplyv na prevádzku vozidla | 2.1. | Útok na server back-end má za následok, že server prestane fungovať, napríklad mu znemožní komunikáciu s vozidlami a poskytovanie služieb, od ktorých vozidlá závisia |

| Vysoké úrovne a podúrovne opisov zraniteľnosti/hrozby | | | Príklad zraniteľnosti alebo spôsobu útoku | |
|---|---|---|---|---|
| | 3. | Strata alebo zneužitie údajov súvisiacich s vozidlami uchovávaných na serveroch back-end (tzv. únik údajov) | 3.1. | Zneužitie oprávnení zamestnancami (útok zvnútra) |
| | | | 3.2. | Strata informácií v cloude. Keď sa údaje uchovávajú prostredníctvom poskytovateľov cloudových služieb tretích strán, v dôsledku útokov alebo nehôd môže dôjsť k strate citlivých údajov |
| | | | 3.3. | Neoprávnený internetový prístup na server (umožnený napríklad prostredníctvom zadných vrátok, neopravených zraniteľností softvéru operačného systému, napadnutia databázy SQL alebo iných prostriedkov) |
| | | | 3.4. | Neoprávnený fyzický prístup k serveru (ktorý sa uskutočnil napríklad pripojením USB kľúčov alebo iných médií k serveru) |
| | | | 3.5. | Únik informácií prostredníctvom neúmyselného zdieľania údajov (napr. chyby správcov) |
| 4.3.2. Hrozby pre vozidlá týkajúce sa ich komunikačných kanálov | 4. | Útok predstieraním iného odosielateľa správ alebo údajov prijímaných vozidlom | 4.1. | Útok predstieraním iného odosielateľa správ [napr. predstieranie komunikácie typu V2X (vozidlo s okolím – vehicle-to-everything) prostredníctvom bezdrôtovej technológie 802.11p počas jazdy v konvoji (tzv. platooning), správy systému GNSS atď.] |
| | | | 4.2. | Útok Sybil (tzv. Sybil attack) (s cieľom predstierať iné vozidlá, ako keby sa na ceste nachádzalo veľa vozidiel) |
| | 5. | Komunikačné kanály používané na neoprávnenú manipuláciu kódu/údajov uchovávaných vo vozidle, ich vymazanie alebo iné úpravy | 5.1. | Komunikačné kanály umožňujú vkladanie kódu, napríklad neoprávnene zmanipulovaný binárny kód softvéru by sa mohol vložiť do komunikačného prúdu údajov |
| | | | 5.2. | Komunikačné kanály umožňujú manipuláciu údajov/kódu uchovávaného vo vozidle |
| | | | 5.3. | Komunikačné kanály umožňujú prepisovanie údajov/kódu uchovávaného vo vozidle |
| | | | 5.4. | Komunikačné kanály umožňujú vymazanie údajov/kódu uchovávaného vo vozidle |
| | | | 5.5. | Komunikačné kanály umožňujú zavádzať do vozidla údaje/kód (zapisovanie údajov/kódu) |
| | 6. | Komunikačné kanály umožňujú akceptovať nedôveryhodné/ nespoľahlivé správy alebo sú zraniteľné voči ukradnutiu relácie/útokom prehratím | 6.1. | Prijímanie informácií z nespoľahlivého alebo nedôveryhodného zdroja |
| | | | 6.2. | Útok z pozície medzičlánku/ukradnutie relácie |
| | | | 6.3. | Útok prehratím, napríklad útok proti komunikačnej bráne útočníkovi umožňuje prejsť na staršiu verziu softvéru elektronickej riadiacej jednotky alebo firmvéru brány |

| Vysoké úrovne a podúrovne opisov zraniteľnosti/hrozby | | | Príklad zraniteľnosti alebo spôsobu útoku | |
|---|---|---|---|---|
| | 7. | Informácie je možné jednoducho zverejniť. Napríklad prostredníctvom odpočúvania komunikácie alebo umožnením neoprávneného prístupu k citlivým súborom alebo priečinkom | 7.1. | Zachytenie informácií/rušivé žiarenie/ monitorovanie komunikácií |
| | | | 7.2. | Získanie neoprávneného prístupu k súborom alebo údajom |
| | 8. | Útoky zahltením servera služby (DoS) prostredníctvom komunikačných kanálov na narušenie funkcií vozidla | 8.1. | Odosielanie veľkého množstva neplatných údajov do informačného systému vozidla, aby vozidlo nebolo schopné poskytovať služby bežným spôsobom |
| | | | 8.2. | Útok čiernej diery, keď s cieľom narušiť komunikáciu medzi vozidlami je útočník schopný blokovať správy medzi vozidlami |
| | 9. | Neprivilegovaný používateľ je schopný získať privilegovaný prístup do systémov vozidla | 9.1. | Neprivilegovaný používateľ je schopný získať privilegovaný prístup, napríklad administrátorský prístup |
| | 10. | Vírusy vložené v komunikačnom médiu sú schopné infikovať systémy vozidla | 10.1. | Vírus vložený v komunikačnom médiu infikuje systémy vozidla |
| | 11. | Správy prijímané vozidlom (napríklad V2X alebo diagnostické správy) alebo prenášané v rámci neho obsahujú škodlivý obsah | 11.1. | Škodlivé interné správy (napr. CAN) |
| | | | 11.2. | Škodlivé správy komunikácie typu V2X, napr. správy z infraštruktúry do vozidla alebo správy medzi vozidlami [napr. správy CAN, DENM (správy decentralizovaného oznámenia prostredia)] |
| | | | 11.3. | Škodlivé diagnostické správy |
| | | | 11.4. | Škodlivé súkromné správy (napr. správy bežne odosielané výrobcom pôvodného zariadenia alebo dodávateľom komponentu/systému/funkcie) |
| 4.3.3. Hrozby pre vozidlá týkajúce sa ich postupov aktualizácie | 12. | Zneužitie alebo ohrozenie postupov aktualizácie | 12.1. | Ohrozenie aktualizácií softvéru šírených vzduchom. Zahŕňa aj zhotovenie programu alebo firmvéru na aktualizáciu systému |
| | | | 12.2. | Ohrozenie lokálnych/fyzických postupov aktualizácie softvéru. Zahŕňa aj zhotovenie programu alebo firmvéru na aktualizáciu systému |
| | | | 12.3. | Softvér bol zmanipulovaný pred vykonaním aktualizácie (a preto je poškodený), hoci samotný proces aktualizácie je nedotknutý |

| Vysoké úrovne a podúrovne opisov zraniteľnosti/hrozby | | | Príklad zraniteľnosti alebo spôsobu útoku | |
|---|---|---|---|---|
| | | | 12.4. | Ohrozenie kryptografických kľúčov poskytovateľa softvéru tak, že sa tým umožní neplatná aktualizácia |
| | 13. | Je možné odmietnuť oprávnené aktualizácie | 13.1. | Útok zahltením aktualizačného servera alebo siete (DoS) s cieľom zabrániť sprístupneniu kritických aktualizácií softvéru a/alebo odblokovať funkcie pre zákazníkov |
| 4.3.4. Hrozby pre vozidlá, pokiaľ ide o neúmyselnú ľudskú činnosť, ktorá umožňuje kybernetický útok | 15. | Oprávnené subjekty môžu konať tak, že nevedomky umožnia kybernetický útok | 15.1. | Nevinná obeť (napr. vlastník, operátor alebo technik údržby) je oklamaná tak, aby podnikla nejaký krok s cieľom nevedomky nahrať malvér alebo umožniť útok |
| | | | 15.2. | Vymedzené bezpečnostné postupy sa nedodržiavajú |
| 4.3.5. Hrozby pre vozidlá týkajúce sa ich externej pripojiteľnosti a pripojení | 16. | Manipulácia funkcií pripojiteľnosti vozidla umožňuje kybernetický útok, čo môže zahŕňať telematiku, systémy umožňujúce operácie na diaľku a systémy využívajúce bezdrôtovú komunikáciu s krátkym dosahom | 16.1. | Manipulácia funkcií určených na prevádzku systémov na diaľku, ako je diaľkové ovládanie zamykania, imobilizér a nabíjacia stanica |
| | | | 16.2. | Manipulácia telematiky vozidla (napr. manipulácia merania teploty citlivých tovarov, diaľkové odomknutie dverí nákladného priestoru) |
| | | | 16.3. | Rušenie bezdrôtových systémov s krátkym dosahom alebo senzorov |
| | 17. | Hosťovaný softvér tretej strany, napr. zábavné aplikácie, použitý ako nástroj útoku proti systémom vozidla | 17.1. | Poškodené aplikácie alebo aplikácie so slabým softvérovým zabezpečením slúžiace ako spôsob útoku na systémy vozidla |
| | 18. | Zariadenia pripojené k externým rozhraniam, napr. do portov USB, portov palubného diagnostického systému (OBD), použité ako nástroj útoku proti systémom vozidla | 18.1. | Externé rozhrania, ako sú porty USB alebo iné porty, používané ako miesto vniknutia, napríklad prostredníctvom vloženia kódu |
| | | | 18.2. | Médiá infikované vírusom pripojené k systému vozidla |
| | | | 18.3. | Diagnostický prístup (napr. hardvérové kľúče v porte systému OBD) použitý na umožnenie útoku, napr. na manipuláciu parametrov vozidla (priamu alebo nepriamu) |
| 4.3.6. Hrozby pre údaje/kód vozidla | 19. | Extrahovanie údajov/kódu vozidla | 19.1. | Extrahovanie softvéru chráneného autorským právom alebo proprietárneho softvéru zo systémov vozidla (pirátstvo výrobkov) |
| | | | 19.2. | Neoprávnený prístup k informáciám o súkromí vlastníka, ako je osobná identita, informácie o platobnom účte, informácie z adresára, informácie o polohe, elektronický identifikačný kód vozidla atď. |
| | | | 19.3. | Extrahovanie kryptografických kľúčov |

| Vysoké úrovne a podúrovne opisov zraniteľnosti/hrozby | | | Príklad zraniteľnosti alebo spôsobu útoku | |
|---|---|---|---|---|
| | 20. | Manipulácia údajov/kódu vozidla | 20.1. | Nezákonné/nepovolené zmeny elektronického identifikačného kódu vozidla |
| | | | 20.2. | Podvod s osobnými údajmi. Napríklad v prípade, keď sa chce používateľ preukázať inou totožnosťou pri komunikácii so systémami mýta, so serverom výrobcu |
| | | | 20.3. | Opatrenie na obchádzanie monitorovacích systémov (napr. hakovanie/neoprávnená manipulácia/blokovanie správ, ako sú údaje o sledovaní záznamov ODR alebo počet spustení) |
| | | | 20.4. | Manipulácia údajov s cieľom falšovať údaje o jazde vozidla (napr. počet prejdených kilometrov, rýchlosť jazdy, navigačné pokyny pre vodičov atď.) |
| | | | 20.5. | Neoprávnené zmeny systémových diagnostických údajov |
| | 21. | Vymazanie údajov/kódu | 21.1. | Neoprávnené vymazanie/manipulácia systémových denníkov udalostí |
| | 22. | Zanesenie malvéru | 22.2. | Zavedenie škodlivého softvéru alebo pôsobenie škodlivého softvéru |
| | 23. | Zavedenie nového softvéru alebo prepísanie existujúceho softvéru | 23.1. | Zhotovenie softvéru riadiaceho alebo informačného systému vozidla |
| | 24. | Narušenie systémov alebo prevádzky | 24.1. | Odmietnutie služby sa môže spustiť napríklad v internej sieti zaplavením zbernice CAN alebo vyprovokovaním chýb v elektronickej riadiacej jednotke prostredníctvom vysokej miery odosielania správ |
| | 25. | Manipulácia parametrov vozidla | 25.1. | Neoprávnený prístup na sfalšovanie konfiguračných parametrov kľúčových funkcií vozidla, ako sú údaje o brzdách, prahová hodnota aktivácie airbagu atď. |
| | | | 25.2. | Neoprávnený prístup na sfalšovanie parametrov o nabíjaní, ako je nabíjacie napätie, nabíjací výkon, teplota batérie atď. |
| 4.3.7. Potenciálne zraniteľnosti, ktoré by bez dostatočnej ochrany alebo sprísnenia mohli byť zneužité | 26. | Kryptografické technológie môžu byť narušené alebo je ich uplatňovanie nedostatočné | 26.1. | Spojenie krátkych šifrovacích kľúčov a dlhého obdobia platnosti umožňuje útočníkovi prelomiť šifrovanie |
| | | | 26.2. | Nedostatočné využívanie kryptografických algoritmov na ochranu citlivých systémov |
| | | | 26.3. | Používanie kryptografických algoritmov, ktoré už sú alebo čoskoro budú zastarané |

| Vysoké úrovne a podúrovne opisov zraniteľnosti/hrozby | | | Príklad zraniteľnosti alebo spôsobu útoku | |
|---|---|---|---|---|
| | 27. | Mohlo by dôjsť k narušeniu častí alebo dodávok, čo by umožnilo útok proti vozidlám | 27.1. | Hardvér alebo softvér navrhnutý tak, aby umožnil útok alebo taký, ktorý nespĺňa kritériá projektovania na zastavenie útoku |
| | 28. | Vývoj softvéru alebo hardvéru umožňuje vznik zraniteľností | 28.1. | Softvérové chyby. Prítomnosť softvérových chýb môže predstavovať základ potenciálne zneužiteľných zraniteľností. To platí predovšetkým v prípade softvéru, ktorý nebol preskúšaný, aby sa overilo, že neobsahuje chybný kód/chyby, a aby sa znížilo riziko prítomnosti chybného kódu/chýb |
| | | | 28.2. | Používanie zvyškov z vývoja (napr. ladiace porty, porty JTAG, mikroprocesory, vývojové certifikáty, vývojárske heslá…) môže umožniť prístup k elektronickým riadiacim jednotkám alebo môže útočníkom umožniť získanie vyšších oprávnení |
| | 29. | Návrhom siete sa zavádzajú zraniteľnosti | 29.1. | Nadbytočné internetové porty zostávajú otvorené a poskytujú prístup k sieťovým systémom |
| | | | 29.2. | Obchádzanie oddelenia sietí s cieľom získať kontrolu. Konkrétnym príkladom je používanie nezabezpečených brán alebo prístupových bodov (ako sú brány prepájajúce ťahač a prípojné vozidlo) na obídenie zabezpečenia a na získanie prístupu do iných segmentov siete s cieľom vykonávať škodlivé úkony, ako je odosielanie arbitrárnych správ prostredníctvom zbernice CAN |
| | 31. | Môže dôjsť k neúmyselnému prenosu údajov | 31.1. | Únik informácií. K úniku osobných údajov môže dôjsť vtedy, keď automobil zmení používateľa (napr. pri predaji alebo pri nových prenajímateľoch, keď sa používa ako vozidlo na prenájom) |
| | 32. | Fyzická manipulácia systémov môže umožniť útok | 32.1. | Manipulácia elektronického zariadenia, napr. pridanie neschváleného elektronického zariadenia do vozidla, ktoré umožní útok z pozície medzičlánku<br>Výmena schváleného elektronického zariadenia (napr. senzorov) za neschválené elektronické zariadenie<br>Manipulácia informácií zhromaždených senzorom (napríklad použitím magnetu na ovplyvnenie Hallovho senzora pripojeného k prevodovej skrini) |

Časť B. Opatrenia na zmiernenie hrozieb určené pre vozidlá

1. Zmierňujúce opatrenia týkajúce sa komunikačných kanálov vozidiel

Opatrenia na zmiernenie hrozieb, ktoré súvisia s komunikačnými kanálmi vozidiel, sa uvádzajú v tabuľke B1.

*Tabuľka B1*

**Opatrenia na zmiernenie hrozieb, ktoré súvisia s komunikačnými kanálmi vozidiel**

| Odkaz na tabuľku A1 | Hrozby pre komunikačné kanály vozidiel | Ref. č. | Zmierňujúce opatrenie |
|---|---|---|---|
| 4.1. | Útok predstieraním iného odosielateľa správ [napr. predstieranie komunikácie typu V2X prostredníctvom bezdrôtovej technológie 802.11p počas jazdy v konvoji (tzv. platooning), správy systému GNSS atď.] | M10 | Vozidlo overí pravosť a integritu správ, ktoré prijíma |
| 4.2. | Útok Sybil (tzv. Sybil attack) (s cieľom predstierať iné vozidlá, ako keby sa na ceste nachádzalo veľa vozidiel) | M11 | Implementujú sa bezpečnostné kontroly na ukladanie kryptografických kľúčov (napr. použitím hardvérových bezpečnostných modulov) |
| 5.1. | Komunikačné kanály umožňujú vkladanie kódu do údajov/kódu uchovávaného vo vozidle, napríklad neoprávnene zmanipulovaný binárny kód softvéru by sa mohol vložiť do komunikačného prúdu údajov | M10<br>M6 | Vozidlo overí pravosť a integritu správ, ktoré prijíma<br>Na minimalizáciu rizík sa v systémoch musí implementovať bezpečnosť už v štádiu návrhu |
| 5.2. | Komunikačné kanály umožňujú manipuláciu údajov/kódu uchovávaného vo vozidle | M7 | Na ochranu systémových údajov/kódu sa použijú postupy a koncepcie na riadenie prístupu |
| 5.3. | Komunikačné kanály umožňujú prepisovanie údajov/kódu uchovávaného vo vozidle | | |
| 5.4.<br>21.1. | Komunikačné kanály umožňujú vymazanie údajov/kódu uchovávaného vo vozidle | | |
| 5.5. | Komunikačné kanály umožňujú zavádzať údaje/kód do systémov vozidla (zapisovanie údajov/kódu) | | |
| 6.1. | Prijímanie informácií z nespoľahlivého alebo nedôveryhodného zdroja | M10 | Vozidlo overí pravosť a integritu správ, ktoré prijíma |
| 6.2. | Útok z pozície medzičlánku/ukradnutie relácie | M10 | Vozidlo overí pravosť a integritu správ, ktoré prijíma |
| 6.3. | Útok prehratím, napríklad útok proti komunikačnej bráne útočníkovi umožňuje prejsť na staršiu verziu softvéru elektronickej riadiacej jednotky alebo firmvéru brány | | |
| 7.1. | Zachytenie informácií/rušivé žiarenie/ monitorovanie komunikácií | M12 | Dôverné údaje prenášané do vozidla alebo z neho sa musia zabezpečiť |
| 7.2. | Získanie neoprávneného prístupu k súborom alebo údajom | M8 | Prostredníctvom koncepcie systému a riadenia prístupu by nemalo byť možné, aby neoprávnený personál získal prístup k osobným alebo systémovo dôležitým údajom. Príklad bezpečnostných kontrol uvádza nadácia OWASP |

| Odkaz na tabuľku A1 | Hrozby pre komunikačné kanály vozidiel | Ref. č. | Zmierňujúce opatrenie |
|---|---|---|---|
| 8.1. | Odosielanie veľkého množstva neplatných údajov do informačného systému vozidla, aby vozidlo nebolo schopné poskytovať služby bežným spôsobom | M13 | Zavedú sa opatrenia na odhaľovanie útokov zahltením servera služby (DoS) a na zotavenie sa po tomto type útoku |
| 8.2. | Útok čiernej diery – narušenie komunikácie medzi vozidlami prostredníctvom blokovania prenosu správ ostatným vozidlám | M13 | Zavedú sa opatrenia na odhaľovanie útokov zahltením servera služby (DoS) a na zotavenie sa po tomto type útoku |
| 9.1. | Neprivilegovaný používateľ je schopný získať privilegovaný prístup, napríklad administrátorský prístup | M9 | Zavedú sa opatrenia, ktoré majú zabrániť neoprávnenému prístupu a odhaľovať takýto prístup |
| 10.1. | Vírus vložený v komunikačnom médiu infikuje systémy vozidla | M14 | Zvážiť by sa mali opatrenia na ochranu systémov proti vloženým vírusom/malvéru |
| 11.1. | Škodlivé interné správy (napr. CAN) | M15 | Zvážiť by sa mali opatrenia na odhaľovanie škodlivých interných správ alebo aktivít |
| 11.2. | Škodlivé správy komunikácie typu V2X, napr. správy z infraštruktúry do vozidla alebo správy medzi vozidlami [napr. správy CAN, DENM (správy decentralizovaného oznámenia prostredia)] | M10 | Vozidlo overí pravosť a integritu správ, ktoré prijíma |
| 11.3. | Škodlivé diagnostické správy | | |
| 11.4. | Škodlivé súkromné správy (napr. správy bežne odosielané výrobcom pôvodného zariadenia alebo dodávateľom komponentu/systému/funkcie) | | |

2. Zmierňujúce opatrenia týkajúce sa procesu aktualizácie

Opatrenia na zmiernenie hrozieb, ktoré súvisia s procesom aktualizácie, sa uvádzajú v tabuľke B2.

*Tabuľka B2*

**Opatrenia na zmiernenie hrozieb, ktoré súvisia s procesom aktualizácie**

| Odkaz na tabuľku A1 | Hrozby pre proces aktualizácie | Ref. č. | Zmierňujúce opatrenie |
|---|---|---|---|
| 12.1. | Ohrozenie aktualizácií softvéru šírených vzduchom. Zahŕňa aj zhotovenie programu alebo firmvéru na aktualizáciu systému | M16 | Použijú sa zabezpečené postupy aktualizácie softvéru |
| 12.2. | Ohrozenie lokálnych/fyzických postupov aktualizácie softvéru. Zahŕňa aj zhotovenie programu alebo firmvéru na aktualizáciu systému | | |
| 12.3. | Softvér bol zmanipulovaný pred vykonaním aktualizácie (a preto je poškodený), hoci samotný proces aktualizácie je nedotknutý | | |

| Odkaz na tabuľku A1 | Hrozby pre proces aktualizácie | Ref. č. | Zmierňujúce opatrenie |
|---|---|---|---|
| 12.4. | Ohrozenie kryptografických kľúčov poskytovateľa softvéru tak, že sa tým umožní neplatná aktualizácia | M11 | Implementujú sa bezpečnostné kontroly na ukladanie kryptografických kľúčov |
| 13.1. | Útok zahltením aktualizačného servera alebo siete (DoS) s cieľom zabrániť sprístupneniu kritických aktualizácií softvéru a/alebo odblokovať funkcie pre zákazníkov | M3 | Na serverové systémy back-end sa budú uplatňovať bezpečnostné kontroly. V prípade, ak sú servery back-end kľúčové na poskytovanie služieb, musia existovať opatrenia na obnovenie v prípade výpadku systému. Príklad bezpečnostných kontrol uvádza nadácia OWASP |

3. Zmierňujúce opatrenia týkajúce sa neúmyselnej ľudskej činnosti, ktorá umožňuje kybernetický útok

Opatrenia na zmiernenie hrozieb, ktoré súvisia s neúmyselnou ľudskou činnosťou, ktorá umožňuje kybernetický útok, sa uvádzajú v tabuľke B3.

*Tabuľka B3*

**Opatrenia na zmiernenie hrozieb, ktoré súvisia s neúmyselnou ľudskou činnosťou, ktorá umožňuje kybernetický útok**

| Odkaz na tabuľku A1 | Hrozby, ktoré súvisia s neúmyselnou ľudskou činnosťou | Ref. č. | Zmierňujúce opatrenie |
|---|---|---|---|
| 15.1. | Nevinná obeť (napr. vlastník, operátor alebo technik údržby) je oklamaná tak, aby podnikla nejaký krok s cieľom nevedomky nahrať malvér alebo umožniť útok | M18 | Implementujú sa opatrenia na vymedzenie a kontrolu rolí používateľov a oprávnení na prístup na základe zásady najmenšieho oprávnenia na prístup |
| 15.2. | Vymedzené bezpečnostné postupy sa nedodržiavajú | M19 | Organizácie musia zaistiť vymedzenie bezpečnostných postupov a ich dodržiavanie vrátane zaznamenávania akcií a prístupu v súvislosti s riadením bezpečnostných funkcií |

4. Zmierňujúce opatrenia týkajúce sa externej pripojiteľnosti a pripojení

Opatrenia na zmiernenie hrozieb, ktoré súvisia s externou pripojiteľnosťou a pripojeniami, sa uvádzajú v tabuľke B4.

*Tabuľka B4*

**Opatrenia na zmiernenie hrozieb, ktoré súvisia s externou pripojiteľnosťou a pripojeniami**

| Odkaz na tabuľku A1 | Hrozby pre externú pripojiteľnosť a pripojenia | Ref. č. | Zmierňujúce opatrenie |
|---|---|---|---|
| 16.1. | Manipulácia funkcií určených na prevádzku systémov na diaľku, ako je diaľkové ovládanie zamykania, imobilizér a nabíjacia stanica | M20 | Bezpečnostné kontroly sa uplatňujú na systémy, ktoré majú vzdialený prístup |
| 16.2. | Manipulácia telematiky vozidla (napr. manipulácia merania teploty citlivých tovarov, diaľkové odomknutie dverí nákladného priestoru) | | |

| Odkaz na tabuľku A1 | Hrozby pre externú pripojiteľnosť a pripojenia | Ref. č. | Zmierňujúce opatrenie |
|---|---|---|---|
| 16.3. | Rušenie bezdrôtových systémov s krátkym dosahom alebo senzorov | | |
| 17.1. | Poškodené aplikácie alebo aplikácie so slabým softvérovým zabezpečením slúžiace ako spôsob útoku na systémy vozidla | M21 | Softvér sa musí posúdiť z hľadiska bezpečnosti, musí sa overiť a ochrániť jeho integrita<br>Bezpečnostné kontroly sa uplatňujú s cieľom minimalizovať riziko softvéru tretích strán, ktorý je určený na hosťovanie v systéme vozidla alebo sa pri ňom predpokladá jeho hosťovanie v systéme vozidla |
| 18.1. | Externé rozhrania, ako sú porty USB alebo iné porty, používané ako miesto vniknutia, napríklad prostredníctvom vloženia kódu | M22 | Bezpečnostné kontroly sa budú uplatňovať na externé rozhrania |
| 18.2. | Médiá infikované vírusmi pripojené k vozidlu | | |
| 18.3. | Diagnostický prístup (napr. hardvérové kľúče v porte systému OBD) použitý na umožnenie útoku, napr. na manipuláciu parametrov vozidla (priamu alebo nepriamu) | M22 | Bezpečnostné kontroly sa budú uplatňovať na externé rozhrania |

5. Zmierňujúce opatrenia týkajúce sa potenciálnych cieľov útoku alebo motivácií na útok

Opatrenia na zmiernenie hrozieb, ktoré súvisia s potenciálnymi cieľmi útoku alebo s motiváciami na útok, sa uvádzajú v tabuľke B5.

*Tabuľka B5*

**Opatrenia na zmiernenie hrozieb, ktoré súvisia s potenciálnymi cieľmi útoku alebo s motiváciami na útok**

| Odkaz na tabuľku A1 | Hrozby týkajúce sa potenciálnych cieľov útoku alebo motivácií na útok | Ref. č. | Zmierňujúce opatrenie |
|---|---|---|---|
| 19.1. | Extrahovanie softvéru chráneného autorským právom alebo proprietárneho softvéru zo systémov vozidla (pirátstvo výrobkov/krádež softvéru) | M7 | Na ochranu systémových údajov/kódu sa použijú postupy a koncepcie na riadenie prístupu. Príklad bezpečnostných kontrol uvádza nadácia OWASP |
| 19.2. | Neoprávnený prístup k informáciám o súkromí vlastníka, ako je osobná identita, informácie o platobnom účte, informácie z adresára, informácie o polohe, elektronický identifikačný kód vozidla atď. | M8 | Prostredníctvom koncepcie systému a riadenia prístupu by nemalo byť možné, aby neoprávnený personál získal prístup k osobným alebo systémovo dôležitým údajom. Príklady bezpečnostných kontrol uvádza nadácia OWASP |
| 19.3. | Extrahovanie kryptografických kľúčov | M11 | Implementujú sa bezpečnostné kontroly na ukladanie kryptografických kľúčov, napr. bezpečnostné moduly |
| 20.1. | Nezákonné/nepovolené zmeny elektronického identifikačného kódu vozidla | M7 | Na ochranu systémových údajov/kódu sa použijú postupy a koncepcie na riadenie prístupu. Príklad bezpečnostných kontrol uvádza nadácia OWASP |
| 20.2. | Podvod s osobnými údajmi. Napríklad v prípade, keď sa chce používateľ preukázať inou totožnosťou pri komunikácii so systémami mýta, so serverom výrobcu | | |
| 20.3. | Opatrenie na obchádzanie monitorovacích systémov (napr. hakovanie/neoprávnená manipulácia/blokovanie správ, ako sú údaje o sledovaní záznamov ODR alebo počet spustení) | M7 | Na ochranu systémových údajov/kódu sa použijú postupy a koncepcie na riadenie prístupu. Príklad bezpečnostných kontrol uvádza nadácia OWASP |

| Odkaz na tabuľku A1 | Hrozby týkajúce sa potenciálnych cieľov útoku alebo motivácií na útok | Ref. č. | Zmierňujúce opatrenie |
|---|---|---|---|
| 20.4. | Manipulácia údajov s cieľom falšovať údaje o jazde vozidla (napr. počet prejdených kilometrov, rýchlosť jazdy, navigačné pokyny pre vodičov atď.) | | Útoky súvisiace s manipuláciou údajov zamerané na senzory alebo prenášané údaje by sa mohli zmierniť prostredníctvom korelácie údajov z rôznych zdrojov informácií |
| 20.5. | Nepovolené zmeny systémových diagnostických údajov | | |
| 21.1. | Neoprávnené vymazanie/manipulácia systémových denníkov udalostí | M7 | Na ochranu systémových údajov/kódu sa použijú postupy a koncepcie na riadenie prístupu. Príklad bezpečnostných kontrol uvádza nadácia OWASP |
| 22.2. | Zavedenie škodlivého softvéru alebo pôsobenie škodlivého softvéru | M7 | Na ochranu systémových údajov/kódu sa použijú postupy a koncepcie na riadenie prístupu. Príklad bezpečnostných kontrol uvádza nadácia OWASP |
| 23.1. | Zhotovenie softvéru riadiaceho alebo informačného systému vozidla | | |
| 24.1. | Odmietnutie služby sa môže spustiť napríklad v internej sieti zaplavením zbernice CAN alebo vyprovokovaním chýb v elektronickej riadiacej jednotke prostredníctvom vysokej miery odosielania správ | M13 | Zavedú sa opatrenia na odhaľovanie útokov zahltením servera služby (DoS) a na zotavenie sa po tomto type útoku |
| 25.1. | Neoprávnený prístup na sfalšovanie konfiguračných parametrov kľúčových funkcií vozidla, ako sú údaje o brzdách, prahová hodnota aktivácie airbagu atď. | M7 | Na ochranu systémových údajov/kódu sa použijú postupy a koncepcie na riadenie prístupu. Príklad bezpečnostných kontrol uvádza nadácia OWASP |
| 25.2. | Neoprávnený prístup na sfalšovanie parametrov o nabíjaní, ako je nabíjacie napätie, nabíjací výkon, teplota batérie atď. | | |

6. Zmierňujúce opatrenia týkajúce sa potenciálnych zraniteľností, ktoré by bez dostatočnej ochrany alebo sprísnenia mohli byť zneužité

Opatrenia na zmiernenie hrozieb, ktoré súvisia s potenciálnymi zraniteľnosťami, ktoré by bez dostatočnej ochrany alebo sprísnenia mohli byť zneužité, sa uvádzajú v tabuľke B6.

*Tabuľka B6*

**Opatrenia na zmiernenie hrozieb, ktoré súvisia s potenciálnymi zraniteľnosťami, ktoré by bez dostatočnej ochrany alebo sprísnenia mohli byť zneužité**

| Odkaz na tabuľku A1 | Hrozby týkajúce sa potenciálnych zraniteľností, ktoré by bez dostatočnej ochrany alebo sprísnenia mohli byť zneužité | Ref. č. | Zmierňujúce opatrenie |
|---|---|---|---|
| 26.1. | Spojenie krátkych šifrovacích kľúčov a dlhého obdobia platnosti umožňuje útočníkovi prelomiť šifrovanie | M23 | Dodržiavať sa musia najlepšie postupy v oblasti kybernetickej bezpečnosti týkajúce sa vývoja softvéru a hardvéru |

| Odkaz na tabuľku A1 | Hrozby týkajúce sa potenciálnych zraniteľností, ktoré by bez dostatočnej ochrany alebo sprísnenia mohli byť zneužité | Ref. č. | Zmierňujúce opatrenie |
|---|---|---|---|
| 26.2. | Nedostatočné využívanie kryptografických algoritmov na ochranu citlivých systémov | | |
| 26.3. | Používanie zastaraných kryptografických algoritmov | | |
| 27.1. | Hardvér alebo softvér navrhnutý tak, aby umožnil útok alebo taký, ktorý nespĺňa kritériá projektovania na zastavenie útoku | M23 | Dodržiavať sa musia najlepšie postupy v oblasti kybernetickej bezpečnosti týkajúce sa vývoja softvéru a hardvéru |
| 28.1. | Prítomnosť softvérových chýb môže predstavovať základ potenciálne zneužiteľných zraniteľností. To platí predovšetkým v prípade softvéru, ktorý nebol preskúšaný, aby sa overilo, že neobsahuje chybný kód/chyby, a aby sa znížilo riziko prítomnosti chybného kódu/chýb | M23 | Dodržiavať sa musia najlepšie postupy v oblasti kybernetickej bezpečnosti týkajúce sa vývoja softvéru a hardvéru.<br>Skúšky v oblasti kybernetickej bezpečnosti s primeraným pokrytím |
| 28.2. | Používanie zvyškov z vývoja (napr. ladiace porty, porty JTAG, mikroprocesory, vývojové certifikáty, vývojárske heslá…) môže útočníkovi umožniť prístup k elektronickým riadiacim jednotkám alebo získanie vyšších oprávnení | | |
| 29.1. | Nadbytočné internetové porty zostávajú otvorené a poskytujú prístup k sieťovým systémom | | |
| 29.2. | Obchádzanie oddelenia sietí s cieľom získať kontrolu. Konkrétnym príkladom je používanie nezabezpečených brán alebo prístupových bodov (ako sú brány prepájajúce ťahač a prípojné vozidlo) na obídenie zabezpečenia a na získanie prístupu do iných segmentov siete s cieľom vykonávať škodlivé úkony, ako je odosielanie arbitrárnych správ prostredníctvom zbernice CAN | M23 | Dodržiavať sa musia najlepšie postupy v oblasti kybernetickej bezpečnosti týkajúce sa vývoja softvéru a hardvéru.<br>Dodržiavať sa musia najlepšie postupy v oblasti kybernetickej bezpečnosti týkajúce sa koncepcie systému a systémovej integrácie |

7. Zmierňujúce opatrenia týkajúce sa straty údajov/úniku údajov z vozidla

Opatrenia na zmiernenie hrozieb, ktoré súvisia so stratou údajov/únikom údajov z vozidla, sa uvádzajú v tabuľke B7.

*Tabuľka B7*

**Opatrenia na zmiernenie hrozieb, ktoré súvisia so stratou údajov/únikom údajov z vozidla**

| Odkaz na tabuľku A1 | Hrozba straty údajov/úniku údajov z vozidla | Ref. č. | Zmierňujúce opatrenie |
|---|---|---|---|
| 31.1. | Únik informácií. K úniku osobných údajov môže dôjsť vtedy, keď automobil zmení používateľa (napr. pri predaji alebo pri nových prenajímateľoch, keď sa používa ako vozidlo na prenájom) | M24 | Na uchovávanie osobných údajov sa musia dodržiavať najlepšie postupy týkajúce sa ochrany integrity údajov a ich dôvernosti. |

8. Zmierňujúce opatrenia týkajúce sa fyzickej manipulácie systémov s cieľom umožniť útok

Opatrenia na zmiernenie hrozieb, ktoré súvisia s fyzickou manipuláciou systémov s cieľom umožniť útok, sa uvádzajú v tabuľke B8.

*Tabuľka B8*

**Opatrenia na zmiernenie hrozieb, ktoré súvisia s fyzickou manipuláciou systémov s cieľom umožniť útok**

| Odkaz na tabuľku A1 | Hrozby týkajúce sa fyzickej manipulácie systémov s cieľom umožniť útok | Ref. č. | Zmierňujúce opatrenie |
|---|---|---|---|
| 32.1. | Manipulácia hardvéru od výrobcu pôvodného zariadenia, napr. pridanie neschváleného zariadenia do vozidla s cieľom umožniť útok z pozície medzičlánku | M9 | Zavedú sa opatrenia, ktoré majú zabrániť neoprávnenému prístupu a odhaľovať takýto prístup |

Časť C. Opatrenia na zmiernenie hrozieb mimo vozidiel

1. Zmierňujúce opatrenia týkajúce sa serverov back-end

Opatrenia na zmiernenie hrozieb, ktoré súvisia so servermi back-end, sa uvádzajú v tabuľke C1.

*Tabuľka C1*

**Opatrenia na zmiernenie hrozieb, ktoré súvisia so servermi back-end**

| Odkaz na tabuľku A1 | Hrozby pre servery back-end | Ref. č. | Zmierňujúce opatrenie |
|---|---|---|---|
| 1.1 a 3.1 | Zneužitie oprávnení zamestnancami (útok zvnútra) | M1 | V záujme minimalizácie rizika útoku zvnútra sa na serverové systémy back-end uplatňujú bezpečnostné kontroly |
| 1.2 a 3.3 | Neoprávnený internetový prístup na server (umožnený napríklad prostredníctvom zadných vrátok, neopravených zraniteľností softvéru operačného systému, napadnutia databázy SQL alebo iných prostriedkov) | M2 | V záujme minimalizácie rizika neoprávneného prístupu sa na serverové systémy back-end uplatňujú bezpečnostné kontroly. Príklad bezpečnostných kontrol uvádza nadácia OWASP |
| 1.3 a 3.4 | Neoprávnený fyzický prístup k serveru (ktorý sa uskutočnil napríklad pripojením USB kľúčov alebo iných médií k serveru) | M8 | Prostredníctvom koncepcie systému a riadenia prístupu by nemalo byť možné, aby neoprávnený personál získal prístup k osobným alebo systémovo dôležitým údajom |
| 2.1. | Útok na server back-end má za následok, že server prestane fungovať, napríklad mu znemožní komunikáciu s vozidlami a poskytovanie služieb, od ktorých vozidlá závisia | M3 | Na serverové systémy back-end sa uplatňujú bezpečnostné kontroly. V prípade, ak sú servery back-end kľúčové na poskytovanie služieb, musia existovať opatrenia na obnovenie v prípade výpadku systému. Príklad bezpečnostných kontrol uvádza nadácia OWASP |
| 3.2. | Strata informácií v cloude. Keď sa údaje uchovávajú prostredníctvom poskytovateľov cloudových služieb tretích strán, v dôsledku útokov alebo nehôd môže dôjsť k strate citlivých údajov | M4 | V záujme minimalizácie rizík súvisiacich s cloud computingom sa uplatňujú bezpečnostné kontroly. Príklad bezpečnostných kontrol uvádza nadácia OWASP a nachádza sa v usmerneniach centra NCSC pre cloud computing |
| 3.5. | Únik informácií prostredníctvom neúmyselného zdieľania údajov (napr. chyby správcov, ukladanie údajov na serveroch v autoservisoch) | M5 | S cieľom zabrániť úniku údajov sa na serverové systémy back-end uplatňujú bezpečnostné kontroly. Príklad bezpečnostných kontrol uvádza nadácia OWASP |

2. Zmierňujúce opatrenia týkajúce sa neúmyselnej ľudskej činnosti

Opatrenia na zmiernenie hrozieb, ktoré súvisia s neúmyselnou ľudskou činnosťou, sa uvádzajú v tabuľke C2.

*Tabuľka C2*

**Opatrenia na zmiernenie hrozieb, ktoré súvisia s neúmyselnou ľudskou činnosťou**

| Odkaz na tabuľku A1 | Hrozby, ktoré súvisia s neúmyselnou ľudskou činnosťou | Ref. č. | Zmierňujúce opatrenie |
|---|---|---|---|
| 15.1. | Nevinná obeť (napr. vlastník, operátor alebo technik údržby) je oklamaná tak, aby podnikla nejaký krok s cieľom nevedomky nahrať malvér alebo umožniť útok | M18 | Implementujú sa opatrenia na vymedzenie a kontrolu rolí používateľov a oprávnení na prístup na základe zásady najmenšieho oprávnenia na prístup |
| 15.2. | Vymedzené bezpečnostné postupy sa nedodržiavajú | M19 | Organizácie musia zaistiť vymedzenie bezpečnostných postupov a ich dodržiavanie vrátane zaznamenávania akcií a prístupu v súvislosti s riadením bezpečnostných funkcií |

3. Zmierňujúce opatrenia týkajúce sa fyzickej straty údajov

Opatrenia na zmiernenie hrozieb, ktoré súvisia s fyzickou stratou údajov, sa uvádzajú v tabuľke C3.

*Tabuľka C3*

**Opatrenia na zmiernenie hrozieb, ktoré súvisia s fyzickou stratou údajov**

| Odkaz na tabuľku A1 | Hrozby fyzickej straty údajov | Ref. č. | Zmierňujúce opatrenie |
|---|---|---|---|
| 30.1. | Škoda spôsobená treťou stranou. K strate alebo narušeniu citlivých údajov môže dôjsť z dôvodu materiálnych škôd v prípadoch dopravných nehôd alebo krádeže | M24 | Na uchovávanie osobných údajov sa musia dodržiavať najlepšie postupy týkajúce sa ochrany integrity údajov a ich dôvernosti. Príklad bezpečnostných kontrol uvádza pracovná skupina ISO/SC27/WG5 |
| 30.2. | Strata v dôsledku konfliktov súvisiacich so správou digitálnych prístupových práv (DRM). Z dôvodu problémov spojených s DRM môže dôjsť k vymazaniu používateľských údajov | | |
| 30.3. | Strata (integrity) citlivých údajov môže nastať v dôsledku opotrebovania komponentov informačných technológií, čo môže vyvolať dominový efekt (napríklad v prípade zmeny kľúča) | | |