SOR Libchavy spol. s r.o.
Dolní Libchavy 48, 561 16 Libchavy
IČ: 15030865, DIČ: CZ15030865
Tel.: +420 465 519 411, sor@sor.cz
www.sor.cz

Účel

Tento předpis je souhrnem požadavků společnosti SOR Libchavy spol. s r.o. na dodavatele a zboží, které bylo vyhodnoceno jako KB relevantní. Účelem je splnění požadavků systému CSMS (Cyber Security Management System) definované nařízením UNECE R 155.

Seznam pojmů

KB nebo CySe (Cyber Security)	kybernetická bezpečnost
CSMS (Cyber Security Management System)	systém řízení kybernetické bezpečnosti
SUMS (Software Update Management System)	systém řízení aktualizací software
SBOM (Software Bill of Materials)	softwarový kusovník (seznam komponent, knihoven, nástrojů a procesů používaných k vývoji, sestavení a publikování software)
KB komponenta	KB relevantní zboží (řídící jednotky, převodníky, sensory,…)

Definice KB relevantního zboží (komponenty)

KB relevantní zboží definuje SOR. Obecně se jedná o každé zboží, které je relevantní s pohledu kybernetické bezpečnosti. Zboží je KB relevantní, pokud

1. má vliv na život, životní prostředí, nebo důvěrné informace (včetně osobních údajů osob)
2. a zároveň se jedná o elektronickou komponentu (např. řídící jednotka, gateway, převodník,..).

KB POŽADAVKY NA DODAVATELE A ZBOŽÍ

KB požadavky na dodavatele

Před realizací první dodávky KB komponenty a dále v rámci pravidelného hodnocení dodavatelů, doloží dodavatel SOR následující podklady, které dokumentují dostatečný přístup k zajištění kybernetické bezpečnosti jeho organizace:

1. certifikát CSMS organizace dle **UNECE R 155** vydaný autorizovanou osobou; nebo
2. certifikát systému managementu bezpečnosti informací dle standardu **ISO 27001** vydaný autorizovanou osobou; nebo
3. osvědčení o managementu bezpečnosti informací dle standardu **TISAX** (Trusted Information Security Assessment Exchange) vydaný autorizovanou osobou; nebo
4. doklad o zařazení organizace jako povinné osoby dle nařízení Směrnice Evropského parlamentu a rady (EU) 2022/2555 – zkráceně jako „**NIS2**“; nebo
5. vyplněný dotazník „**Ověření úrovně kybernetické bezpečnosti dodavatelů SOR**“ obsahující čestné prohlášení. SOR si vymezuje právo ověřit pravdivost čestného prohlášení provedením **zákaznického auditu u dodavatele**.

Při každoročním hodnocení dodavatelů je ověřováno, zda dodavatel stále některou z výše požadovaných podmínek plní. Za stranu SOR toto hodnocení a kontakt s dodavatelem zajišťuje oddělení Nákup ve spolupráci s Manažerem KB.

SOR Libchavy spol. s r.o.
Dolní Libchavy 48, 561 16 Libchavy
IČ: 15030865, DIČ: CZ15030865
Tel.: +420 465 519 411, sor@sor.cz
www.sor.cz

Požadavky na KB nakupované komponenty

V případě, že je se jedná o KB komponentu, dodá dodavatel:

1. **certifikát** CSMS ke zboží dle UNECE R 155 vydaný autorizovanou osobou (pokud jej má);
2. aktuální **TARA** analýzu KB komponenty (preferujeme využití metodiky dle ISO/SAE 21434), případně pouze rizika vyplývající z TARA analýzy, v případě změn operačního prostředí, funkce nebo rozhraní komponenty se zavazuje dodavatel tyto vstupy aktualizovat a dodat do SOR;
3. k identifikovaným rizikům navrhovaná **technická opatření**, která zmírňují jejich negativní dopady;
    - např. dle hrozeb: odposlech, přerušení kabeláže, zahlcení / rušení komunikace, podvržení zprávy,
    - také pro software (pokud je to relevantní): ověření a oprávnění uživatele pro vyčtení dat a aktualizaci SW (případně i parametrů nebo datasetů), šifrování komunikace, přenosu a ukládání dat (úroveň bezpečnosti např. dle doporučení ENISA, NÚKIB);
4. **prohlášení o shodě** (s UNECE R 155) nebo **protokoly o testování:**
    - v případě komponenty ověření funkčnosti technických opatření,
    - v případě software porovnání SBOM se známými zranitelnostmi, např. dle nvd.nist.gov, snyk.io;
5. pokud je to relevantní, bezpečné **postupy aktualizace software, datasetů a parametrů**;
6. v případě **řídící jednotky** (ECU), seznam dotazů, na které jednotka **přes CAN odpoví**:
    - ECU hardware version (model number nebo product number),
    - ECU serial number,
    - software version,
    - Integrity Validation Data;
7. **termín ukončení podpory** zboží (vývoje a výroby zboží/komponenty).

Pokud dodavatel není schopen dodat bod 2, nebo 3, je nutná spolupráce SOR (ředitel nákupu, manažer KB, vedoucí konstrukce) a technických expertů dodavatele. K tomu dodavatel předem připraví:

1. technickou dokumentaci komponenty včetně blokového schématu zapojení, komunikačního rozhraní a provozních stavů,
2. popis bezpečnostních mechanismů a využitých opatření,
3. zajištění dostatečné personální a odborné kapacity ke konzultacím a návrh jejich termínů.

KB POŽADAVKY NA VÝVOJ

Požadavky na vývoj KB komponent

Cílem je, aby KB komponenta byla v souladu s požadavky kybernetické bezpečnosti, které jsou definovány pro její zamýšlený účel použití – splňovala cíle KB určené výrobcem pro dané vozidlo.

Obecné doporučení pro vývoj KB komponenty

Výrobce komponenty by měl při jejím návrhu a aktualizacích brát zřetel nejen na funkční požadavky, ale i na požadovanou úroveň KB zejména v následujících oblastech:

1. stanovení požadavků na KB / cílů KB komponenty v návaznosti na její zamýšlené operačního prostředí,
2. stanovení bezpečnostních mechanismů, které zajistí potřebnou úroveň KB při:
    - čtení dat z jednotky (komponenty),
    - zápisu nebo update software do jednotky,
    - komunikaci s jinou jednotkou na sběrnici,

SOR Libchavy spol. s r.o.
Dolní Libchavy 48, 561 16 Libchavy
IČ: 15030865, DIČ: CZ15030865
Tel.: +420 465 519 411, sor@sor.cz
www.sor.cz

- komunikaci s dalšími připojenými komponentami (např. senzory),
- zajišťování záznamů o provedených akcích (např. ukládání logů),
- komunikaci mimo vozidlo;

3. známé zranitelnosti (např. zastaralá verze komunikačního protokolu, známé nedostatky použitého čipu,..);
4. vytvoření a údržbu technické dokumentace, včetně popisu ochranných mechanismů, opatření ke známým rizikům, včetně neošetřených rizik;
5. testování komponenty (viz níže);
6. stanovení plánovaného termínu ukončení podpory zboží (vývoje a výroby, SW podpory).

Detailní požadavky na úroveň zajištění KB a technické řešení mohou být součástí technických jednání mezi dodavatelem a SOR. Po provedených konzultacích mohou být požadavky definovány ve specifikaci dílčích objednávek.

Protokol o testování HW komponenty

Před označení elektronické komponenty jako finální verze, určené pro běžný provoz vozidla, je třeba provést finální testování z hlediska kybernetické bezpečnosti a vytvořit o tom záznam ve formě protokolu.

Protokol by měl obsahovat zejména:

1. obchodní název výrobce, název a označení KB komponenty, model no., part no.;
2. pokud je to relevantní, informace o tom, že je komponenta certifikována dle UNECE R 155;
3. pokud je to relevantní, verze software, verze datasetu nebo výpis konfigurace parametrů;
4. seznam předepsaných testů (funkční testování, ověření funkčnosti technických opatření, případně vulnerability scanning nebo pen-testing);
5. k seznamu jednotlivých testů, datum provedení a identifikace zhotovitele testu.

Výrobce je povinen

1. označit komponentu, pokud není určena pro běžný provoz vozidla na pozemní komunikaci;
2. dodat všechny body, definované odstavcem „Požadavky na KB nakupované komponenty“, pokud je komponenta určena pro běžný provoz vozidla na pozemní komunikaci;
3. neprodleně informovat SOR o výskytu závažného rizika nebo kybernetické události na email: oznameni@sor.cz (nebo notification@sor.cz).

KB požadavky na vývoj software

Cílem je, aby software byl v souladu s požadavky kybernetické bezpečnosti, které jsou definovány pro jeho zamýšlený účel použití – splňoval cíle KB určené výrobcem pro dané vozidlo.

Obecné doporučení pro vývoj software

Výrobce software by měl při návrhu a aktualizacích brát zřetel nejen na funkční požadavky, ale i na požadovanou úroveň KB zejména v následujících oblastech:

1. stanovení požadavků na KB / cílů KB v návaznosti na jeho zamýšlené operačního prostředí, zahrnout i požadavky na komponentu (odstavec „Požadavky na vývoj KB komponent“);
2. stanovení KB požadavků na software, zahrnout i bezpečnostní mechanismy komponenty (odstavec „Požadavky na vývoj KB komponent“);
3. známá rizika (např. nedostatečná validace dat, nedostatečné kontrolní mechanismy, zastaralá verze frameworku,.. např. dle nvd.nist.gov, snyk.io);

SOR Libchavy spol. s r.o.
Dolní Libchavy 48, 561 16 Libchavy
IČ: 15030865, DIČ: CZ15030865
Tel.: +420 465 519 411, sor@sor.cz
www.sor.cz

4. vytvoření sady dokumentace k SW, včetně popisu ochranných mechanismů, opatření ke známým rizikům, včetně neošetřených rizik a postupů správné aktualizace software, datasetů a parametrů;
5. testování software (viz níže);
6. stanovení plánovaného termínu ukončení vývoje a podpory software.

Protokol o testování software

Před označení verze software jako „finální / schválený“ a uvolněním pro běžný provoz vozidla na pozemní komunikaci, je třeba provést finální testování z hlediska kybernetické bezpečnosti a vytvořit tom záznam ve formě protokolu.

Protokol by měl obsahovat zejména:

1. obchodní název výrobce software, název a označení software;
2. verzi software, stav nebo jeho vývojová fáze;
3. pokud je to relevantní, informace o tom, že jednotka, pro který je software určen, je certifikována dle UNECE R 155;
4. pokud je to relevantní, verze datasetu nebo výpis konfigurace parametrů;
5. porovnání SBOM se známými zranitelnostmi, např. dle nvd.nist.gov, snyk.io;
6. k seznamu provedených testů, datum provedení a identifikace zhotovitele testu.

Výrobce je povinen

1. zajistit SOR zabezpečený přístup k úložišti uvolněných verzí software;
2. označit verzi software tak, aby byla evidentní jeho vývojové fáze, například těmito stavy:
   - TESTOVACÍ – není určený pro běžný provoz, jen pro testování komponenty nebo prototypu,
   - SCHVÁLENÝ – určen pro běžný provoz vozidla na pozemní komunikaci,
   - NEBEZPEČNÝ – zastaralý, nebo obsahující závažnou chybu;
3. nebo zajistit, aby byl umožněn přístup pouze k software verzi „SCHVÁLENÝ“;
4. neprodleně informovat SOR o výskytu závažného rizika nebo kybernetické události na email: oznameni@sor.cz (nebo notification@sor.cz). Na stejný email neprodleně informovat o vytvoření (kritické) opravy.