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

KB komponenta KB relevantní zboží (řídící jednotky, převodníky, sensory,…)

Definice KB relevantního zboží (komponenty)

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

1. se jedná o elektronickou komponentu připojenou na sběrnici A
2. může mít vliv na zdraví nebo život člověka (např. vznik nebezpečné situace nebo vliv na řízení vozidla) nebo životní prostředí nebo důvěrné informace NEBO
3. má možnost externího připojení (konektor, internet, WIFI).

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. KB certifikát organizace, např: **UNECE R 155, ISO 27001, ISO 21434** nebo **TISAX** vydaný autorizovanou osobou; nebo
2. doklad o zařazení organizace jako povinné osoby dle nařízení Směrnice Evropského parlamentu a rady (EU) 2022/2555 – zkráceně jako „**NIS2**“; nebo
3. vyplněný dotazník [**KB (CySe) dotazník pro dodavatele**](https://www.sor.cz/wp-content/uploads/2024/04/MPQ-840-2-Příloha-4-KB-dotazník-pro-dodavatele.docx) obsahující čestné prohlášení. SOR si vymezuje právo ověřit pravdivost čestného prohlášení provedením zákaznického auditu u dodavatele.
4. A zároveň [**KB (CySe) dohoda o rozhraní kybernetické bezpečnosti DIA**](https://www.sor.cz/wp-content/uploads/2024/04/MPQ-840-2-Příloha-2-DIA.xlsx), případně vlastní verzi dohody.

Při každoročním hodnocení dodavatelů je ověřováno, zda dodavatel stále výše zmíněné podmínky plní. Za stranu SOR toto hodnocení a kontakt s dodavatelem zajišťuje oddělení Nákup (ve spolupráci s Manažerem KB).

Dodavatel je dále povinen:

1. neprodleně informovat SOR o výskytu závažné **zranitelnosti** nebo **kybernetickém incidentu** nebo **vydání kritické aktualizace** (mající potenciální vliv na bezpečnost cestujících) na email: [oznameni@sor.cz](mailto:oznameni@sor.cz).

Požadavky na KB nakupované komponenty

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

1. **certifikát** CSMS ke zboží dle UNECE R 155 vydaný autorizovanou osobou, pokud jej má;
2. aktuální výsledky **TARA** analýzy (preferujeme využití metodiky dle ISO/SAE 21434):

* **rizika** vyplývající z TARA analýzy,
* **technická opatření**, která zmírňují jejich negativní dopady;

1. komponenta:

* jednoznačně **označit komponentu,** pokud je určena pro testovací nebo vývojové účely,
* pro sériová vozidla využívat pro CAN diagnostiku a aktualizaci SW **pouze OBD zásuvku a UDS protokol**,
* **výsledky penetračních testů** včetně oprav nálezů, pokud jsou k dispozici;

1. software:

* **návody k diagnostickému SW**,
* bezpečné **postupy aktualizace** **SW** nebo parametrů jednotky,
* bezpečný **přístup k aktuálním verzím SW**,
* jednoznačně **odlišit SW** určený pro provoz vozidla na pozemní komunikaci od nebezpečného nebo testovacího SW,
* zabezpečit **neměnnost SW během aktualizace** (např. on-line aktualizace, el. podpis případně kontrolní součet, šifrování, atd.),
* výsledky **SW testů** (např. CVE a CVSS nebo porovnání s [nvd.nist.gov](https://nvd.nist.gov/vuln/search));

1. šifrování:

* komponenty a SW chráněné **bezpečnými kryptografickými protokoly, šifry a hashovacími funkcemi**, to je bez známých zranitelností (dle NÚKIB nebo NIST) a pravidelně (alespoň 1 x ročně) tento stav porovnávat,
* v případě použití jiných (neschválených) šifrovacích algoritmů je třeba informovat SOR,
* aktuální odkazy:
  + [NÚKIB](https://nukib.gov.cz/download/uredni_deska/Minimalni%20pozadavky%20na%20kryptograficke%20algoritmy.pdf),
  + [NIST](https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines);

1. 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;

1. **termín ukončení podpory** zboží (vývoje a výroby zboží/komponenty).

Pokud dodavatel není schopen dodat bod 2, je nutná spolupráce SOR (ředitel nákupu a logistiky, manažer KB) 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.