KB pravidla pro dodavatele a zboží

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) dle UNECE R 155 a SUMS (Software Update Management System) dle UNECE R 156.

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,…)
ECU (Electronic Control Unit)	elektronická řídící jednotka

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

a. se jedná o EE komponentu řízenou ECU pomocí datové sběrnice a zároveň
b. má vliv na zdraví nebo život člověka nebo životní prostředí nebo důvěrné informace nebo
c. lze na komponentě provést aktualizaci SW.

Požadavky KB 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** 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**, 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:

5. 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.

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 KB na nakupované komponenty

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

1. **certifikát** CSMS ke zboží (UNECE R 155, ISO21434, TISAX) vydaný autorizovanou osobou, pokud jej má;
2. aktuální výsledky **TARA** analýzy (dle metodiky ISO/SAE 21434 nebo obdobné), alespoň vyplývající **rizika** včetně **nápravných opatření**, která zmírňují jejich negativní dopady;
3. aktuální **výsledky penetračních testů** včetně implementovaných oprav nálezů;
4. jednoznačně **označit komponentu,** pokud je určena pro testovací nebo vývojové účely,
5. **seznam CAN dotazů**, na které řídící jednotka ECU přes CAN odpoví:
   - ECU hardware version (model number nebo product number),
   - ECU serial number,
   - software version,
   - Integrity Validation Data;
6. **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:

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

Požadavky na SW

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

1. **zasílat informace o jakékoliv aktualizaci SW** na email: swupdate@sor.cz, informace musí obsahovat:
   - HW verze řídící jednotky,
   - SW verze, případně verze datasetu nebo popis konfigurace parametrů,
   - účel a rozšířený popis o možný vliv na homologační parametry,
   - jaké systémy nebo funkce vozidla může ovlivnit,
2. pro sériová vozidla:
   - využívat pro CAN diagnostiku a aktualizaci SW **pouze OBD zásuvku a UDS protokol**,
   - **nevyužívat vzdálenou aktualizaci SW typu OTA** (Over The Air) a aktualizovat SW bez přítomnosti technika SOR,
3. dodat **návody k diagnostickému SW** a bezpečné **postupy aktualizace SW** nebo parametrizace ECU,
4. umožnit bezpečný **přístup k aktuálním verzím SW**,
5. jednoznačně **odlišit SW** určený pro sériovou výrobu od nebezpečného nebo testovacího SW,
6. zabezpečit **neměnnost SW během procesu aktualizace** (např. šifrování, el. podpis, případně kontrolní součet, ověření původu a neměnnosti, atd.),
7. dodat výsledky **SW testů** (např. CVE a CVSS a porovnání s nvd.nist.gov);
8. využívat **šifrování** pro komponenty i SW**:**
   - pomocí **bezpečných kryptografických protokolů, šifer a hashovacích funkcí,** 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.