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: **ISO 27001, ISO 21434, TISAX** vydaný autorizovanou osobou; nebo
2. vyplněný dotazník **KB (CySe) dotazník pro dodavatele** obsahující čestné prohlášení; a zároveň
3. **KB (CySe) dohoda o rozhraní kybernetické bezpečnosti CIA**, 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).

Požadavky na KB komponenty

V případě, že se jedná o KB (CySe) komponentu, je dodavatel 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;
2. dodat aktuální CySe dokumentaci:
   - **popis jednotky** / systému (včetně SBOM),
   - aktuální **TARA** jednotky / systému,
   - popis **implementovaných opatření** (stávající vlastnosti = secured by design, další = additional mitigations),
   - reporty z testování opatření (**penetrační testy**);
3. jednoznačně **označit komponentu,** pokud je určena pro testovací nebo vývojové účely;

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

Pokud dodavatel není schopen dodat bod 2, je nutná spolupráce SOR (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.

Doporučení pro vývoj „CySe ready“ komponent:

6. **technická opatření**:
   - vypnout / zamknout **nepoužívaná rozhraní**,
   - vypnout / zamknout **debug**,
   - **šifrování**
     - komunikace s potencionálně vysokými dopady (např. vysoké dopady z TARA),
     - přenosu dat (SW, FW, změny parametrů, logů) pomocí diagnostického nástroje,
     - přenosu dat mezi komponentou a backend serverem,
     - úroveň šifrování porovnat s doporučením nist.gov nebo nukib.gov.cz,
   - **ověření uživatele certifikátem** (případně 2-factor autentizací)
     - pro přihlášení a komunikaci diagnostického nástroje,
     - pro přihlášení a komunikaci backend serveru,
   - další technická opatření, jako: secure boot, Integrity Data Validation, atd.;
7. **vyjádření** ke všem bodům Přílohy č. 5 z předpisu UN Regulation No. 155,
   - bylo aplikováno / nebylo aplikováno a proč.

Požadavky na SW

V případě, že se jedná o KB (CySe) 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 **nepoužívat vzdálenou aktualizaci SW typu OTA** (Over The Air), aktualizovat SW vzdáleně 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. pomocí šifrování a ověření certifikátem (zmíněné výše).