Zweck

Diese Verordnung ist eine Zusammenfassung der Anforderungen von SOR Libchavy spol. s r.o. über Lieferanten und Waren, die als KB-relevant bewertet wurden. Der Zweck besteht darin, die Anforderungen des CSMS (Cyber Security Management System) zu erfüllen, das in der UNECE R 155-Verordnung definiert ist.

Übersicht der Begriffe

KB oder CySe (Cyber Security) Cyber-Sicherheit

CSMS (Cyber Security Management System) Managementsystem für Cyber-Sicherheit

SUMS (Software Update Management System) Managementsystem für Softwareaktualisierung

KB Komponente KB relevante Ware (Steuergeräte, Converter, Sensoren, …)

Definition der KB relevanten Ware (Komponenten)

**Die KB relevante Ware definiert die SOR.** Im Allgemeinen handelt es sich hierbei um jede Ware, das aus Sicht der Cybersicherheit relevant ist. Die Ware ist KB relevant, wenn

1. es sich um eine elektronische Komponente, die an Bus A angeschlossen ist, handelt
2. die Gesundheit oder das Leben einer Person (z. B. indem sie eine gefährliche Situation herbeiführt oder das Fahren eines Fahrzeugs beeinträchtigt) oder die Umwelt oder vertrauliche Informationen beeinträchtigen kann ODER
3. bei ihr die Möglichkeit einer externen Verbindung besteht (Anschluss, Internet, WIFI).

KB ANFORDERUNGEN AN LIEFERANTEN UND WAREN

KB Anforderungen an Lieferanten

Vor der Umsetzung der ersten Lieferung der KB Komponente und darüber hinaus im Rahmen der regelmäßigen Lieferantenbewertung muss der Lieferant der SOR folgende Dokumente vorlegen, die einen ausreichenden Ansatz zur Gewährleistung der Cybersicherheit seiner Organisation dokumentieren:

1. KB Zertifikat der Organisation, z. B.:**UNECE R 155, ISO 27001, ISO 21434** oder **TISAX** ausgestellt durch eine autorisierte Person; oder
2. Nachweis über die Klassifizierung der Organisation als Pflichtperson gemäß der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates – abgekürzt „**NIS2**“; oder
3. ausgefüllte Umfrage [**KB (CySe) Umfrage für Lieferanten**](https://www.sor.cz/wp-content/uploads/2024/04/MPQ-840-2-P%C5%99%C3%ADloha-4-KB-dotazn%C3%ADk-pro-dodavatele.docx), die eine eidesstattliche Erklärung enthält. SOR behält sich das Recht vor, die Wahrhaftigkeit der eidesstattlichen Erklärung durch ein Kundenaudit beim Lieferanten zu überprüfen.
4. Und gleichzeitig [**KB (CySe) Abkommen über Schnittstelle der Cyber-Sicherheit DIA**](https://www.sor.cz/wp-content/uploads/2024/04/MPQ-840-2-P%C5%99%C3%ADloha-2-DIA.xlsx), ggf. die eigene Version des Abkommens.

Bei der jährlichen Lieferantenbewertung wird überprüft, ob der Lieferant die oben genannten Bedingungen stets erfüllt. Seitens SOR erfolgt diese Beurteilung und Kontaktaufnahme mit dem Lieferanten durch die Einkaufsabteilung (in Zusammenarbeit mit dem KB-Manager).

Der Lieferant ist ferner verpflichtet:

1. SOR unverzüglich über das Auftreten einer schwerwiegenden **Sicherheitslücke** oder **Cyber-Vorfall** oder der **Erstellung einer kritischen Aktualisierung** (mit potentiellen Auswirkungen auf die Sicherheit der Fahrgäste) informieren, und dies auf die E-Mail: oznameni@sor.cz.

KB Anforderungen an eingekaufte Komponenten

Handelt es sich um eine KB Komponente, ist der Lieferant verpflichtet, zur Lieferung beizulegen:

1. CSMS **Zertifikat** für Ware gemäß UNECE R 155, ausgestellt von einer autorisierten Person, sofern vorhanden;
2. aktuelle Ergebnisse der **TARA** Analyse (wir bevorzugen die Methodik nach ISO/SAE 21434):
* **Risiken**, die sich aus der TARA Analyse ergeben,
* **technische Maßnahmen**, die ihre negativen Auswirkungen abmildern;
1. Komponente:
* die Komponente **eindeutig identifizieren**, wenn sie für Test- oder Entwicklungszwecke bestimmt ist,
* bei Serienfahrzeugen **ausschließlich die OBD-Buchse und das UDS-Protokoll** für CAN-Diagnose und SW-Update nutzen,
* **Ergebnisse von Penetrationstests**, einschließlich Korrekturen von Befunden, sofern verfügbar;
1. Software:
* **Anleitungen für Diagnosesoftware,**
* sichere **Verfahren zum Aktualisieren von SW** oder Geräteparametern,
* sicherer **Zugriff auf aktuelle SW-Versionen**,
* **SW**, die für den Fahrzeugbetrieb an Land bestimmt sind, eindeutig von gefährlichen SW oder Test-SW **unterscheiden**,
* Gewährleistung der **Unveränderlichkeit der SW während des Updates** (z. B. Online-Update, elektronische Signatur oder Prüfsumme, Verschlüsselung usw.),
* Ergebnisse der **SW Tests** (z. B. CVE und CVSS oder Vergleich mit [nvd.nist.gov](https://nvd.nist.gov/vuln/search));
1. Verschlüsselung:
* Komponenten und SW, die durch **sichere kryptografische Protokolle, Verschlüsselungen und Hashing-Funktionen** geschützt sind, also keine bekannten Schwachstellen aufweisen (gemäß NÚKIB oder NIST) und diesen Status regelmäßig (mindestens einmal im Jahr) vergleichen,
* bei Verwendung anderer (nicht zugelassener) Verschlüsselungsalgorithmen ist der SOR zu informieren,
* aktuelle Links:
	+ [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. im Fall des Steuergeräts (ECU) **die Liste der Fragen**, auf die das Gerät über CAN antwortet:
* ECU hardware version (model number nebo product number),
* ECU serial number,
* software version,
* Integrity Validation Data;
1. **Datum der Beendigung** **des Produktsupports** (Entwicklung und Produktion von Ware / Komponente).

Sollte der Lieferant nicht in der Lage sein, Punkt 2 zu liefern, ist die Zusammenarbeit zwischen SOR (Einkaufs- und Logistikdirektor, KB Manager) und der technischen Experten des Lieferanten erforderlich. Hierzu bereitet der Lieferant vorab vor:

1. technische Dokumentation der Komponente, einschließlich des Blockschaltbildes, der Kommunikationsschnittstelle und der Betriebszustände,
2. Beschreibung der eingesetzten Sicherheitsmechanismen und -maßnahmen,
3. Sicherstellung ausreichender personeller und fachlicher Kapazitäten für Beratungen und Vorschlagen ihrer Termine.