Kraftfahrt-
Bundesamt

Leitlinien

zur Berichterstattung der Hersteller an das KBA und den Technischen Dienst im Rahmen der UN-R 155/156

Revision 1.0 final, Stand: 27.06.2022

Inhaltsverzeichnis

Seite

1 Zweck

Dieses Dokument erläutert die Berichtspflichten der im Geltungsbereich genannten Organisationen gegenüber dem KBA als zertifikatserteilender Behörde und den in diesem Zusammenhang tätigen Technischen Diensten (TD). Es bestimmt die im Prozess der Ersterteilung und Erneuerung sowie im Rahmen der Überwachung der Konformitätsbescheinigung (CoC, im weiteren als Zertifikat bezeichnet) mindestens zur Verfügung zu stellenden Informationen.
Form, Umfang und Kommunikationskanal sind mit dem KBA und mit dem zuständigen TD gesondert zu vereinbaren, sofern in diesem Dokument keine Anforderungen dazu formuliert werden.
Da die TD die Information im Auftrag des KBA analysieren, wird empfohlen, dass zwischen TD und Herstellern ebenfalls ein Berichtswesen auf Basis dieses Dokuments vereinbart wird
Informationen im Rahmen der Genehmigungserteilung und -erweiterung, von CoP und von Marktüberwachung werden in diesem Dokument nur betrachtet, sofern sie Rückschlüsse auf die Funktionsfähigkeit und Angemessenheit des Managementsystems erlauben. Hier nicht genannte sonstige Anforderungen an solche Berichtspflichten bleiben unberührt.

2 Geltungsbereich

Dieses Dokument richtet sich an Organisationen, die ein Zertifikat nach den UN-Regelungen 155 bzw. 156 beim KBA anstreben bzw. denen ein solches Zertifikat erteilt wurde.[1]

3 Abkürzungen

CSMS	Cybersicherheits-Managementsystem
CVE	Common Vulnerabilities and Exposures
BSI	Bundesamt für Sicherheit in der Informationstechnik
KBA	Kraftfahrt-Bundesamt
SUMS	Softwareaktualisierungs-Managementsystem
TD	Technischer Dienst
UN-R	UN-Regelung

4 Mitgeltende Unterlagen

Anwendung der Regeln für die Benennung/Anerkennung von TD (Kategorien A, B, D) zu Prüfungen im Rahmen des KBA-Typgenehmigungsverfahrens nach den UN-Regelungen 155/156

5 Zuständigkeiten

Der Hersteller stellt die im Folgenden genannten Informationen unaufgefordert dem KBA zur Verfügung.
Auf Verlangen des KBA bzw. des zuständigen TD stellt der Hersteller weitergehende Informationen zur Verfügung bzw. ändert die Häufigkeit der Meldung.
Der Hersteller wertet die zur Verfügung stehenden Informationen in Bezug auf Wirksamkeit und Angemessenheit des jeweils zu überwachenden Managementsystems aus und übermittelt dem KBA und dem TD entsprechend aufbereitete Daten in Form eines mindestens jährlichen Berichts.
Der TD analysiert die vom Hersteller zur Verfügung gestellte und sonstige relevante Information im Rahmen seiner Prüf- und Überwachungsaufgaben und stellt dem KBA das Ergebnisdieser Analyse einschließlich event. Entscheidungsvorschläge zur Verfügung.
Das KBA (Dresden) wertet die durch Hersteller und TD gelieferte Information in Bezug auf den Hersteller und die Sicherheitslage aus und trifft ggf. notwendige Entscheidungen. Sofern die Information auch für andere Bereiche der Abteilungen Typgenehmigung und Marktüberwachung des KBA relevant sein können, erfolgt eine entsprechende Weiterleitung. Forderungen, die

[1] im weiteren als Hersteller bezeichnet

unmittelbar aus anderen Bereichen des KBA gestellt werden, bzw. die aus anderen Vorgaben des KBA resultieren, bleiben unberührt.
Eine Auswertung erfolgt auch in Bezug auf die Wirksamkeit und Angemessenheit der durch das KBA festgelegten Anforderungen.
Das BSI unterstützt das KBA auf dessen Bitte. Das KBA wird dem BSI die dafür notwendigen Informationen zur Verfügung stellen. Das KBA wird das BSI auch Informationen weitergeben, die zur Bewertung der Bedrohungslage durch diese Behörde von wesentlicher Bedeutung sein könnten.

6 Allgemeines

(1) Der Hersteller liefert die in den Rechtsakten und in diesem Leitfaden geforderte Information schriftlich in digitaler verarbeitbarer Form[2], über einen der nachfolgenden Meldewege an das KBA.

- Mail: cybersecurity@kba.de
  (nur UN-R 155; pgp-basierte Verschlüsselung wird akzeptiert)
- E-Typ
- sonstige mit dem KBA vereinbarte Kommunikationswege.

Sofern die Dringlichkeit dies gebietet, sollte die Meldung vorab telefonisch erfolgen (Telefon: 0461-316-2611).

(2) Bisher etablierte Meldewege können beibehalten werden. Gleiche Informationen müssen grundsätzlich nicht an mehrere Adressaten gemeldet werden. Das KBA bittet aber darum, andere möglicherweise interessierte Organisationseinheiten des KBA und/oder : cybersecurity@kba.de cc: zu setzen bzw. die zuständigen Stellen direkt zu informieren, wenn davon ausgegangen werden kann, dass die Information auch für diese von Interesse sein kann[3].

(3) Alternativ bzw. ergänzend zur schriftlichen Berichterstattung kann der Hersteller andere Formen der Berichterstattung vorschlagen (siehe auch “Anwendung der Regeln für die Benennung/Anerkennung von TD (Kategorien A, B, D) zu Prüfungen im Rahmen des KBA-Typgenehmigungsverfahrens nach den UN-Regelungen 155/156”, Abschnitt B 2.2).

(4) Der Bericht an das KBA ersetzt nicht die Berichtspflicht an den TD. Die Kommunikation zwischen Hersteller und dem zuständigen TD ist gesondert zwischen diesen zu vereinbaren.

(5) Bei digitaler Kommunikation muss der Absender eindeutig zu identifizieren und die Information gegen Verfälschung geschützt sein. Die genutzten Verfahren sind mit dem KBA abzustimmen.

(6) Regelmäßige Meldungen des Herstellers dienen dem Nachweis der Wirksamkeit des CSMS/SUMS und ermöglichen dem TD und dem KBA, ihren Kontrollpflichten nachzukommen. Sie sind mindestens alle 12 Monate nach Erteilung der Konformitätsbescheinigung an beide Stellen zu übermitteln. Sie enthalten für den Berichtszeitraum zusammengefasste Informationen[4]. Falls ein kürzerer Berichtszeitraum vereinbart worden ist, sind quantitative Angaben zusätzlich kumulativ für das gesamte Jahr anzugeben.

---

2 Digitale Signaturen und ähnliche Maßnahmen zum Schutz der Integrität und Authentizität sind gestattet, sofern die Entnahme der Daten nicht behindert wird.

3 gilt nicht für die regelmäßig zu liefernden Berichte

4 Betrifft auch bereits gemeldete Ereignisse. Details müssen nicht wiederholt werden.

Zur Zusammenstellung und Übermittlung des Berichts wird dem Hersteller eine Karenzzeit von drei Monaten gewährt.[5]

(7) Ad-hoc-Meldungen zu internen sowie externe Ereignissen[6] sind an das KBA zu richten, nachdem die Relevanz intern geprüft wurde. In Zweifelsfällen, insbesondere, wenn möglicherweise Ereignisse von erheblicher Tragweite vorliegen, muss eine vorläufige Meldung vor Abschluss der Prüfung erfolgen. Der Hersteller sollte ad-hoc-Meldungen nach eigenem Ermessen sowie auf Verlangen des TD bei dessen berechtigtem Interesse auch an diesen adressieren.

(8) Die Berichte und Meldungen sind unabhängig von eventuell geplanten oder bereits erfolgten Anträgen auf Änderung des Zertifikats für das Managementsystem oder der Typgenehmigung zu liefern.

(9) Zu Managementsystem und Genehmigungsobjekt kann dem KBA getrennt berichtet werden; ggf. wird die Information intern an die zuständigen Stellen des KBA weitergeleitet.

(10) Alle Beteiligten behandeln die zur Verfügung gestellten Informationen vertraulich[7].

(11) Sofern bestimmte Detailinformationen aus Geheimhaltungsgründen nicht vom Hersteller herausgegeben werden können, sind eine angemessen neutrale Darstellung und Referenzen zu den Detailinformationen zulässig. Das KBA wird Detailinformationen in geeigneter mit dem Hersteller abgestimmter Art und Weise einsehen und bewerten.

(12) Vom Hersteller wird erwartet, dass er auch Informationen zu neu erkannten Schwachstellen meldet, selbst, wenn für diese bereits Korrekturen und Korrekturmaßnahmen umgesetzt worden sind und deren Wirksamkeit nachgewiesen werden kann. Je nach Bedeutung kann dies eine Ad-hoc-Meldung erfordern. Diese Information wird bezüglich der Wirksamkeit der Maßnahmen ausgewertet.

(13) Verallgemeinerte und durch das KBA anonymisierte Aussagen werden vom KBA ggf. in geeigneter Form öffentlich gemacht (z.B. in Arbeitsgruppen, auf Fachtagungen, im Erfahrungsaustausch usw.). Damit soll erreicht werden, dass „best practice“ verallgemeinert wird und sich ggf. Vorkommnisse oder Beinahe-Vorfälle nicht wiederholen. Der betroffene Hersteller wird in jedem Fall informiert, bevor Informationen öffentlich gemacht werden (unabhängig davon, ob es sich um anonymisierte oder nicht anonymisierte Informationen handelt). Der Hersteller kann verlangen, dass Informationen nicht öffentlich kommuniziert werden, sofern dies nicht gesetzlich vorgeschrieben ist.

(14) Die Effektivität des Berichtswesens wird unter Beteiligung aller interessierten Kreise regelmäßig durch das KBA ausgewertet. In der Folge werden ggf. Anpassungen vorgenommen.

(15) Sofern hier nicht anders dargestellt, wird das KBA vorerst keine weitergehenden Vorgaben zur Berichterstattung machen. Der Hersteller sollte die beabsichtigte Art der Berichte zum CSMS/SUMS allerdings mit dem KBA (Dresden) abstimmen.

(16) In diesem Dokument werden Mindestforderungen formuliert. Forderungen des TD, anderer Bereiche des KBA oder anderer Behörden an den Hersteller, die über diese Leitlinien hinausgehen, bleiben unberührt.

(17) Ebenso unberührt bleiben spezielle Forderungen im Rahmen der Überprüfung der Konformität der Produktion oder der Marktüberwachung. Sofern Meldungen, für mehrere Bereiche

---

5 Dies ermöglicht alternativ die Meldung bis zu 3 Monaten nach dem Termin oder den Abschluss des Berichtszeitraums bis zu 3 Monaten vor dem Termin (mit folgendem Berichtszeitraum von maximal 12 Monaten).

6 Ereignisse können z.B. sein: Angriffe, wesentliche Nichtkonformitäten oder sonstige Schwachstellen im Managementsystem, nachträglich erkannte wesentliche Lücken in der Risikoanalyse, Anfälligkeit bzw. Versagen von Produkten, die im Zusammenhang mit den UN-R 155/156 stehen usw.

7 Dies schließt den erforderlichen Informationsaustausch zwischen KBA-BSI und TD nicht aus.

des KBA relevant sein könnten, wird empfohlen, diese bereits durch den Hersteller in Kopie an alle betroffenen Bereiche zu senden.

(18) Der Berichtspflicht unterliegen auch cybersecurity-relevante Ereignisse, Vorfälle und Kontrollergebnisse mit Bezug auf die für den Betrieb des Genehmigungsobjekts notwendigen Backend-, Service- und ähnliche Lösungen.

7 Berichterstattung im Rahmen der UN-R 155

7.1 Regelmäßiger Bericht entsprechend UN-R 155 Abschnitt 7.4.1

7.1.1 Allgemeines

Sofern sinnvoll, sind quantitative Daten vorzugsweise grafisch darzustellen. Dabei gilt der in 7.1.2 definierte Mindestinhalt. Der Hersteller stimmt sich bzgl. des Detaillierungsgrads mit dem KBA (Dresden) ab. Tendenzen gegenüber früheren Berichtsperioden sollten dargestellt werden.

7.1.2 Mindestinhalt des Berichts an das KBA (Dresden)

7.1.2.1 In Bezug auf das CSMS

- Geplante Maßnahmen für den Berichtszeitraum, Angaben zur Realisierung, zusätzlich durchgeführte Maßnahmen[8]
- Ergebnisse (ggf. unterteilt nach Kategorien des Herstellers) einschließlich wesentlicher Korrekturmaßnahmen
- Bewertung der Angemessenheit und Wirksamkeit von
    - Internem Monitoringprogramm (einschl. Personal, sonstige Ressourcen, Art/Häufigkeit/Umfang der Maßnahmen usw.)
    - Korrekturmaßnahmen

7.1.2.2 In Bezug auf das Genehmigungsobjekt jeweils für Produktions- und - Nach-Produktionsphase

- Art- des Ereignisses[9]
- Anzahl der Ereignisse je Ereignisart
- Ergebnisse von Ursachenanalysen und Korrekturmaßnahmen für jedes Ereignis
- Bewertung und Bestätigung der Angemessenheit und Wirksamkeit von Korrekturmaßnahmen

7.1.2.3 Sonstige Information

- Geplante und realisierte wesentliche Änderungen an Struktur und Prozessen des CSMS sowie an der Risikoanalyse
    - Beschreibung der Aktivität
    - Ziel und Begründung
    - Mögliche Auswirkungen auf die relevanten Genehmigungsobjekte und sonstige zu schützende Werte in Bezug auf deren Cybersicherheit
- Bewertung möglicher Einflüsse von neuen Typgenehmigungen und Änderungen von Typgenehmigungen auf das CSMS

7.1.2.4 Zusammenfassende Bewertung bzgl. der Angemessenheit und Effektivität der umgesetzten Maßnahmen

8 z.B. System-/Prozess-/Sicherheitsaudit, Managementbewertungen, Zertifizierungsaudits durch den TD, usw.

9 Insbesondere Informationen in Bezug auf die Abschnitte 7.2.2.2 g und h der UN-R 155

7.2 Ad-hoc-Meldung

7.2.1 Notwendigkeit

Ad-hoc-Meldungen sind notwendig bei[10]

- Ereignissen, die unmittelbaren Einfluss auf die Gültigkeit von CSMS-Zertifikat oder Typgenehmigung haben könnten.
- wesentliche Nichtkonformitäten des CSMS.
- Erfolgreichen und versuchten Angriffen.

7.2.2 Inhalt der Meldung (soweit sinnvoll und möglich)

- Datum des Ereignisses[11]
- Beschreibung des Ereignisses
  - Art/Kategorie des Ereignisses
  - Betroffene Elemente des CSMS bzw. genehmigungsrelevante Elemente der E/E-Architektur
  - Angriffspfade und -szenarien, mögliche(s) Angriffsziel(e)
  - reale und mögliche Folgen, Bewertung des Schweregrades
- Ursachenanalyse
- Sofort- und andere (geplante) Maßnahmen
- Geplante Maßnahmen zur Wirksamkeitskontrolle
- Von der Art her wiederholtes Ereignis (ja/nein)
- Anpassung des Maßnahmenkataloges, der Risikoanalyse für das Genehmigungsobjekt (und ggf. der Typgenehmigung) oder des CSMS (und ggf. der Konformitätsbescheinigung für das CSMS) erforderlich/erfolgt (ja/nein)[12]
- Interne Vorgangsnummer des Herstellers
- Ggf. Registrierungsmerkmal in externen Systemen (z.B. CVE-Nummer)

7.3 Ergänzende Information

Zur Stärkung des internationalen Typgenehmigungsverfahrens bittet das KBA darum, im Rahmen der regelmäßigen bzw. Ad-hoc-Meldungen auch zu informieren zu

- sonstigen neu erkannten möglichen Bedrohungen und Problemen, die potenziell herstellerübergreifend von Bedeutung sein könnten (z.B. offensichtlich gehäuft auftretende reale oder versuchte Angriffe, auch, wenn über diese bereits unmittelbar bei Bekanntwerden (ad-hoc) berichtet wurde[13])
- Anfragen Externer, die für das KBA von Bedeutung sein könnten[14]
- Verwendung des CSMS-Zertifikats für Genehmigungen bei anderen Genehmigungsbehörden

8 Berichterstattung im Rahmen der UN-R 156

8.1 Mindestinhalt des regelmäßigen Berichts an das KBA (Dresden)

8.1.1 Internes Monitoring des Managementsystems

- Planung von Maßnahmen für den Berichtszeitraum, Angaben zur Realisierung, zusätzlich durchgeführte Maßnahmen[15]

---

10 s. auch Abschnitt 6 Ziffer (13)

11 sofern nicht bekannt, des Datum des Bekanntwerdens

12 "Nein" bitte begründen

13 auch, wenn keine Anpassung des eigenen CSMS notwendig war

14 insbesondere Anfragen anderer Genehmigungs- und Marktüberwachungsbehörden und sonstige Anfragen mit Bezug auf das Zertifikat, der auf dessen Grundlage erteilten Genehmigungen und das Verfahren der Erteilung und Überwachung von Zertifikat und Genehmigung insgesamt

15 z.B. System-/ Prozess-/Sicherheitsaudit, Managementbewertungen, Zertifizierungsaudit durch den TD, usw.

- Ergebnisse (ggf. unterteilt nach Kategorien des Herstellers) einschließlich wesentlicher Korrekturmaßnahmen
- Bewertung der Angemessenheit und Wirksamkeit von
    - Internem Monitoringprogramm (einschl. Personal, sonstige Ressourcen, Art/Häufigkeit/Umfang der Maßnahmen usw.)
    - Korrekturmaßnahmen

8.1.2 Sonstige Information

- Geplante und realisierte wesentliche Änderungen an Struktur und Prozessen des SUMS sowie an der Risikoanalyse
    - Beschreibung der Aktivität
    - Ziel und Begründung
    - Mögliche Auswirkungen auf die relevanten Genehmigungsobjekte und sonstige zu schützende Werte in Bezug auf die Sicherheit von Softwareupdates
- Bewertung möglicher Einflüsse von neuen Typgenehmigungen und Änderungen von Typgenehmigungen auf das SUMS

8.2 Ad-hoc-Meldung

8.2.1 Notwendigkeit

Ad-hoc-Meldungen sind notwendig bei[16]

- Ereignissen, die unmittelbaren Einfluss auf die Gültigkeit von SUMS-Zertifikat oder Typgenehmigung haben könnten.
- Wesentliche Nichtkonformitäten

8.2.2 Inhalt der Meldung (soweit sinnvoll und möglich)

- Datum des Ereignisses[17]
- Beschreibung des Ereignisses
    - Art/Kategorie des Ereignisses
    - Betroffene Elemente des SUMS
    - reale und mögliche Folgen, Bewertung des Schweregrades
- Ursachenanalyse
- Sofort- und andere (geplante) Maßnahmen
- Geplante Maßnahmen zur Wirksamkeitskontrolle
- Von der Art her wiederholtes Ereignis (ja/nein)
- Anpassung der Risikoanalyse für das Genehmigungsobjekt (und ggf. der Typgenehmigung) oder des SUMS (und ggf. der Konformitätsbescheinigung für das SUMS) erforderlich/erfolgt (ja/nein) [18]
- Interne Vorgangsnummer des Herstellers

8.3 Ergänzende Information

Das KBA bittet darum, im Rahmen der regelmäßigen bzw. ad-hoc-Information im Interesse des internationalen Typgenehmigungsverfahrens auch zu informieren zu

- Anfragen Externer, die für das KBA von Bedeutung sein könnten[19]

---

16 s. auch Abschnitt 6 Ziffer (13)

17 sofern nicht bekannt, des Datum des Bekanntwerdens

18 "Nein" bitte begründen

19 insbesondere Anfragen anderer Genehmigungs- und Marktüberwachungsbehörden und sonstige Anfragen mit Bezug auf das Zertifikat, der auf dessen Grundlage erteilten Genehmigungen und das Verfahren der Erteilung und Überwachung von Zertifikat und Genehmigung insgesamt

Verwendung des SUMS-Zertifikats für Genehmigungen bei anderen Genehmigungsbehörden

Impressum

Herausgeber:
Kraftfahrt-Bundesamt
24932 Flensburg

Internet: www.kba.de

Fachliche Auskünfte und Beratung:

Telefon: +49 461 316-2600
E-Mail: cybersecurity@kba.de

Revision 1.0 final, Stand: 27.06.2022

Bildquelle: KBA/www.shutterstock.com (© Bauer Alexander)

Alle Rechte vorbehalten. Die Vervielfältigung und Verbreitung dieser Veröffentlichung, auch auszugsweise und in digitaler Form, ist nur mit Quellenangabe gestattet. Dies gilt auch, wenn Inhalte dieser Veröffentlichung weiterverbreitet werden, die nur mittelbar erlangt wurden.

© Kraftfahrt-Bundesamt, Flensburg