Verordnung zum IT-Sicherheitskennzeichen des Bundesamtes für Sicherheit in der Informationstechnik (BSI-IT-Sicherheitskennzeichenverordnung - BSI-ITSiKV)

Vom 24. November 2021 (BGBl. I S. 4978)

Auf Grund des § 10 Absatz 3 des BSI-Gesetzes vom 14. August 2009 (BGBl. I S. 2821), der durch Artikel 1 Nummer 21 des Gesetzes vom 18. Mai 2021 (BGBl. I S. 1122) eingefügt worden ist, verordnet das Bundesministerium des Innern, für Bau und Heimat im Einvernehmen mit dem Bundesministerium der Justiz und für Verbraucherschutz und dem Bundesministerium für Wirtschaft und Energie:

§ 1 Anwendungsbereich

Diese Verordnung regelt die Gestaltung und Verwendung des IT-Sicherheitskennzeichens im Sinne des § 9c Absatz 1 Satz 1 des BSI-Gesetzes und legt das Verwaltungsverfahren zur Sicherstellung der Anforderungen im Zusammenhang mit der Verwendung des Kennzeichens fest.

§ 2 Begriffsbestimmungen

Im Sinne dieser Verordnung ist oder sind:

1. Hersteller

   jede juristische oder natürliche Person, die einen Dienst anbietet oder ein Produkt herstellt beziehungsweise entwickeln oder herstellen lässt und dieses Produkt oder diesen Dienst unter ihrem eigenen Namen oder ihrer eigenen Marke vermarktet; nicht erfasst sind die Hersteller einzelner Teile oder Komponenten davon;

2. Verkäufer

   jede juristische oder natürliche Person, die gewerblich ein Produkt unmittelbar Verbrauchern und Verbraucherinnen auf dem Markt bereitstellt;

3. Branche

die Unternehmen und Organisationen und ihre Verbände, die für den jeweiligen Wirtschaftsbereich Produkte oder Dienstleistungen im Geltungsbereich dieses Gesetzes herstellen oder vertreiben;

4. branchenabgestimmte IT-Sicherheitsvorgabe

   ein Anforderungskatalog, der von einer Branche erstellt und gepflegt wird und dessen Geeignetheit das Bundesamt nach § 9c Absatz 3 Satz 1 des BSI- Gesetzes festgestellt hat;

5. geeignete und qualifizierte Dritte

   juristische oder natürliche Personen, die aufgrund ihrer fachlichen Qualifikation eine Aussage darüber treffen können, ob Sicherheitsversprechen eines Produktes eingehalten werden oder bestimmte Eigenschaften nachgewiesen werden können;

6. Plausibilitätsprüfung

   die Sichtung der Herstellererklärung, der Angaben des Herstellers im Antrag und eventueller Unterlagen zur Ermittlung, ob die Konformität mit den vom Bundesamt festgelegten Sicherheitsanforderungen plausibel und nachvollziehbar zugesichert wird;

7. Produktkategorie

   ein durch das Bundesamt festgelegter Oberbegriff für die Erfassung einer Gruppe von vergleichbaren informationstechnischen Produkten in einem eingrenzbaren Bereich;

8. zugehörige Internetseite

   der für das einzelne Produkt angepasste Zielbereich auf der Internetseite des Bundesamtes, auf der Informationen zu diesem Produkt vorgehalten werden;

9. Etikett

   die physische oder elektronische Kennzeichnung am Produkt oder seiner Umverpackung, welche produktspezifisch mit dem Verweis auf die zugehörige Internetseite angepasst wird.

§ 3 Gestaltung des Etiketts und der Internetseite zum IT-Sicherheitskennzeichen

(1) Das IT-Sicherheitskennzeichen besteht aus der Herstellererklärung und der Sicherheitsinformation nach § 9c Absatz 2 des BSI-Gesetzes, auf die beide auf dem Etikett verwiesen wird. Das Etikett versetzt den Verbraucher in die Lage, sich ohne erhebliche Hürden mittels gängiger technischer Hilfsmittel über die Art und Aussage der Herstellererklärung gegenüber den Vorgaben des Bundesamtes, die eventuell zur Verfügung stehenden aktuellen Sicherheitsinformationen und die Laufzeit des Kennzeichens zu informieren.

(2) Das Etikett hat dafür jedenfalls zwingend zu umfassen:

1. einen Verweis auf die zugehörige Internetseite des Bundesamtes nach Absatz 4;
2. die Nennung des Bundesamtes.

(3) Das Etikett kann durch das Bundesamt mit einer grafischen Darstellung ausgestaltet werden, um mittels dieser bildlich für den Verbraucher einen sofortigen Wiedererkennungswert zu erzeugen.

(4) Auf der Internetseite des Bundesamtes sind die Herstellererklärung und die Sicherheitsinformation in aktueller Fassung mit der Laufzeit des Kennzeichens abrufbar. Der Hersteller stellt dem Bundesamt hierfür in eigener Verantwortung aktuelle Sicherheitsinformationen zur Konformität des Produktes zur Verfügung, die das Bundesamt auf der zugehörigen Internetseite einstellt. Das Bundesamt kann zudem weitere Informationen über sicherheitsrelevante IT-Eigenschaften und darüber, ob und inwieweit die Herstellererklärung nach derzeitiger Kenntnis eingehalten wird, einstellen.

(5) Das Bundesamt kann eine Applikation zur Verfügung stellen, in der die Informationen zum Herstellerversprechen von Produkten bereitgestellt und abgerufen werden können.

§ 4 Antrag

(1) Ein Antrag auf Freigabe des IT-Sicherheitskennzeichens für ein Produkt kann nur innerhalb der vom Bundesamt nach § 11 bekannt gegebenen Produktkategorien gestellt werden. Der Antrag kann vom Hersteller des Produktes gestellt werden.

(2) Der Antrag ist unter Verwendung der dafür geltenden Vorlage einzureichen, wenn das Bundesamt eine solche veröffentlicht hat. Der Hersteller hat dafür Sorge zu tra-

gen, dass die Erklärung und beigefügten Unterlagen ausschließlich zutreffende Angaben enthalten.

(3) Der Eingang des Antrags wird vom Bundesamt bestätigt. Das Bundesamt teilt dabei die geltende Prüfungsfrist für die Freigabeerklärung nach dieser Verordnung mit.

§ 5 Antragsprüfung

(1) Das Bundesamt führt anhand der eingereichten Unterlagen eine Plausibilitätsprüfung durch. Die Prüfung erfolgt innerhalb der nach § 11 Absatz 1 festgelegten Prüfungsfrist und anhand einer Verfahrensbeschreibung zum Ablauf des Prüfverfahrens, die vom Bundesamt veröffentlicht wird.

(2) Das Bundesamt kann die Überprüfung von Herstellerdokumenten auf qualifizierte Dritte im Sinne des § 2 Nummer 5 übertragen.

(3) Ist für ein Produkt eine geeignete branchenabgestimmte IT-Sicherheitsvorgabe nach § 10 einschlägig, sind für die Plausibilitätsprüfung die Vorgaben dieses Standards ausschlaggebend.

(4) Liegen die gesetzlichen Voraussetzungen gemäß § 9c Absatz 5 BSIG vor, erteilt das Bundesamt die Freigabe zur Nutzung des IT-Sicherheitskennzeichens.

(5) Das Bundesamt kann den Antrag ablehnen, wenn Hinweise dafür vorliegen, dass

1. das Produkt oder die mit dem Produkt ausgelieferte Software bekannte Sicherheitslücken enthält oder
2. Produkte des Herstellers bereits Gegenstand einer Warnung oder Information nach den §§ 7 oder 7a des BSI-Gesetzes oder von Maßnahmen nach § 9c Absatz 8 des BSI-Gesetzes betroffen waren.

Das Bundesamt kann die Freigabe der Nutzung auch dann verweigern, wenn der Freigabe unabhängig von den eingereichten Unterlagen ernstliche Zweifel an der Herstellererklärung entgegenstehen.

(6) Entscheidungen, mit denen abschließend über einen nach dieser Verordnung gestellten Antrag entschieden wird, sind schriftlich oder elektronisch zu erlassen.

§ 6 Vereinfachtes Verfahren

(1) Das Bundesamt kann auf die Plausibilitätsprüfung verzichten, wenn das Bundesamt für das Produkt ein Zertifikat nach § 9 des BSI-Gesetzes auf Grundlage des gleichen Prüfstandards erteilt hat.

(2) Ist für ein Produkt bereits ein ausländisches staatliches Kennzeichen auf Grundlage des gleichen oder eines vergleichbaren Prüfstandards und auf Grundlage der gleichen oder vergleichbarer Prüfspezifikationen vergeben worden, kann das Bundesamt den Antrag unter Vorlage dieses Kennzeichens und der zugrunde liegenden Unterlagen in deutscher oder englischer Sprache prüfen. Das Bundesamt legt in einem Kriterienkatalog fest, unter welchen Voraussetzungen ein Prüfstandard eines anderen Kennzeichens mit solchen nach dieser Verordnung vergleichbar ist und veröffentlicht diesen auf seiner Internetseite.

§ 7 Gegenstand der Herstellererklärung

(1) Die Herstellererklärung enthält die Zusicherung, dass das Produkt für die nach § 8 festgelegte Dauer die für die einschlägige Produktkategorie geltenden IT- Sicherheitsanforderungen erfüllt. Der Hersteller verpflichtet sich innerhalb des Zeitraumes nach § 8 Absatz 1 Satz 1, das Bundesamt unaufgefordert zu informieren, wenn sich die vom Hersteller erklärten Eigenschaften des Produktes ändern, sobald sie ihm bekannt werden, einschließlich Störungen der Informationssicherheit des Produktes und Sicherheitslücken. Der Hersteller verpflichtet sich des Weiteren, ihm bekannt werdende Sicherheitslücken unverzüglich zu beheben und den Stand der dafür erfolgten Maßnahmen dem Bundesamt mit den in § 3 Absatz 4 Satz 2 genannten Informationen anzuzeigen.
(2) Das Bundesamt informiert auf seiner Internetseite über die Änderung oder Aufhebung der für die einschlägige Produktkategorie geltenden IT-Sicherheitsanforderungen, Technischen Richtlinien oder die Ungeeignetheit von branchenabgestimmten IT-Sicherheitsvorgaben.
(3) Bedient sich der Antragsteller zur Antragstellung oder zur Erfüllung seiner Pflichten aus § 9c des BSI- Gesetzes oder dieser Rechtsverordnung eines Dritten, werden ihm die Handlungen des Dritten wie eigene zugerechnet.

§ 8 Laufzeit des IT-Sicherheitskennzeichens und Erlöschen

(1) Der Hersteller versichert, dass die Herstellererklärung für die dafür festgelegte Dauer erfüllt wird (Laufzeit). Die Laufzeit beträgt regelmäßig zwei Jahre. Eine abweichende Laufzeit kann durch das Bundesamt für die Produktkategorie festgelegt oder in der zugrunde gelegten Technischen Richtlinie oder branchenabgestimmten IT-

Sicherheitsvorgaben bestimmt werden. Das Bundesamt hat bei abweichenden Laufzeiten diese gemeinsam mit der Produktkategorie zu veröffentlichen.
(2) Mit Ablauf der Laufzeit erlischt die Freigabe des Bundesamtes. Das Bundesamt weist in der BSI-Sicherheitsinformation öffentlich auf den Ablauf der Laufzeit hin.
(3) Für ein Produkt, für das ein gültiges IT-Sicherheitskennzeichen besteht, kann derselbe Hersteller frühestens drei Monate und spätestens sechs Wochen vor Ablauf der Gültigkeit des IT-Sicherheitskennzeichens dessen Verlängerung beantragen. Die für die erstmalige Freigabe geltenden Vorschriften gelten entsprechend.
(4) Wird eine für die einschlägige Produktkategorie geltende IT-Sicherheitsvorgabe geändert oder für ungültig erklärt, erlischt die Freigabe nach einer Frist von sechs Wochen, wenn der Hersteller die Herstellererklärung nicht auf einer gültigen Prüfgrundlage aktualisiert. Das Bundesamt weist auf entsprechende Änderungen, Ungeeignetheit oder Aufhebungen in der Veröffentlichung der Produktkategorie nach § 11 hin.
(5) Bei einem Verstoß gegen die Herstellererklärung, die gesetzlichen Herstellerpflichten, bei unzutreffenden oder unvollständigen Angaben, sowie dem sonstigen Wegfall der Erfüllung der gesetzlichen Voraussetzungen oder Anforderungen des Bundesamtes kann das Bundesamt die Freigabe unverzüglich widerrufen. Dem Antragsteller ist eine angemessene Frist zur Stellungnahme zu geben, es sei denn, gewichtige Sicherheitsgründe erfordern eine sofortige Maßnahme.

§ 9 Verwendung des Sicherheitskennzeichens

(1) Das produktspezifische Etikett darf in physischer und elektronischer Ausführung für die Dauer der Freigabe nach den Vorgaben des § 9c des BSI-Gesetzes und dieser Rechtsverordnung verwendet werden. Das Bundesamt legt die grafische Gestaltung des Sicherheitskennzeichens sowie des Etiketts fest und veröffentlicht diese auf seiner Internetseite. Hersteller dürfen gemäß ihrer Freigabe keine von diesen Vorgaben abweichende Gestaltung verwenden.
(2) Mit der Freigabe stellt das Bundesamt dem Hersteller das produktspezifische Etikett zur Verfügung. Das Etikett darf nach der Freigabe auf Produkten oder deren Umverpackungen vom Hersteller angebracht werden.
(3) Hersteller und Verkäufer sind berechtigt, das Kennzeichen für die Dauer der Freigabe zu Werbezwecken für das Produkt zu verwenden. Dabei ist ein Verweis auf die zugehörige Internetseite nach § 3 Absatz 4 gut sichtbar anzuzeigen.

(4) Liegt keine Freigabe mehr vor, erlöschen die Rechte von Hersteller und Verkäufer nach dieser Vorschrift. Der Hersteller hat dafür Sorge zu tragen, dass keine nach dem Erlöschen hergestellten Produkte mehr mit dem Etikett auf den Markt gebracht werden.

§ 10 Anerkennung von Normen, Standards oder branchenabgestimmten IT-Sicherheitsvorgaben

(1) Das Bundesamt kann von Amts wegen feststellen, dass eine bestehende Norm oder ein Standard geeignet ist, die Anforderungen nach § 5 Absatz 3 zu gewährleisten. Ein Anspruch auf diese Feststellung besteht nicht.
(2) Branchenverbände oder Hersteller können branchenabgestimmte IT-Sicherheitsvorgaben zur Gewährleistung der Anforderungen nach § 5 Absatz 3 vorschlagen. Das Bundesamt stellt auf Antrag fest, ob diese geeignet sind, die Anforderungen nach § 5 Absatz 3 zu gewährleisten. Die Feststellung befristet das Bundesamt entsprechend der zu erwartenden Entwicklungen in der Produktkategorie. Ein Anspruch auf diese Feststellung besteht nicht.
(3) Für eine Norm, einen Standard oder eine branchenabgestimmte IT-Sicherheitsvorgabe, der oder die nicht mehr diesen Anforderungen oder dem Stand der Technik entspricht oder in eine Technische Richtlinie überführt wurde, kann die Feststellung nach Absatz 1 vom Bundesamt vor Ablauf der Frist widerrufen werden.
(4) Wird für eine Produktkategorie mehr als ein Antrag nach Absatz 2 gestellt, so gibt das Bundesamt den Standard mit einer angemessenen Frist zur Einigung an die Vorschlagenden zurück; es kann nach Ablauf dieser Frist ohne Einigung einen der Standards zur Prüfung auswählen.
(5) Ein oder mehrere branchenspezifische Sicherheitsstandards oder eine oder mehrere branchenabgestimmte IT-Sicherheitsvorgaben können vom Bundesamt im Benehmen mit der Branche in eine Technische Richtlinie überführt werden.

§ 11 Produktkategorien

(1) Das Bundesamt legt die Produktkategorien fest, für deren Produkte es die Freigabe des IT-Sicherheitskennzeichens erteilt. Es gibt die Produktkategorie und die regelmäßige Prüfungsfrist für die Antragsbearbeitung durch im Bundesanzeiger veröffentlichte Allgemeinverfügung bekannt, bevor es die für die jeweilige Produktkategorie einschlägigen IT-Sicherheitsanforderungen veröffentlicht. Legt das Bundesamt

keine Prüfungsfrist für die Produktkategorie fest, gilt eine Prüfungsfrist ab vollständigem Antragseingang von sechs Wochen.
(2) Das Bundesamt kann für die konkreten Sicherheitsanforderungen auf bestehende Vorgaben, Standards, Technische Richtlinien, Prüfgrundlagen oder branchenabgestimmte IT-Sicherheitsvorgaben verweisen und bemüht sich um den Gleichlauf mit international etablierten Standards.
(3) Die Produktkategorien veröffentlicht das Bundesamt nach Bekanntgabe mit den aktuellen Anforderungen und der Prüfungsfrist auf seiner Internetseite. Es weist ebenso auf eventuelle Änderungen, Aufhebungen oder eine Feststellung der Ungeeignetheit der Anforderungen hin.
(4) Änderungen der Produktkategorie, welche die Kategorie wesentlich verändern oder ganz entfernen, bedürfen ebenfalls der Bekanntgabe mit einer im Bundesanzeiger veröffentlichten Allgemeinverfügung.

§ 12 Aufsicht

(1) Eine Aufsicht über Produkte und Hersteller, welche die Freigabe zur Nutzung des Sicherheitskennzeichens erhalten haben, erfolgt für die Dauer der
Freigabe. Sie erfolgt anlasslos auf der Grundlage eines Überwachungskonzeptes sowie anlassbezogen reaktiv und kann eine Sachprüfung umfassen.
(2) Ein Marktüberwachungskonzept im Sinne des Absatzes 1 wird vom Bundesamt erarbeitet. Die dortigen Regelungen sollen bei der anlasslosen Marktüberwachung zugrunde gelegt werden.
(3) Zur effektiven Marktaufsicht kann das Bundesamt sich Dritter im Sinne des § 2 Nummer 5 bedienen und Testkäufe vornehmen. Es kann öffentlich bekannt gewordene Sicherheitsinformationen und Berichte von Verbraucherorganisationen zur Grundlage seiner Aufsicht machen.

§ 13 Informationen für Verbraucher

Verbraucherinformationen zu Produkten mit der Freigabe zur Nutzung des IT-Sicherheitskennzeichens werden in der Sicherheitsinformation nach § 9c Absatz 2 des BSI-Gesetzes auf der Internetseite des Bundesamtes veröffentlicht. Davon unberührt bleiben die Bestimmungen der §§ 7 und 7a des BSI-Gesetzes.

§ 14 Evaluierung

Drei Jahre nach Inkrafttreten dieser Rechtsverordnung und folgend alle drei Jahre sind unter Beteiligung der in § 10 Absatz 3 Satz 1 des BSI-Gesetzes genannten Ressorts zu evaluieren:

1. die Produktkategorien;
2. die Anerkennung von Branchenstandards;
3. die Freigabekriterien für das Kennzeichen.

§ 15 Inkrafttreten

Diese Verordnung tritt am Tag nach der Verkündung in Kraft.