verbraucherzentrale
Baden-Württemberg

Stellungnahme zum

Referentenentwurf zur Rechtsverordnung zum IT-Sicherheitskennzeichen des Bundesamtes für Sicherheit in der Informationstechnik (BSI-ITSiKV)

6. September 2021

Impressum

Verbraucherzentrale
Baden-Württemberg e.V.

Verbraucherpolitik

Paulinenstraße 47
70178 Stuttgart

Vorstand@vz-bw.de

Verbraucherzentrale Baden-Württemberg e.V.

1. WÜRDIGUNG

Die Bestimmungen der Rechtsverordnung zum IT-Sicherheitskennzeichen des Bundesamtes für Sicherheit in der Informationstechnik (BSI-ITSiKV) sollen dazu dienen, das nach § 9c Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (BSI-Gesetz) einzuführende IT-Sicherheitskennzeichen konkret auszugestalten und das erforderliche Verwaltungsverfahren festzulegen.

Durch die konkrete Ausgestaltung sollen Verbraucher:innen in die Lage versetzt werden, den Aspekt der IT-Sicherheit bei der Auswahl ihrer IT-Produkte in einfacher und verständlicher Form zu berücksichtigen.

Die Verbraucherzentrale Baden-Württemberg nimmt gerne wie folgt zur BSI-ITSiKV Stellung.

2. SACHVERHALT

Die zentralen Elemente des Gesetzeszwecks sind in den §§ 3, 5, 12 und 13 BSI-ITSiKV benannt.

- **§3 - Gestaltung des Etiketts und der Website zum IT-Sicherheitskennzeichen**

Ein Etikett, das auf dem Produkt oder der Umverpackung angebracht ist bzw. unter bestimmten Umständen elektronisch auf der Homepage des Herstellers angegeben ist, soll den Verbraucher:innen ermöglichen, zu überprüfen, ob das jeweilige IT-Produkt bzw. dessen Hersteller aktuelle Sicherheitsstandards in ausreichend berücksichtigt. Dazu soll das Etikett einen Verweis auf die zugehörige Website des BSI und die Nennung des BSI umfassen.

Auf der zugehörigen Webseite stellt das BSI den Verbraucher:innen die Herstellererklärung und die Sicherheitsinformation in aktueller Fassung mit der Laufzeit des Kennzeichens zur Verfügung. Dort soll das BSI zudem weitere Informationen über sicherheitsrelevante IT-Eigenschaften und darüber, ob und inwieweit die Herstellererklärung nach derzeitiger Kenntnis eingehalten wird, aufführen können.

Um den Vebraucher:innen die produkt- bzw. herstellerübergreifende Widererkennung des Etiketts zu ermöglichen, soll das BSI das Etikett grafisch entsprechend ausgestalten können.

Zudem soll das BSI eine Applikation zur Verfügung stellen können, in der die Informationen zum Herstellerversprechen von Produkten bereitgestellt und abgerufen werden können.

- **§ 5 - Antragsprüfung**

Grundlage des Etiketts ist die Antragsprüfung gemäß § 5 BSI-ITSiKV. Die Antragsprüfung soll vom Bundesamt für Sicherheit in der Informationstechnik (BSI) als Plausibilitätsprüfung durchgeführt werden. § 1 Nr. 6 definiert die Plausibilitätsprüfung als die Sichtung der Herstellererklärung, der Angaben des Herstellers im Antrag und eventueller Unterlagen zur Ermittlung, ob die Konformität mit den vom BSI festgelegten Sicherheitsanforderungen plausibel und nachvollziehbar zugesichert wird.

Die Begründung zu § 5 stellt dazu klar, dass die Plausibilitätsprüfung keine Tiefenprüfung der erklärten Sicherheitsvorgaben umfasst. Schon aus der Begründung zu § 9c

BSI-Gesetz geht hervor, dass dem Etikett auch die Voraussetzungen fehlen werden, als Gütezeichen zu fungieren. (Gütezeichen beruhen mindestens auf, a) eine unabhängige Stelle prüft die objektiven Kriterien einer Aussage - hier der IT-Sicherheitseigenschaften - vorab und b) die Einhaltung der Voraussetzungen wird regelmäßig überprüft. Vgl. BGH I ZR 161/18 vom 4. Juli 2019) Die Sichtung von Selbstauskünften und Herstellerklärungen erfüllt die an ein Gütezeichen gestellten Voraussetzungen nicht.

Zudem macht schon § 9 c BSI-Gesetz, Absatz 1 Satz 2 deutlich, dass die Antragsprüfung keine Prüfung der den Datenschutz betreffenden Eigenschaften eines Produktes umfasst.

- **§ 9 - Verwendung des IT-Sicherheitskennzeichens**

Das Etikett darf vom Hersteller nur über den Zeitraum der Freigabe auf Produkten oder deren Umverpackungen beziehungsweise in der Werbung verwendet werden. In der Werbung ist auf die zugehörige Webseite des BSI gut sichtbar hinzuweisen. Nach Ende der Freigabe hat de Hersteller dafür sorgezutragen, dass keine mit dem Etikett gekennzeichneten Produkte mehr auf den Markt kommen

Der Entwurf der Rechtsverordnung enthält aber keine Bestimmungen darüber, was nach Ablaufen beziehungsweise Erlöschen der Freigabe mit den Produkten zu erfolgen hat, die mit dem Etikett gekennzeichnet sind und auf dem Markt sind.

- **§12 - Aufsicht**

Zu den Aufgaben des BSI wird neben der Plausibilitätsprüfung die Aufsicht (§ 12 BSI-ITSiKV) gehören. Diese Aufsicht soll die registrierten Produkte, die das Etikett erhalten haben, hinsichtlich der Einhaltung der von BSI gesetzten Sicherheitsvorgaben sowohl anlasslos als auch anlassbezogen ggf. unter Einbeziehung von Testkäufen überprüfen.

- **§13 - Informationen für Verbraucher**

Das BSI soll nach § 13 BSI-ITSiKV auf der zugehörigen Webseite zusätzliche Informationen veröffentlichen. Diese zusätzlichen Informationen sollen über die Veröffentlichung der Angaben der Hersteller (Herstellererklärung, Sicherheitsinformationen) hinausgehen und den Verbraucher:innen helfen können, das Produkt für sich zu bewerten. So soll das BSI beispielsweise Abweichungen der tatsächlichen Beschaffenheit des Produktes gegenüber der Herstellererklärung, die einen Widerruf des Etiketts nach §8 Abs. 4 der Rechtsverordnung nicht rechtfertigen würden, auf der Webseite aufzeigen können. Insbesondere sollen diese Informationen Aktualisierungszyklen, Sicherheitseinstellungen ab Werk oder entdeckte Schwachstellen beinhalten können.

3. SCHLUSSFOLGERUNG UND FORDERUNGEN

Die mit BSI-ITSiKV angestrebte Konkretisierung macht deutlich, dass für Verbraucher:innen der Informationswert des IT-Sicherheitskennzeichens aufgrund fehlender Tiefenprüfung allenfalls in den vom BSI zusätzlich zur Verfügung gestellten Informationen gemäß § 13 besteht.

Vor diesem Hintergrund sind folgende Anforderungen an das Etikett, die Verbraucherkommunikation, die Applikation und die Werbung zu stellen:

- Die Bezeichnung IT-Sicherheitskennzeichen darf weder allgemein im Gesetz bzw. der Verordnung, noch in Bezug auf das Etikett, und auch nicht in der Verbraucherkommunikation, der Applikation, der Webseite und der Werbung verwendet werden,

da diese Bezeichnung in Zusammenhang mit der gesetzlichen Regelung den irrigen Eindruck vermittelt, die IT-Sicherheit des mit dem Etikett gekennzeichneten Produkts wäre durch eine staatliche Institution (hier das BSI) tiefenüberprüft und als gesichert anerkannt worden. Die vorgesehene Aufsicht wird diese Beschränkung nicht aufheben können, da von ihr nur ein geringer Teil der gekennzeichneten Produkte betroffen sein wird.

- Jeglicher Vermittlung des irrigen Eindrucks, das mit dem Etikett gekennzeichnete Produkt unterläge einer Prüfung der IT-Sicherheit beziehungsweise des Datenschutzes ist entgegenzutreten. Dazu werden folgende Bestimmungen in die BSI-ITSiKV aufgenommen:

  - *§ 3 Absatz 2 Nr. 3*
    3. einen leicht verständlichen und leicht wahrnehmbaren Hinweis, dass das mit dem Etikett gekennzeichneten Produkt keiner Tiefenprüfung der IT-Sicherheit beziehungsweise des Datenschutzes unterliegt.

  - *§ 3 Absatz 6*
    Im Rahmen der Verbraucherinformation und in der Applikation wird in einfacher, leicht verständlicher und leicht wahrnehmbarer Form darauf hingewiesen, dass das mit dem Etikett gekennzeichnete Produkt keiner Tiefenprüfung zur IT-Sicherheit und auch keiner Prüfung der Einhaltung der Datenschatzbestimmungen unterliegt Sternchentexte sind dabei auszuschließen.

  - *§ 9 Absatz 4*
    Im Rahmen der Werbung wird in einfacher, leicht verständlicher und leicht wahrnehmbarer Form darauf hingewiesen, dass das mit dem Etikett gekennzeichnete Produkt keiner Tiefenprüfung zur IT-Sicherheit und auch keiner Prüfung der Einhaltung der Datenschatzbestimmungen unterliegt Sternchentexte sind dabei auszuschließen.

- Das Etikett ist grafisch auszugestalten. Dabei darf das Etikett allerdings nicht durch seine grafische Gestaltung suggerieren, dass eine Tiefenprüfung der IT-Sicherheit stattgefunden hätte (d.h. eine sicherheitsbezogene Ikonografie, wie bspw. Schutzschilder, ist auszuschließen),

- Um bei Ablauf der Freigabe oder deren Erlöschen sicherzustellen, dass Verbraucher:innen weiterhin das Etikett als Information ansehen können, die ihnen ermöglicht, den Aspekt der IT-Sicherheit bei der Auswahl ihrer IT-Produkte in einfacher und verständlicher Form zu berücksichtigen, sind die Hersteller darauf zu verpflichten, umgehend dafür sorgezutragen, dass das Etikett nicht mehr auf dem Produkt beziehungsweise auf der Umverpackung, in der Werbung, der Applikation, der Verbraucherinformation verwendet wird. Zudem sind die Hersteller darauf zu verpflichten, die Verbraucher:innen über das Ende der Freigabe bzw. deren Erlöschen umgehend, leicht wahrnehmbar und verständlich zu informieren. Dazu wird folgende Bestimmung in die BSI-ITSiKV aufgenommen:

  - *§ 9 Absatz 5*
    Hersteller stellen nach Ablauf der Freigabe oder bei deren Erlö-

schen sicher, dass das Etikett auf keinem auf dem Markt befindlichen Produkt beziehungsweise deren Umverpackung und auch nicht mehr in der Werbung, der Applikation beziehungsweise der Verbraucherinformation verwendet wird.

- *§ 9 Absatz 6*
  Hersteller informieren nach Ablauf der Freigabe oder bei deren Erlöschen Verbraucher:innen umgehend, leicht wahrnehmbar und verständlich über das Ende der Freigabe oder deren Erlöschen.

➢ Um den Verbraucher:innen zu ermöglichen, überprüfen zu können, ob die von ihnen erworbene IT-Produkt bzw. dessen Hersteller aktuelle Sicherheitsstandards in ausreichend berücksichtigen, ist das BSI zu verpflichten, auf seiner Webseite alle seine Aufsichtserkenntnisse produkt- und herstellerbezogen zu veröffentlichen. Dazu wird folgende Bestimmung in die BSI-ITSiKV aufgenommen:

- *§ 12 Absatz 4*
  Das Bundesamt veröffentlicht alle seine im Rahmen der BSI-ITSiKV gewonnenen Aufsichtserkenntnisse unter Nennung des Produktes und des Herstellers auf der Webseite.

...