# Stellungnahme zum Entwurf einer Rechtsverordnung zum IT-Sicherheitskennzeichen

Das geplante IT-Sicherheitskennzeichen muss auf internationalen und Europäischen Normen und Standards basieren.

11. August 2021


**DIN e. V**.

Am DIN-Platz
Burggrafenstraße 6
10787 Berlin
www.din.de

**Kontakt:**

Katja Krüger
Senior Government Relations Manager
Tel.: 030 2601-2439
E-Mail: katja.krueger@din.de

**DKE**

Stresemannallee 15
60596 Frankfurt
Germany
www.dke.de

**Kontakt:**

Johannes Koch
Leiter Normungspolitik
Tel.: 069 6308-268
E-Mail: johannes.koch@vde.com

Den Zielen der nationalen Cyber-Sicherheitsstrategie 2016 und 2021 folgend betrifft IT-Sicherheit nicht mehr nur Konzerne und Kritische Infrastrukturen, sondern verstärkt auch den Verbraucher. Mit dem neuen IT-Sicherheitsgesetz 2.0 wurde speziell zur Beförderung digitaler Verbrauchersicherheit die gesetzliche Grundlage für ein neues, freiwilliges IT-Sicherheitskennzeichen geschaffen, das in § 9c BSIG geregelt ist.

Die Anforderungen zur konkreten Ausgestaltung des IT-Sicherheitskennzeichens ergeben sich gem. § 10 Abs. 3 BSIG aus einer Rechtsverordnung des Bundesministeriums des Innern, für die am 28. Juli 2021 ein Referentenentwurf veröffentlicht wurde („Rechtsverordnung zum IT-Sicherheitskennzeichen des Bundesamtes für Sicherheit in der Informationstechnik": Rechtsverordnung IT-Sicherheitskennzeichen – BSI-ITSiKV).

DIN und DKE – als durch den Normenvertrag von 1975 anerkannte nationale Normungsorganisationen – bedanken sich für die Möglichkeit der Kommentierung des Referentenentwurfs und merken Folgendes an:

(1) Ziel des IT-Sicherheitsgesetzes 2.0 ist ein ausreichendes Schutz- und Sicherheitsniveau, insbesondere für Verbraucher. **Dieses Ziel kann bestmöglich erreicht werden, wenn dem einzuführenden IT-Sicherheitskennzeichen internationale und Europäische Normen zugrunde gelegt werden**, an deren Erarbeitung und Pflege sich deutsche Stakeholder sowie die öffentliche Hand, z. B. vertreten durch das BSI, über die nationalen Normungsorganisationen DIN und DKE aktiv beteiligen. Ergänzt werden können diese Normen durch Standards, die mit dem deutschen Normenwerk kohärent sind (z. B. DIN SPEC 27072 „Informationstechnik - IoT-fähige Geräte - Mindestanforderungen zur Informationssicherheit"). Dadurch beugt der Gesetzgeber einer Fragmentierung der Standardisierungslandschaft und der digitalen Märkte vor. Zusätzlich schafft er praxistaugliche Regeln für Hersteller, Anwender, Beschaffer und Verbraucher und stellt sicher, dass die geschaffenen Lösungen europäisch skalierbar sind und in die internationale Normung eingebracht werden.

(2) Der Referentenentwurf der Verordnung hält sich recht genau an die gesetzlichen Vorgaben aus § 9c BSIG, weicht aber bei der Nennung der Normen und Standards in § 10 BSI-ITSiKV-E ab. So geht aus der Regelung in § 9c Abs. 3 BSIG eindeutig hervor, dass Normen, Standards und branchenabgestimmte IT-Sicherheitsvorgaben, bei denen die Standardisierung auch eine Rolle spielen kann, Vorrang vor den Technischen Richtlinien des BSI genießen. Ein solcher eindeutiger Vorrang wird in der gegenwärtigen Fassung von § 10 BSI-ITSiKV-E nicht wiedergegeben. **Um der Gesetzesvorlage zu entsprechen, bedarf es einer Angleichung, die den Vorrang von Normen gegenüber Technischen Richtlinien aufnimmt und so auch Rechtssicherheit für Unternehmen, Verbände und Verbraucher schafft.**

| **BSI-ITSiKV-E** | **Änderungsvorschlag** |
|---|---|
| § 7 Gegenstand der Herstellererklärung | § 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 | (1) Die Herstellererklärung enthält die Zusicherung, dass das Produkt für die nach § 8 festgelegte Dauer die für die einschlägige Produktkategorie geltenden IT-Sicherheitsanforderungen erfüllt. **Die IT-Sicherheitsanforderungen ergeben sich aus einer** |

| | |
|---|---|
| § 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. | **Norm oder einem Standard oder aus einer branchenabgestimmten IT-Sicherheitsvorgabe, sofern das Bundesamt diese nach § 10 Absatz 1 als geeignet anerkannt hat. Liegt keine Anerkennung nach § 10 Absatz 1 vor, ergeben sich die Sicherheitsanforderungen aus einer vom Bundesamt veröffentlichten Technischen Richtlinie, die die jeweilige Produktkategorie umfasst.** 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. |
| § 10 Anerkennung von Normen, Standards oder branchenabgestimmten IT-Sicherheitsvorgaben | § 10 Anerkennung von Normen, Standards oder branchenabgestimmten IT-Sicherheitsvorgaben<br><br>*[neuer Absatz 3]*<br>**(3) Bestehende Normen, Standards, und branchenabgestimmte IT-Sicherheitsvorgaben, deren Eignung nach Absatz 1 und Absatz 2 festgestellt wurde, sind bei der Konkretisierung der IT-Sicherheitsanforderungen für die einschlägigen Produktkategorien vorrangig zu behandeln.**<br><br>*[Absatz 3 wird Absatz 4]*<br>*[Absatz 4 wird Absatz 5]* |

(3) Ebenso ist die Berücksichtigung der (internationalen) Standardisierung bei der zentralen Festlegung der Produktkategorien und deren Sicherheitsanforderungen gemäß § 11 BSI-ITSiKV-E unzureichend. Festgestellt wird lediglich, dass für die konkreten Sicherheitsanforderungen auf Standards verwiesen werden kann, wobei diese im gleichen Rang zur Technischen Richtlinie stehen. Auch hier ist nicht ersichtlich, warum der gesetzlich grundlegend eingeräumte Vorrang internationaler Standardisierung zugunsten nationaler Alleingänge

– auch mit Blick auf die Zertifizierung nach EU Cybersecurity Act – entfallen sollte. **In der Formulierung ist daher der Normung und Standardisierung eine eindeutige Vorrangstellung gegenüber Technischen Richtlinien des BSI einzuräumen.**

| **BSI-ITSiKV-E** | **Änderungsvorschlag** |
|---|---|
| § 11 Produktkategorien<br><br>(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. | § 11 Produktkategorien<br><br>(2) Das Bundesamt **verweist** für die konkreten Sicherheitsanforderungen auf bestehende Vorgaben, **Normen,** Standards, **branchenabgestimmte IT-Sicherheitsvorgaben,** Technische Richtlinien **oder** Prüfgrundlagen und bemüht sich dabei um einen **größtmöglichen** Gleichlauf mit international **und europäisch** etablierten **Normen und** Standards. |

## Hintergrund

Durch kohärente internationale Normen haben deutsche Unternehmen Zugang zu Weltmärkten und gestalten diese mit. Der Weg zu europäischen und internationalen Standards führt über DIN und DKE.

Mit dem Normenvertrag von 1975 hat die Bundesrepublik Deutschland DIN als nationale Normungsorganisation und Vertreter Deutschlands in der europäischen und internationalen Normung anerkannt. Die Deutsche Normungsstrategie (2016) bekräftigt den Auftrag an DIN und DKE, als führende Moderationsplattformen Normungs- und Standardisierungsprozesse über die Grenzen der jeweils eigenen Organisation hinweg, auch für Foren und Konsortien, zu koordinieren. Gleichzeitig wird sichergestellt, dass das deutsche Normenwerk, bestehend aus internationalen, Europäischen und nationalen Normen, in sich kohärent und widerspruchsfrei ist. Die deutsche Wirtschaft baut auf dieses einheitliche Normenwerk, das ihr den Zugang zu Weltmärkten deutlich und nachhaltig erleichtert.

- Nationale technische Richtlinien, die außerhalb des bestehenden Normungs- und Standardisierungssystems erstellt werden, schaffen zusätzlichen Orientierungs- und Erfüllungsaufwand für Hersteller, Anwender und Verbraucher, führen zu höheren Kosten, begünstigen den Aufbau nicht-tarifärer Handelshemmnisse und wirken sich nachteilig auf die heimische Wirtschaft aus, da ihre Inhalte konträr zu europäischen und internationalen Normen und Standards sein können Die dadurch entstehenden Barrieren wirken einer europäischen Harmonisierung bei der Entwicklung von IT-Sicherheitsstandards im gemeinsamen europäischen Binnenmarkt entgegen.
- DIN und DKE bieten dem BSI zur Formulierung technischer Richtlinien den engen Schulterschluss an, um soweit möglich internationale bzw. europäische Lösungen anzustreben. Über DIN und DKE können Mitarbeiter des BSI die Erarbeitung kohärenter Normen und Standards anstoßen und in europäischen und internationalen Standardisierungsgremien mitwirken.

### Marktführerschaft in der Standardisierung für IT-Sicherheit

Im Bereich IT-Sicherheit hält Deutschland über DIN und DKE mit der Führung zentraler europäischer und internationaler Arbeitsgremien die Marktführerschaft in der IT-Sicherheits-Standardisierung – ein Standortvorteil, den es zu nutzen gilt. In diesen Gremien werden grundlegende Normen zur IT-Sicherheit gepflegt, beispielsweise die *DIN EN ISO/IEC 27000-Normenreihe für „Informationssicherheit-Managementsysteme“*, die *ISO/IEC 15408 „Evaluationskriterien für IT-Sicherheit"* oder die *Normenreihe IEC 62443 „Industrielle Kommunikationsnetze - IT-Sicherheit für Netze und Systeme“.* Diese internationalen Normen werden von deutschen Unternehmen erfolgreich angewendet. Die Konsolidierung der nationalen Meinung erfolgt im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA) und im DKE-Normungskomitee „IT-Sicherheit in der Automatisierungstechnik“.

- Die konstruktive Zusammenarbeit zwischen BSI, Wirtschaft, Wissenschaft und Forschung in bestehenden und künftigen Normungsgremien sollte fortgesetzt und ausgebaut werden.
- Ein Beispiel, wie dies gelingen kann, ist die Erarbeitung der *DIN SPEC 27072 „IoT-fähige Geräte - Mindestanforderungen zur Informationssicherheit“.* Der Standard richtet sich vor allem an Hersteller, Entwickler und Beschaffer entsprechender Produkte und kann als Grundlage zur Ausgestaltung des geplanten IT-Sicherheitskennzeichens genutzt werden.

- Ein weiteres Beispiel ist der Branchenspezifische Sicherheitsstandard (B3S) für Verkehrssteuerungs- und Leitsysteme im kommunalen Straßenverkehr (DIN VDE V 0832-700), der durch das BSI anerkannt wurde.
- Über DIN und DKE besteht die Möglichkeit, diese und ähnliche Inhalte in die europäische und internationale Normung einzubringen.

**Über DIN**

Das Deutsche Institut für Normung e. V. (DIN) ist die unabhängige Plattform für Normung und Standardisierung in Deutschland und weltweit. Gemeinsam mit Wirtschaft, Wissenschaft, öffentlicher Hand und Zivilgesellschaft trägt DIN wesentlich dazu bei, Zukunftsfelder zu erschließen. Als Mitgestalter des digitalen und grünen Wandels leistet DIN einen wichtigen Beitrag bei der Lösung der aktuellen Herausforderungen und ermöglicht, dass sich neue Technologien, Produkte und Verfahren am Markt und in der Gesellschaft etablieren. Rund 36.000 Experten aus Wirtschaft und Forschung, von Verbraucherseite und der öffentlichen Hand bringen ihr Fachwissen in den Normungsprozess ein, den DIN als privatwirtschaftlich organisierter Projektmanager steuert. Die Ergebnisse sind marktgerechte Normen und Standards, die den weltweiten Handel fördern und der Rationalisierung, der Qualitätssicherung, dem Schutz der Gesellschaft und Umwelt sowie der Sicherheit und Verständigung dienen. Weitere Informationen unter www.din.de.

**Über DKE**

Die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE ist die in Deutschland zuständige Organisation für die Erarbeitung von Standards, Normen und Sicherheitsbestimmungen in den Themenfeldern Elektrotechnik, Elektronik und Informationstechnik. Als deutsches Mitglied in den internationalen und europäischen Organisationen für die Normung der Elektro- und Telekommunikationstechnik – IEC, CENELEC und ETSI – vertritt die DKE die deutschen Interessen bei der Erarbeitung und Weiterentwicklung der Internationalen und Europäischen Normen zum Abbau von Handelshemmnissen und zur weltweiten Öffnung der Märkte.