

Stellungnahme

Entwurf einer Rechtsverordnung zum IT-Sicherheitskennzeichen des Bundesamtes für Sicherheit in der Informationstechnik

(Rechtsverordnung IT-Sicherheitskennzeichen – BSI-ITSiKV)

August 2021

Anlass und Ziel – Transparenz europäisch herstellen

Der ZVEI begrüßt, dass zunehmend Schritte unternommen werden, dafür zu sensibilisieren, dass Cybersicherheitsaspekte auch ein Qualitätsmerkmal eines Produktes sind. Die Herstellung von mehr Transparenz hinsichtlich der Frage der IT-Sicherheit von Produkten ist vor allem für Verbraucherinnen und Verbraucher ein wichtiges Vorhaben. Der zu wünschende vermehrte Einsatz von Produkten mit einem höheren Grad der Cybersicherheit dürfte sich dabei auch positiv auf das allgemeine Resilienzniveau auswirken.

Die Unternehmen der Elektroindustrie sind hier sowohl als Hersteller von qualitativ hochwertigen Produkten als auch Betreiber von (Produktionsanlagen-)Anlagen, die ebenfalls von einem höheren allgemeinen Resilienzniveau profitieren, betroffen.

Auch wenn man das IT-Sicherheitskennzeichen als wertvollen Testlauf sehen kann, so bleibt doch weiterhin fraglich, ob die Vorteile einer solchen nationalen Erprobung die zu erwartenden Nachteile aufwiegen. Zumindest stellt sich die Frage, nach der reibungslosen Einbettung des nationalen Kennzeichens in eine übergreifende europäische Lösung, sobald diese erarbeitet wurde. Aus Sicht der Mitgliedsunternehmen des ZVEI erfordert daher ein solcher nationaler „Testlauf“ ein schnelles Eintreten der verantwortlichen Ministerien und Behörden für eine zeitnahe europäische Adressierung. Es darf zu keinen Schwierigkeiten in der Umsetzung durch einen nationalen Alleingang kommen, vielmehr ist eine rasche Substituierung auf der europäischen Ebene notwendig.

Nach Ansicht des ZVEI folgt aus dem, durch das IT-Sicherheitskennzeichen gegeben, Anstoß der Auftrag, Überzeugungsarbeit für eine rasche europäische Adressierung zu leisten: Hierfür sollte das IT-Sicherheitskennzeichen schnellstmöglich in der Verbindung mit einer horizontalen europäischen Produktregulierung im NLF (New Legislative Framework) konsolidiert werden. Nur die rasche Einbettung in den etablierten Rahmen des Inverkehrbringens ermöglicht eine breite Umsetzung und beugt der Entwicklung ineffizienter Parallelstrukturen vor. Bereits eine horizontale Produktregulierung für Cybersicherheit im NLF würde zur Erlangung der CE-Kennzeichnung Informations- und Transparenzpflichten bzw. eine entsprechend Nutzerinformation erfordern. Ob darüberhinausgehende europäische Kennzeichnungssysteme einen Mehrwert bieten, müsste in der weiteren Umsetzung betrachtet werden.

Zur praktischen Umsetzung – auf Erfahrungen zurückgreifen

Erfahrungen mit „Siegel“ und Kennzeichen in anderen Kontexten zeigen, dass viele Herausforderungen oftmals besonders in der direkten Umsetzung zu finden sind bzw. dort auftreten. Häufig sind es Detailspekte, welche unbeachtet zu Problemen führen können. Der ZVEI empfiehlt aus dieser Erfahrung, dass sich bei der Ausgestaltung der Umsetzungsanforderungen des IT-Sicherheitskennzeichens an anderen etablierten Kennzeichnungen orientiert werden sollte. Hier existiert ein umfangreicher Erfahrungsschatz, auch hinsichtlich von Festlegungen zur direkten Umsetzung und praktischen Fragen, welcher genutzt werden sollte.

Zusätzlich muss gewährleistet und kommuniziert werden, dass das IT-Sicherheitskennzeichen keine geeignete Informationsquelle für höhere bzw. komplexere Cybersicherheitsanforderungen ist, wie sie in KRITIS-Betrieben sowie multinationalen und den meisten mittelständischen Unternehmen erfüllt werden müssen. Das IT-Sicherheitskennzeichen sollte höherwertige Prüfbescheinigungen weder schwächen noch entwerten.

Zusätzlich besteht nach Ansicht des ZVEI zu folgenden Aspekten noch Klärungsbedarf:

zu § 3

Gestaltung des Etiketts und der Website zum IT-Sicherheitskennzeichen

Hinsichtlich § 3 existiert vor allem Klärungsbedarf zum Umfang der weiteren Informationen, diese sollten verhältnismäßig und Rezipienten gerecht sein. Außerdem sollte für Hersteller ein schneller und einfacher Weg eingerichtet werden, welcher es erlaubt „aktuelle Sicherheitsinformationen“ zur Verfügung zu stellen und diese bei Bedarf zu aktualisieren.

zu § 6

Vereinfachtes Verfahren

Der ZVEI begrüßt das Vorliegen eines vereinfachten Verfahrens, besonders angesichts einer raschen Konsolidierung auf der europäischen Ebene sind Anknüpfungspunkte an einheitliche europäische Verfahren bzw. Regelungen sehr wichtig.

zu § 9

Verwendung des Sicherheitskennzeichens

Besonders hinsichtlich § 9 „Verwendung des Sicherheitskennzeichens“ stellen sich in der praktischen Umsetzung Fragen: So besteht zum einen zur Verwendung des Kennzeichens im Werbekontext Klärungsbedarf: Es ist z. B. unklar, wie der Verweis auf die zugehörige Website bei Bild- und Ton-Medien zu erfolgen hat, ist hier z. B. ein Medienbruch zulässig bzw. wie hat der Hinweis prinzipiell bei Bild- und Ton-Medien zu erfolgen?

Zum anderen muss rechtssicher aufgezeigt werden, wie im Detail mit bereits produzierter und verpackter Ware beim Erlöschen der Rechte von Hersteller und Verkäufer zu verfahren ist. Nach der aktuellen Formulierung könnte davon ausgegangen werden, dass Lagerware in diesem Fall noch restlos abverkauft werden könnte, auch wenn die Verpackung mit dem produktspezifischen Etikett versehen ist, solange es sich dabei um Ware handelt, die vor dem Erlöschen des Kennzeichens produziert wurde. Hier wäre eine weitere Klärung von Verkaufsfristen bzw. der Gestattung des restlosen Abverkaufs sinnvoll. Auch in dieser Frage sieht der ZVEI es als zielführend an, sich ein Beispiel an etablierten Kennzeichen nehmen, bei denen diese Aspekte, z. B. wie Verbraucherhinweise funktionieren sollten, gut gelöst werden.

zu § 10

Anerkennung von Normen, Standards oder branchenabgestimmten IT-Sicherheitsvorgaben

Der ZVEI erachtet den Bezug auf internationale Normen und Standards als sehr wichtig. Angesichts der Notwendigkeit einer raschen europäischen Adressierung und einer schnellen europäischen Umsetzung, würde eine stärkere Einbringung des BSI in die internationale Normung mittel- bis langfristig einen großen Beitrag leisten. Zumal auf diese Weise Erfahrungen, die mit dem IT-Sicherheitskennzeichen gewonnen werden, auch international anschlussfähig für die europäische Adressierung genutzt werden könnten.

Weiterer Klärungsbedarf besteht in der Frage, warum die Überführung in eine Technische Richtlinie zum Widerruf führen kann? Hinzu kommt, dass die Möglichkeit der Überführung in Technische Richtlinien auch Fragen hinsichtlich der Versionspflege bei erfolgter Überführung aufwerfen kann – besonders, wenn die Anzahl der betrachteten Produktkategorien deutlich zunehmen würde. Es wäre hier von Interesse, dass die angenommenen Vorteile einer solchen Überführung erläutert würden.

zu § 11

Produktkategorien

Hinsichtlich der Definition der Produktkategorien erachtet der ZVEI eine stärkere Einbindung der jeweilig betroffenen Hersteller als zielführend an. Zumindest sollte, ähnlich der Regelung in § 10 Abs. (2) zu den Branchenstandards, ein Vorschlagsrecht etabliert werden. Zugleich empfiehlt der ZVEI das Heranziehen von etablierten Kategorisierungen aus einschlägigen internationalen Normen und Standards.

zu § 13

Informationen für Verbraucher

Neben den in der ITSiKV referenzierten Informationen, sollte die, zu dem Produkt gehörende, Website des Bundesamtes auch dazu genutzt werden, über die Umsetzung von Cybersicherheit beim Betrieb eines Produktes zu informieren. So könnte neben der Darlegung von Cybersicherheitsmerkmalen auch eine entsprechende Aufklärung über den cybersicheren Betrieb erfolgen, schließlich kann Cybersicherheit nur durch die Übernahme geteilter Verantwortung adäquat adressiert werden.

zu § 14

Evaluierung

Der ZVEI begrüßt, dass von Beginn an eine Evaluierung vorgesehen wird, sieht die Beteiligung der Industrie bei dieser Evaluierung jedoch als notwendig und zielführend an.

zu § 15

Inkrafttreten

Zum Zeitpunkt des Inkrafttretens müssen den Herstellern alle Details bekannt sein, die eine rechtssichere Nutzung des IT-Sicherheitskennzeichens erlauben.

Herausgeber:

ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e.V.
Innovationspolitik

Lyoner Str. 9
60528 Frankfurt am Main

Verantwortlich:
Marcel Hug
Telefon: +49 69 6302-432
E-Mail: Marcel.Hug@zvei.org

www.zvei.org

August 2021

Über den ZVEI

Der **ZVEI** - Zentralverband Elektrotechnik- und Elektronikindustrie e.V. vertritt die gemeinsamen Interessen der Elektroindustrie und der zugehörigen Dienstleistungsunternehmen in Deutschland und auf internationaler Ebene. Die Branche beschäftigt rund 873.000 Arbeitnehmer im Inland und 790.000 im Ausland. 2020 lag ihr Umsatz bei rund 180 Milliarden Euro. Ein Fünftel aller privaten F+E-Aufwendungen in Deutschland kommen von der Elektroindustrie. Jährlich wendet die Branche rund 20 Milliarden Euro auf für F+E und mehr als sechs Milliarden Euro für Investitionen. Ein Drittel des Branchenumsatzes entfallen auf Produktneuheiten. Jede dritte Neuerung im Verarbeitenden Gewerbe insgesamt erfährt ihren originären Anstoß aus der Elektroindustrie.