VERBAND DER INTERNETWIRTSCHAFT E.V.

Stellungnahme zum Referentenentwurf Bundesministerium des Innern, für Bau und Heimat für eine Rechtsverordnung zum IT-Sicherheitskennzeichen des Bundesamtes für Sicherheit in der Informationstechnik (Rechtsverordnung IT-Sicherheitskennzeichen – BSI-ITSiKV)

Berlin, 19. August 2021

Mit dem am 27. Mai veröffentlichten zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG 2.0) wurde für das Bundesministerium des Innern, für Bau und Heimat (BMI) eine Grundlage für eine Verordnung geschaffen, mit der ein IT-Sicherheitskennzeichen eingeführt werden soll. Mit dem nunmehr vorgelegten Entwurf der Rechtsverordnung für ein IT-Sicherheitskennzeichen (BSI-ITSiKV) wird die Einführung, Pflege und Vergabe des Kennzeichens genauer geregelt.

eco hatte im Rahmen verschiedener Diskussionen insbesondere auch im Kontext zur europäischen NIS-2 Richtlinie darauf hingewiesen, dass Gütesiegel oder Sicherheitskennzeichen einen sinnvollen Beitrag zur Transparenz über das IT-Sicherheitsniveau von Produkten und Diensten leisten können, sofern sie nicht zu ambitioniert angegangen werden. Dabei muss auch berücksichtigt werden, dass IT-Sicherheitskennzeichen einen Mehrwert für und Nutzer:innen bieten können, zugleich aber auch sichergestellt sein muss, dass eine entsprechende Kennzeichnung von Produkten kein falsches Gefühl von Sicherheit vermitteln darf. Die nunmehr vorliegenden BSI-ITSiKV greift zahlreiche Fragen diesbezüglich auf und bietet eine grundsätzlich solide Grundlage für die Vergabe eines IT-Sicherheitskennzeichens. Im Rahmen der weiteren Diskussion des vorliegenden Entwurfs und die Einführung von IT-Sicherheitskennzeichens sollten die damit verbundenen Fragestellungen berücksichtigt, einzelne Regelungen präzisiert sowie weiter klargestellt werden.

Diese möchte eco nachfolgend aufzeigen und nimmt die Gelegenheit gerne wahr zu dem vorliegenden Verordnungsentwurf Stellung zu nehmen.

- **Zu § 2: Begriffsbestimmungen**

Der § 2 (4) sieht vor, dass den Vorgaben des IT-Sicherheitsgesetzes folgend auch so genannte „branchenabgestimmte IT-Sicherheitsvorgaben“ verwendet werden können. Das IT-SiG 2.0 führt dazu weiter aus, dass diese neben Normen und Standards herangezogen werden können. Unklar bleibt allerdings, welche Voraussetzungen und Maßgaben branchenabgestimmte IT-Sicherheitsvorgaben erfüllen müssen, damit diese im Rahmen der IT-

Sicherheitskennzeichens berücksichtigt und herangezogen werden. Hier wäre es aus Sicht des eco hilfreich, wenn näher erläutert werden könnte, welche Voraussetzungen und Maßgaben für branchenabgestimmte Sicherheitsvorgaben erfüllt werden müssten.

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

Grundlage für das Vertrauen in das geplante IT-Sicherheitskennzeichen sind Transparenz und angemessene Vermittlung von Informationen. Die Bemühungen der Darstellung eines entsprechenden Etiketts auf den jeweiligen Produkten bzw. Diensten ist nachvollziehbar. Unklar ist allerdings, wie das jeweilige Etikett mit den entsprechenden Produkten verbunden werden soll. Konkret steht zur Debatte, inwieweit sich durch die Ausstellung eines Gütesiegels eine Verpflichtung zum Aufdruck oder zur Integration desselben in die Produktpräsentation ergibt. Entsprechende Auflagen könnten sich als problematisch erweisen, wenn dadurch in größerem Umfang Verpflichtungen zur Umgestaltung von Verpackungen entstehen. Nicht zuletzt ist auch darauf hinzuweisen, dass die Bereitstellung eines Gütesiegels insbesondere bei Weißer Ware und Endgeräten für Hersteller problematisch sein könnte, wenn entsprechende Geräte weiterverkauft werden (Reseller). Eine Verpflichtung des Herstellers zur Bereitstellung eines solchen Gütesiegels sollte daher vermieden werden.

Bei § 3 (4) stellt sich darüber hinaus die Frage, inwieweit das BSI nicht nur Angaben zum Umfang der Einhaltung von Erklärungen veröffentlichen kann, sondern umgekehrt auch Angaben darüber, in welchem Umfang ein Anbieter oder Betreiber dagegen verstößt bzw. verstoßen hat. Mit einem solchen Verfahren könnte Blacklisting begünstigt werden, weswegen eco davon abrät.

- **Zu § 5: Antragsprüfung**

In § 5 (3) werden branchenabgestimmte Sicherheitsstandards gem. § 2 (4) und unter Verweis auf § 10 mit allgemeinen Normen und Standards unter dem Oberbegriff der branchenabgestimmten Sicherheitsstandards zusammengefasst. Aus Gründen der besseren Verständlichkeit und aufgrund deren zentraler Bedeutung für die bisherige Kontrolle und Gestaltung von IT-Sicherheit plädiert eco dafür, an in § 5 (3) neben den branchenabgestimmten IT-Sicherheitsvorgaben auch Normen und Standards explizit aufzuführen. Damit sollte klargestellt sein, dass diese gleichrangig neben den branchenabgestimmten IT-Sicherheitsvorgaben Grundlage für die Vergabe eines Sicherheitskennzeichen herangezogen werden können.

Zudem wäre es zu erwägen, dass das BSI über die Plausibilitätsprüfung eingereichter Unterlagen hinaus auch die zu zertifizierenden Produkte genauer überprüfen kann. Dies ist durch die Möglichkeit, Testkäufe durchführen zu dürfen bereits angelegt. Damit eine kurze Antragsbearbeitungszeit gewährleistet ist, wird zwar in der Regel zunächst nur eine Plausibilitätsprüfung stattfinden können. Dies sollte in einem ersten Schritt auch ausreichen. Um das Vertrauen der Verbraucher in die Aussagekraft des IT-Sicherheitskennzeichnen zu fördern, sollte das BSI jedoch auch die Möglichkeit haben, über die Plausibilitätsprüfung hinaus im Bedarfsfall Sachprüfungen durchzuführen.

- **Zu § 8: Laufzeit des IT-Sicherheitskennzeichens und Erlöschen**

Die Regelungen zur Vergabe und Laufzeit des IT-Sicherheitskennzeichens sehen vor, dass eine Verlängerung des Kennzeichens verweigert werden kann, wenn es nicht auf einer gültigen Prüfgrundlage erneuert wird (vgl. § 8 (3) Satz 1). Dies wirft in der praktischen Handhabung die Fragestellung wie die Erneuerung eines Gütesiegels ausgestaltet wird, welche Anforderungen an die Verlängerung gestellt werden und welche Abläufe vorgesehen sind. Nach Ansicht des eco wäre eine Konkretisierung und klarere Regelungen über die Erneuerung von Sicherheitskennzeichen sinnvoll.

Darüber hinaus wirft der § 8 (1) zur Laufzeit von Sicherheitskennzeichen die Frage auf, welche Grundlagen neben Standards, Normen und branchenabgestimmten IT-Sicherheitsvorgaben noch relevant sein könnten, da hier zusätzlich noch Technische Richtlinien angeführt werden. Auch hier wäre eine detaillierte Angabe und Bezugnahme im Rahmen der ITSiKV wünschenswert.

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

Nach Ansicht des eco wäre es grundsätzlich sinnvoll, wenn die in Bezug genommen Normen, Standards und branchenabgestimmten IT-Sicherheitsvorgaben in einer Liste oder Anlage zur Verordnung konkret benannt und aufgeführt werden. Dies schafft Transparenz und Orientierung. Nicht zuletzt wird damit auch Klarheit über die verschiedenen anwendbaren Vorgaben geschaffen, wenn die möglichen Standards oder Normen, gegen die ein entsprechendes IT-Sicherheitskennzeichen zertifiziert werden kann, benannt sind.

- **Zu § 11: Produktkategorien**

Im Rahmen der Diskussion um die sogenannte TR-Router des Bundesamts für Sicherheit in der Informationstechnik hat eco die strikte Abgrenzung verschiedener Produktkategorien voneinander bei vernetzten Geräten als wenig sinnvoll und zeitgemäß kritisiert. eco plädiert dafür, generelle Regelungen heranzuziehen und nur dort, wo es notwendig und aufgrund des Einsatzszenarios sinnvoll und nachvollziehbar ist, Produktkategorien näher zu definieren. Darüber hinaus wäre wünschenswert, wenn das BSI eine Whitelist von Standards, Normen, Technischen Richtlinien und branchenspezifischen IT-Sicherheitsvorschriften in Form einer Anlage oder einer Ergänzung der Verordnung veröffentlichen würde. Bei Konformität mit den entsprechenden Vorgaben sollten die Voraussetzungen des IT-Sicherheitskennzeichens erfüllt sein und ein entsprechendes Gütesiegel vergeben werden. Dieser Ansatz dürfte auch im Interesse des BSI sein, denn es würde die Prüfung und Vergabe vereinfachen und das Verfahren zur Plausibilitätsprüfung effizienter ausgestalten.

- **Zu § 12: Aufsicht**

eco würde es begrüßen, wenn das Marktüberwachungskonzept, das gem. § 12 (2) erstellt werden soll, näher beschrieben werden könnte, um hierzu eine valide Einschätzung abgeben zu können. Für eine effektive Überprüfung der Sicherheit der gekennzeichneten Produkte wäre zudem neben der Möglichkeit von Testkäufen eine Sachprüfung durch das Bundesamt sinnvoll. Nur bei einer entsprechenden Befugnis des Bundesamtes wäre sichergestellt, dass in das Marktüberwachungskonzept Regelungen zur Sachprüfung aufgenommen werden können.

Fazit:

Mit der BSI-ITSiKV hat das BMI eine grundsätzlich solide Grundlage für die Vergabe des IT-Sicherheitskennzeichens geschaffen.

Damit das IT-Sicherheitskennzeichen des BSI im Markt erfolgreich sein kann, muss es Informationen verständlich und transparent vermitteln. Es sollte keine nicht erfüllbaren Sicherheitsversprechen abgeben, sondern vielmehr einen Mehrwert bieten und einen praktikablen Rahmen setzen. Auch sollte es darauf abheben, dass Produkte mit bestimmten Standards kompatibel sind.

Im Rahmen der weiteren Diskussion des vorliegenden Entwurfs und der Einführung des IT-Sicherheitskennzeichens sollten allerdings einige Fragestellungen berücksichtigt, sowie einzelne Regelungen präzisiert und weiter klargestellt werden.

Dazu gehört insbesondere der Abgleich von Standards, Normen und technischen Richtlinien und deren Bedeutung für die Vergabe des Kennzeichens. eco begrüßt, dass das BMI den Vorgaben des IT-SiG 2.0 gefolgt ist und branchenabgestimmte Sicherheitsstandards als mögliche Grundlage zur Vergabe von IT-Sicherheitskennzeichen heranzieht. Aus der Sicht der Internetwirtschaft wäre allerdings mehr Klarheit und Transparenz für alle Beteiligten hilfreich. Dies könnte durch eine Ergänzung der Verordnung oder auch in Form einer Anlage erreicht werden. Darin sollten die Standards, Normen, Technischen Richtlinien und branchenabgestimmten IT-Sicherheitsvorgaben angeführt werden, die als Grundlage für die Konformitätserklärung herangezogen werden können, um das IT-Sicherheitskennzeichen zu erhalten.

Auch sollte bei der Gestaltung darauf geachtet werden, dass entsprechende weitere Zertifizierungen wie bspw. die durch die im Rahmen der NIS-2.0 Richtlinie vorgesehenen Regelungen zur Zertifizierung und Standardisierung (vgl. Artikel 21 und 22) mit einbezogen und berücksichtigt werden.

Zudem wäre es zu erwägen, dass dem BSI auch die die Befugnis eingeräumt wird, bei zertifizierten oder zu zertifizierenden Produkten über die Plausibilitätsprüfung hinaus im Bedarfsfall auch Sachprüfungen durchführen zu können. Dies würde die Aussagekraft des IT-Sicherheitskennzeichens stärken und auch das Vertrauen der Verbraucher in ein entsprechendes Gütesiegel.

Über eco

Mit über 1.100 Mitgliedsunternehmen ist eco der größte Verband der Internetwirtschaft in Europa. Seit 1995 gestaltet eco maßgeblich das Internet, fördert neue Technologien, schafft Rahmenbedingungen und vertritt die Interessen seiner Mitglieder gegenüber der Politik und in internationalen Gremien. Die Zuverlässigkeit und Stärkung der digitalen Infrastruktur, IT-Sicherheit und Vertrauen sowie eine ethisch orientierte Digitalisierung bilden Schwerpunkte der Verbandsarbeit. eco setzt sich für ein freies, technikneutrales und leistungsstarkes Internet ein.