

# Stellungnahme zum IT-Sicherheitskennzeichen

## Kommentierung des Referentenentwurfes vom 27.07.2021

Mit Schreiben vom 27. Juli 2021 hat das Bundesministerium des Innern, für Bau und Heimat (BMI) den Referentenentwurf zur Rechtsverordnung zum IT-Sicherheitskennzeichen des Bundesamtes für Sicherheit in der Informationstechnik (BSI-ITSiKV) zur Kommentierung gestellt. In dem Anschreiben wird darauf verwiesen, dass dieser Entwurf innerhalb der Bundesregierung noch nicht abgestimmt ist. Der TÜV-Verband bedankt sich für die Gelegenheit zur Stellungnahme und begrüßt die Kommentierungsfrist bis zum 20. August.

Sehr gern ergreift der TÜV-Verband die Möglichkeit zur Kommentierung und bittet um Berücksichtigung nachfolgender Aspekte:

## IT-Sicherheit als europäisches Anliegen

Als TÜV-Verband sehen wir die Notwendigkeit und setzen uns dafür ein, die IT-Sicherheit in der EU zu stärken, einen Digitalen Binnenmarkt zu schaffen und IT-Sicherheit von Produkten für den Verbraucher transparent zu machen, um ihn in seiner Kaufentscheidung zu unterstützen. Ein europäischer Ansatz ist allerdings zu bevorzugen. Dieser nationale Alleingang eines auf einer Herstellererklärung basierten Kennzeichens sollte lediglich eine Brücke hin zu einem europäischen Sicherheitszeichen darstellen, das auf der Prüfung der Geräte durch unabhängige Dritte basiert. Die deutsche Bundesregierung sollte sich daher in Brüssel für ein Europäisches IT-Sicherheitszeichen einsetzen. Nur ein europaweit harmonisiertes und flächendeckend einheitlich eingeführtes, leicht verständliches und mit einer wirkungsvollen Marktaufsicht umgesetztes IT-Sicherheitszeichen kann einen wirklichen Beitrag zur Stärkung der Cyberresilienz Europas und damit Deutschlands leisten. Der „Cybersecurity Act“ stellt hierfür den passenden Regulierungsrahmen. Ein EU-Sicherheitszeichen sollte darauf basieren und dem Markt und Verbrauchern die Konformität mit den Anforderungen aus den Schemes des Cybersecurity Acts anzeigen.

## Wichtige Details jetzt klären

Der vorgelegte Referentenentwurf lässt zu viele Regelungsmöglichkeiten ungenutzt, bzw. verweist auf eine spätere Ausgestaltung durch das BSI. Damit bleiben entscheidende Fragen zunächst offen, deren

Ausgestaltung vor Einführung eines IT-Sicherheitskennzeichens als dringend notwendig erachtet wird. Dies betrifft die grafische Ausgestaltung des IT-Sicherheitskennzeichens, die Kriterien zur Festlegung von zugehörigen Produktkategorien sowie das Überwachungskonzept zur Umsetzung der Marktaufsicht. Diese und andere Fragen sollten durch die Rechtsverordnung geklärt und festgelegt werden und nicht zu einem späteren Zeitpunkt ohne Anhörung beteiligter Kreise in alleiniger Zuständigkeit durch das BSI.

## §2 Begriffsbestimmungen

Der fünfte Aufzählungspunkt benennt „geeignete oder qualifizierte Dritte“. Der TÜV-Verband regt an, die genannte Anforderung mit einem „und“ zu verknüpfen. In der Regel wird das Kriterium der Eignung auch durch eine angemessene Qualifikation nachgewiesen. Unklar bleibt hierbei ebenfalls, welche Qualifikationen erwartet werden und wann ein Dritter im Sinne der Definition als „geeignet“ bezeichnet werden kann.

## §5 Antragsprüfung

Absatz eins sieht eine „Plausibilitätsprüfung“ der eingereichten Unterlagen durch den Hersteller vor. Der Verband begrüßt die Möglichkeit von optionalen Prüfungen im Rahmen von Testkäufen (§12), die Produkte sollten jedoch bereits bevor sie in den Markt gebracht werden grundsätzlich einer tiefergehenden Prüfung durch unabhängige Dritte unterzogen werden. Somit lassen sich mögliche Sicherheitsrisiken bereits erkennen, bevor die Produkte im Einsatz sind.

## §6 Vereinfachtes Verfahren

Absatz zwei beschreibt die Möglichkeit zur Anerkennung eines bereits vorhandenen ausländischen staatlichen Kennzeichens „auf Grundlage des gleichen oder vergleichbaren Prüfstandards (...)“. Aus Sicht des TÜV-Verbandes ist nicht nachvollziehbar, warum die Anerkennung vorhandener Kennzeichen sich nur auf staatlich vergebene Kennzeichen bezieht. Die Unterscheidung zwischen staatlicher Stelle und privatwirtschaftlicher Prüforganisation erscheint als nicht sachgerecht.

Weiterhin ist aus Sicht des Verbandes nicht erkennbar, warum die Anerkennung ausschließlich ausländische Kennzeichen adressiert. Auch nationale Zertifizierungen von staatlichen und nicht-staatlichen Prüfstellen sollten als Nachweis zur Erfüllung der Anforderungen herangezogen werden können.

Grundlage einer Anerkennung sollten Qualitätskriterien und Anforderungen an die Prüfstelle sein sowie

die dem Kennzeichen zugrundeliegenden Normen. Dem Hersteller sollte die Möglichkeit eingeräumt werden, den Nachweis der Konformität zu den Anforderungen des BSI auch durch am Markt etablierte abdeckende Prüfungen zu erbringen (z. B. durch TR 03148 – Sichere Breitbandrouter).

## §9 Verwendung des IT-Sicherheitskennzeichens

Abschnitt 4 sieht vor, dass „keine nach dem Erlöschen hergestellten Produkte mehr mit dem Etikett auf den Markt gebracht werden“ dürfen. Der Zeitpunkt der Herstellung eines Produktes stellt kein angemessenes Kriterium dar, um zu verhindern, dass auch potentiell unsichere Produkte in den Markt gelangen. Aus Sicht des TÜV-Verbands ist es erforderlich, hier den Zeitpunkt des Entzugs des IT-Sicherheitskennzeichens als maßgeblich anzusehen. Nur so ist sichergestellt, dass die ursprüngliche Intention, sicherere Produkte in den Markt zu bringen, gewährleistet ist.

## §12 Aufsicht

Der Entwurf sieht eine anlassbezogene und reaktive Aufsicht über die Produkte der Hersteller vor. Vor dem Hintergrund, dass bei der Vergabe des IT-Sicherheitskennzeichens keine Prüfung durch unabhängige Dritte erfolgt und auch das BSI die eingereichten Unterlagen nur einer Plausibilitätsprüfung unterzieht (siehe §5 (1)), erscheint dieses Vorgehen der Bedeutung der IT-Sicherheit von Produkten in Hinblick auf den Verbraucherschutz als nicht angemessen. Der TÜV-Verband begrüßt deshalb auch die anlasslosen Maßnahmen zur Marktüberwachung, wie sie unter (2) vorgesehen sind.

## Autor und Ansprechpartner



### Marc Fliehe

Bereichsleiter Digitalisierung und IT-Sicherheit

E-Mail: [marc.fliehe@vdtuev.de](mailto:marc.fliehe@vdtuev.de)

Tel. +49 30 760095 460

[www.tuev-verband.de](http://www.tuev-verband.de)

Der Verband der TÜV e. V. (VdTÜV) vertritt die politischen und fachlichen Interessen seiner Mitglieder gegenüber Politik, Verwaltung, Wirtschaft und Öffentlichkeit. Der Verband setzt sich für technische und digitale Sicherheit bei Produkten, Anlagen und Dienstleistungen durch unabhängige Prüfungen und qualifizierte Weiterbildung ein. Mit seinen Mitgliedern verfolgt der TÜV-Verband das Ziel, das hohe Niveau der technischen Sicherheit in unserer Gesellschaft zu wahren und Vertrauen für die digitale Welt zu schaffen.