Stellungnahme zum Entwurf einer Rechtsverordnung zum IT-Sicherheitskennzeichen

16. August 2021

Vorbemerkungen

Mit dem IT-Sicherheitsgesetz 2.0 hat das BSI den Auftrag erhalten, ein freiwilliges IT-Sicherheitskennzeichen einzuführen. Mitte Juli wurde bereits die Infoseite zum IT-Sicherheitskennzeichen freigeschaltet und Breitbandrouter (auf Basis BSI TR-03148) sowie E-Mail-Dienste (auf Basis BSI TR-03108) als die ersten beiden für das IT-Sicherheitskennzeichen relevanten Produktkategorien benannt. Die Antragsstellung soll ab Ende 2021 möglich sein.

Zur künftigen Handhabung und weiteren Ausgestaltung des freiwilligen IT-Sicherheitskennzeichens im Sinne des § 9c Absatz 1 Satz 1 des BSI-Gesetzes wurde am 16. Juli 2021 der Entwurf einer Rechtsverordnung zum IT-Sicherheitskennzeichen an die Wirtschaftsverbände übermittelt.

Bitkom bedankt sich für die Beteiligungs- und Kommentierungsmöglichkeit und nimmt diese gerne wahr. Die Digitalwirtschaft steht dem IT-Sicherheitskennzeichen positiv und offen gegenüber und begrüßt ausdrücklich die strukturierte Einbeziehung der Wirtschaft. Transparenz in der IT-Sicherheit als notwendigen Baustein der Vertrauensbildung unterstützen wir ausdrücklich. Bitkom hofft, dass das angedachte IT-Sicherheitskennzeichen positiv im Endkundengeschäft aufgenommen wird und dazu beiträgt, dass das Sicherheitsbewusstsein der Verbraucherinnen und Verbraucher steigt.

Gleichwohl darf nicht vergessen werden, dass ein IT-Sicherheitskennzeichen nur als ein Mosaikstein eines umfassenden Gesamtkonzepts für mehr IT-Sicherheit zu verstehen ist. Damit das Kennzeichen seine volle Wirkung entfalten kann, muss es zudem von vornherein europäisch skalierbar konzipiert werden. Deshalb sollte das IT-Sicherheitskennzeichen vor allem auf anerkannte internationale, zumindest aber europäisch einheitliche Regelungen, Normen und Standards referenzieren, um die Anschlussfähigkeit an die europäische Ebene zu gewährleisten. Bitkom spricht sich für ein EU-weit gültiges, einheitliches, leicht verständliches und mit einer effizienten Marktaufsicht umgesetztes IT-Sicherheitskennzeichen aus, das auf Basis des EU Cybersecurity Acts sowie horizontalen, NLF-basierten Cybersicherheitsanforderungen eingeführt wird. Im Idealfall wird das deutsche IT-Sicherheitskennzeichen zum künftigen EU-Kennzeichen. Aber, wie auch immer ein künftiges EU-Kennzeichen ausgestaltet wird, es darf keine Co-Existenz eines deutschen und europäischen IT-Sicherheitskennzeichens geben.

Bitkom
Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.

Sebastian Artz
Bereichsleiter Cyber- & Informationssicherheit
T +49 151 27631-531
E-Mail s.artz@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Achim Berg

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Vor diesem Hintergrund und aufbauend auf dem Bitkom Positionspapier zum IT-Sicherheitskennzeichen aus dem April 2019 möchte sich Bitkom mit den nachfolgenden Anmerkungen und Kommentaren weiter konstruktiv in die Debatte einbringen und auf ein möglichst sicherheitssteigerndes und praxistaugliches IT-Sicherheitskennzeichen hinwirken. Mit Blick auf die einzelnen Produktkategorien stehen wir auch in Zukunft für den gemeinsamen Austausch mit den Fachexpertinnen und -experten des BSI gerne zur Verfügung.

Detailbetrachtung

§ 2 Begriffsbestimmungen

Gesetzestextübergreifend sind die Begriffsbestimmungen einheitlich zu halten, um Missverständnisse und Rechtsunsicherheit zu vermeiden. Im vorliegenden Verordnungsentwurf gilt dies insb. für die Definition von Herstellern. Als „Hersteller" sollten auch jene Unternehmen erfasst werden, die Produkte herstellen lassen und diese auf dem deutschen Markt bereitstellen. Es sollten damit auch „Produktentwickeler" als „Hersteller" auftreten können, wenn sie das Produkt durch „Auftragsfertiger", z.B. in Asien, fertigen lassen. Zudem gibt es Unternehmen, die international tätige Herstellende als Bevollmächtigte in Deutschland vertreten. Diese Vertretung sollte auch in der Lage sein, als „Hersteller" gegenüber dem BSI aufzutreten. Nicht zuletzt sollte das gesamte System auch offen gegenüber Unternehmen sein, die in einem anderen Land der europäischen Union tätig sind, um die zukünftige Anschlussfähigkeit für ein europäisches IT-Sicherheitskennzeichen sicherzustellen.

Der angeführte Branchenbegriff wirkt im Digitalzeitalter nicht wirklich zeitgemäß, da eine Vielzahl von Produkten und Dienstleistungen nicht mehr einer Branche zugerechnet werden kann. Damit stellt sich die Frage nach den Beteiligungsmöglichkeiten bei der Abstimmung branchenabgestimmter IT-Sicherheitsvorgaben. Zudem bedarf die Bezugnahme auf den „Geltungsbereich dieses Gesetzes" Klärung – wie, bzw. was genau, ist der Geltungsbereich?

Bei der Bestimmung von „geeigneten oder qualifizierten Dritten" wäre ein Verweis auf das gemäß BSI-Gesetz geltende Begriffsverständnis hilfreich. Darüber hinaus bleiben im vorliegenden Entwurf einige Fragen bzgl. der vorgesehenen Marktüberwachung offen. Es wäre wünschenswert, wenn das Zusammenwirken von BSI und qualifizierten Dritten näher spezifiziert werden würde.

§ 3 Gestaltung des Etiketts und Website zum IT-Sicherheitskennzeichen

Bitkom begrüßt den Ansatz des IT-Sicherheitskennzeichens, die Herstellererklärung und die Sicherheitsinformation nach § 9c Abs. 2 BSIG mit einem Verweis auf die BSI-Homepage zu verknüpfen. Allerdings handelt es sich bei kleinen Geräten (z.B. USB-Sticks, SD-Karten) und der Vorgabe, einen QR-Code und die Nennung des BSI abzubilden, durchaus um eine Herausforderung in der Praxis, die es mitzudenken gilt. Zudem regt Bitkom an, darüber nachzudenken, ob eine Verlinkung des QR-Codes auf eine entsprechende Rubrik der Website des Herstellers nicht zielführender wäre, um dem angestrebten EU-weiten Ansatz besser Rechnung zu tragen. Dadurch müssten in Zukunft keine verschiedenen nationalen Datenbanken zusammengeführt werden. In jedem Fall muss die länderübergreifende Kompatibilität entsprechender Datenbanken bereits vorab mitgedacht werden. Fehlende Kompatibilität verschiedener nationaler Handhabungen darf kein Hindernis für die Skalierung eines EU-weit einheitlichen Ansatzes sein.

Gemäß § 3 Absatz 4 kann *„das Bundesamt zudem weitere Informationen über sicherheitsrelevante IT-Eigenschaften und darüber, ob und inwieweit die Herstellererklärung nach derzeitiger Kenntnis eingehalten wird, einstellen."* Es stellt sich die Frage, ob dies auch für den negativen Fall gilt, d.h. falls ein Kennzeichen abgelehnt wird. Ferner stellt sich die Frage, ob auch aktuelle Infos z.B. zu Sicherheitslücken einfließen werden.

Neben der „Herstellererklärung", dem QR-Code, der BSI-Information sowie dem Link zur BSI-Website sollte zusätzlich das „Verfallsdatum" des IT-Sicherheitskennzeichen so integriert werden, dass eine reibungslose und mit möglichst geringem Aufwand verbundene Verlängerung der Laufzeit des Kennzeichens sichergestellt wird. Unternehmen sollten die Möglichkeit haben, die Laufzeit für Produkte, die länger als zwei Jahre auf dem Markt angeboten werden, mittels eines schlanken, volldigitalisierten Prozesses erneuern zu können.

§ 4 Antrag

Anstelle einer einfachen Vorgabe und Spezifizierung der BSI-seitig für relevant erachteten Produktkategorien, wünscht sich Bitkom eine entsprechende Beteiligung im Zuge der Festlegung künftiger Produktkategorien.

Der Antrag auf Erteilung des IT-Sicherheitskennzeichens muss von Beginn an zu 100% digital erfolgen. Von reinen PDF-basierten Formularen, die per Mail an das BSI gesandt werden müssen, ist abzusehen. Im Falle eines negativen Bescheids des BSI sollten den Antragsstellenden die Beweggründe mitgeteilt werden – auf digitalem Weg.

§ 5 Antragsprüfung

Nach § 5 Abs. 1 wird eine Plausibilitätsprüfung anhand der eingereichten Unterlagen des Antragstellers erlaubt. Eine eingehende Prüfung, bspw. ob die eingereichten Unterlagen inhaltlich auch tatsächlich zutreffend sind, ist nicht vorgesehen. Eine Rechtsgrundlage für eine solche Sachprüfung liegt damit nicht vor, erscheint für Bitkom aber erforderlich.

Gemäß § 5 Abs 5 Nr. 2 kann das BSI den Antrag ablehnen, wenn Hinweise vorliegen, dass Produkte des Herstellers bereits Gegenstand einer Warnung waren. Hierbei stellt sich zwingend die Frage nach den gewählten Kriterien. Die Ablehnung eines Antrags auf Basis aktueller Unzulänglichkeiten ist nachvollziehbar und richtig. Die Ablehnung eines Antrags auf Basis einer früheren Warnung darf allerdings nicht ausschlaggebend sein. Der Zusammenhang zwischen „heutigen" Warnungen und „morgiger" Erteilung / Verlängerung von Kennzeichen bedarf weiterer Klärung. Das bloße Bekanntwerden einer Schwachstelle und eine darauffolgende Warnung dürfen nicht zum Entzug eines Kennzeichens führen. Aus Sicht des Bitkom muss das Herstellerverhalten ausschlaggebend sein.

Bezugnehmend auf die Debatte zum staatlichen Umgang von Schwachstellen stellt sich die Frage, wem genau die Sicherheitslücken bekannt sein müssen, damit es zu einer Ablehnung des Antrags kommt. Wie ist im Falle von Sicherheitslücken zu verfahren, die dem BSI bekannt sind und für die Aufklärung von Straftaten und zur Strafverfolgung genutzt werden?

In § 5 Absatz 3 stellt sich die Frage, welche "branchenabgestimmten Standards" gemeint sind. Zählen international anerkannte Standards ebenfalls dazu?

§ 6 Vereinfachtes Verfahren

Bitkom begrüßt ausdrücklich, dass Unternehmen, die in einem Drittstaat bereits ein IT-Sicherheitskennzeichen für ein Produkt erhalten haben, dieses beim BSI vorlegen können. Allerdings klingt § 6 Absatz 2 Satz 2 nicht ambitioniert genug danach, dass sich das deutsche IT-Sicherheitskennzeichen einer europäischen Initiative unterordnen würde bzw. als europäisch skalierbar angedacht wird. Aus Sicht des Bitkom kann es keine Co-Existenz beider Kennzeichen geben und eine europäische Variante ist langfristig klar zu bevorzugen und anzustreben – idealerweise durch das Aufgehen des deutschen Kennzeichens in einer europäischen Variante.

§ 7 Gegenstand der Herstellererklärung

Gemäß § 7 Absatz 1 verpflichtet sich: "*Der Hersteller innerhalb des Zeitraumes [...] das Bundesamt unaufgefordert zu informieren, wenn ihm [...] Störungen der Informationssicherheit des Produktes und Sicherheitslücken (bekannt werden)*". Hier ist darauf zu achten, dass die Meldungen in Richtung BSI abgestimmt sind und sich mit den Vorgaben des BSI-Gesetzes decken.

In § 7 Absatz 1 heißt es: „*Der Hersteller verpflichtet sich des Weiteren, ihm bekannt werdende Sicherheitslücken unverzüglich zu beheben*“. Der Verweis auf die unverzügliche Behebung von Schwachstellen wirft Folgefragen auf, die es zur Schaffung von Rechtssicherheit für die Hersteller in der Verordnung zu beantworten gilt. Bspw. stellt sich die Frage, wie es um Teilkomponenten in einem Produkt bestellt ist, bei denen ein Hersteller bei der Patch-Bereitstellung auf den Zulieferer angewiesen ist. Bitkom schlägt vor, den Satz wie folgt zu fassen: „*Der Hersteller verpflichtet sich des Weiteren, Maßnahmen zu ergreifen, um ihm bekanntgewordene Sicherheitslücken zu beheben ~~ihm bekannt werdende Sicherheitslücken unverzüglich zu beheben~~*“

§ 8 Laufzeit des IT-Sicherheitskennzeichens und Erlöschen

Aus Sicht des Bitkom sollte das BSI nach § 5 nicht sechs Wochen Zeit erhalten, um Anträge zu prüfen, sondern lediglich vier Wochen. Wettbewerbsverzerrende Auswirkungen dürfen nicht unterschätzt werden, weshalb eine schnellstmögliche Prüfung anzustreben ist.

Gemäß § 8 Absatz 1 beträgt die Laufzeit regelmäßig zwei Jahre. Genügt das verwendete Wort "regelmäßig" in dem Satz bereits aus, um auszudrücken, dass ein Kennzeichen nach zwei Jahren erneuert werden kann und dann erneut 24 Monate Laufzeit bekommt? Ansonsten steht in dem Paragraph nichts zur Erneuerung des Kennzeichens.

Die Laufzeit wird das Merkmal sein, das sich zwischen den Produkten bzw. zwischen den Produktkategorien am meisten unterscheidet. Hersteller, die eine lange Laufzeit und Pflege garantieren sollten dies auch entsprechend kenntlich machen können.

§ 9 Verwendung des Sicherheitskennzeichens

Gemäß § 9 Absatz 4 hat der Hersteller dafür Sorge zu tragen, dass keine nach dem Erlöschen hergestellten Produkte mehr mit dem Etikett auf den Markt gebracht werden. Der damit verbundene logistische Aufwand könnte ein Hinderungsgrund für die Nutzung des Kennzeichens sein.

Hersteller sollten die Möglichkeit haben, ihre Produkte wahlweise physisch oder rein elektronisch (z.B. auf einem Display/Bildschirm) zu kennzeichnen. Dies sollte nicht bloß die Ausnahme darstellen. Die Vorteile von E-Labels sind: gezielte und leichter zugängliche Informationen für die jeweilige Zielgruppe; einfachere Informationsaktualisierung; positive Auswirkungen auf die Umwelt; weniger regulatorische Belastungen für Produktinnovationen; verbesserte Rückverfolgbarkeit und Transparenz von Produkten (Marktüberwachung); leichterer Nachweis der Einhaltung von Vorschriften.

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

Bitkom begrüßt die Möglichkeit, dass Branchenvertreterinnen und -vertreter dem BSI branchenspezifische Standards vorschlagen können und diese sogar in Technische Richtlinien überführt werden können. Dies hat das Potenzial, möglichst zeitnah eine produktgruppenübergreifende Verwendung des IT-Sicherheitskennzeichens zu erreichen. Gleichwohl müssen die nachfolgenden Punkte beachtet werden:

Ziel des IT-Sicherheitsgesetzes 2.0 ist ein ausreichendes Schutz- und Sicherheitsniveau. 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 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 miteinfließen.

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.

§ 11 Produktkategorien

Unmittelbar anknüpfend an die vorangegangenen Ausführungen ist die Berücksichtigung der (internationalen) Standardisierung bei der zentralen Festlegung der Produktkategorien und deren Sicherheitsanforderungen gemäß § 11 BSI-ITSiKV-E noch nicht ausreichend dargelegt. Festgestellt wird lediglich, dass für die konkreten Sicherheitsanforderungen auf Standards verwiesen werden kann, wobei diese im gleichen Rang zur Technischen Richtlinie stehen. Hier ist nicht ersichtlich, warum der gesetzlich grundlegend eingeräumte Vorrang internationaler Standardisierung zugunsten nationaler Ansätze – auch mit Blick auf die Zertifizierung nach EU Cybersecurity Act – entfallen sollte. In der Formulierung sollte die Vorrangstellung der Normung und Standardisierung gegenüber Technischen Richtlinien des BSI zum Ausdruck kommen.

Bitkom spricht sich dafür aus, dass die Erteilung eines IT-Sicherheitskennzeichens auch explizit für reine Softwareprodukte möglich gemacht wird, ganz gleich ob physisch oder digital vertrieben. Der Verordnungstext ist entsprechend zu erweitern.

Im Zusammenspiel der §§ 10 und 11 stellt sich die Frage, weshalb die betroffenen Branchen nicht in die Priorisierung der Produktkategorien einbezogen werden. Rein sachlogisch wäre es deutlich zielführender, wenn zuerst die Produktkategorien in Abstimmung mit der Branche identifiziert würden, und erst anschließend ein Standard

vorgeschlagen wird. Bitkom wünscht sich eine entsprechende Beteiligung im Zuge der Festlegung künftiger Produktkategorien.

Zudem muss gewährleistet sein, dass das IT-Sicherheitskennzeichen einem klar eingegrenzten Fokus auf Endverbraucherinnen und -verbraucher folgt. Höherwertige Prüfbescheinigungen dürfen dagegen nicht geschwächt und in KRITIS-Betrieben sowie mittelständischen oder multinationalen Unternehmen durch ein niederschwelliges IT-Sicherheitskennzeichen verdrängt werden.

§ 12 Aufsicht

§ 12 Absatz 1+2: Es ist wichtig zu klären, wie das erwähnte "Marktüberwachungskonzept" zugänglich gemacht werden soll (sobald es erstellt ist). Wird dies Konzept Teil der Kennzeichen-Website oder handelt es sich um ein BSI-internes Konzept? Falls letzteres der Fall ist, sollten zumindest die relevanten Kriterien spezifiziert werden.

Anknüpfend an die Ausführungen zur fehlenden Sachprüfung in § 5 stellt sich die Situation in § 12 ähnlich dar. Da sich das Martküberwachungskonzept innerhalb der Verordnung bewegen muss, würde sich dieses auf die Plausibilitätsprüfungsergebnisse, also auf die Papierlage, beschränken. Die Möglichkeit von Testkäufen, die § 12 Abs. 3 regelt, liefert in der jetzigen Form nicht die benötigte Klarstellung, dass die Behörde eine entsprechende Sachprüfung vornehmen darf. Das sollte unbedingt ergänzt werden.

§ 14 Evaluierung

Die vorgesehene Evaluierung sollte nicht nur alle drei Jahre unter Beteiligung der in § 10 Absatz 3 Satz 1 des BSI-Gesetzes genannten Ressorts erfolgen, sondern auch unter Einbeziehung der Wirtschaft, Wissenschaft und Zivilgesellschaft stattfinden. Zudem sollte die erste Evaluierungsrunde bereits nach einem Jahr stattfinden, um die größten Umsetzungsprobleme frühzeitig zu identifizieren und zu korrigieren.

Bitkom vertritt mehr als 2.700 Unternehmen der digitalen Wirtschaft, davon gut 2.000 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.