Berlin, 13.08.2021

Stellungnahme

Stellungnahme zum Referentenentwurf der "Rechtsverordnung zum IT-Sicherheitskennzeichen des Bundesamtes für Sicherheit in der Informationstechnik“

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Experten, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Expertenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie des Vertrauenszeichens "IT Security made in Germany". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Chausseestraße 17
10115 Berlin
Tel.: +49 30 4005 4310
https://www.teletrust.de

Wir begrüßen die weitere Ausgestaltung und Konkretisierung des IT-Sicherheitskennzeichens, welches es Verbraucherinnen und Verbrauchern ermöglicht, die IT-Sicherheit des jeweiligen IT-Produkts zu beurteilen. Nur mit transparenten Informationen zum IT-Sicherheitskennzeichen kann Vertrauen geschaffen und damit – aus Sicht des Verbrauchers – eine gut informierte Kaufentscheidung getroffen werden. Um diese Ziele zu erreichen, möchten wir Anregungen geben, die den Erfolg des IT-Sicherheitskennzeichen unterstützen sollen.

Zu § 5 Antragsprüfung

Die Entscheidung über die Vergabe des IT-Sicherheitskennzeichens wird maßgeblich auf Basis von Dokumenten getroffen, die vom Hersteller der Produkte eingereicht werden. In Verbindung mit § 9c Abs. 8 BSIG, der lediglich eine optionale Prüfung des Produkts vorsieht, ist eine ergänzende Prüfung der Produkte – so wie sie dem Verbraucher zum Kauf angeboten werden – empfehlenswert. Im Sinne der Durchführbarkeit der Produktprüfungen sollten automatisierte Testmethoden zum Einsatz kommen, die durch manuelle Tests begleitet werden. Ist die angeregte Produktprüfung zum gegenwärtigen Zeitpunkt nicht durchgängig möglich, so ist der Verbraucher im Sinne der Transparenz des Siegels darüber zu informieren. Dies kann beispielsweise durch Farbgestaltung, kleine Symbolbilder oder Verwendung von Kennzahlen innerhalb des Siegels erfolgen.

Zu § 6 Vereinfachtes Verfahren

Vereinfachte Verfahren haben grundsätzlich das Potential, die Effizienz der Vergabe des IT-Sicherheitskennzeichens zu steigern. Werden die übergeordneten Sicherheitsziele Vertraulichkeit, Verfügbarkeit und Integrität jedoch detaillierter betrachtet, so wird ersichtlich, dass unter Berücksichtigung der jeweils geltenden Gesetzgebung die Anwendung des vereinfachten Verfahrens begrenzt ist. So verlangt die Erfüllung des Sicherheitsziels der "Vertraulichkeit“ vielfach die Anwendung von Verschlüsselungsalgorithmen, deren Anwendung im globalen Kontext unterschiedlich geregelt ist. Am konkreten Beispiel der Verschlüsselung bedeutet das vereinfachte Verfahren, dass mindestens Änderungen der Gesetzgebung, Änderungen der Vergabekriterien des originären Kennzeichens, sowie Änderungen am Produkt bzw. dessen Unterlagen fortwährend zu begutachten sind. Inwieweit damit langfristig Effizienzsteigerungen möglich sind, ist fraglich. In Summe birgt der Einsatz des vereinfachten Verfahrens viele Potentiale zur Effizienzsteigerung. Gerade im Bereich der "Vertraulichkeit“ und vor dem Hintergrund einer langfristigen Anwendung einheitlicher Kriterien zur Vergabe des Sicherheitskennzeichens sollte jedoch über dessen Anwendung selektiv entschieden werden.

Zu § 7 Gegenstand der Herstellererklärung in Verbindung mit § 8 Laufzeit des IT-Sicherheitskennzeichens und Erlöschen

Die gegenwärtige Soft- und Hardwareentwicklung ist durch agile Vorgehensweisen geprägt. Dies hat Entwicklungszyklen zur Folge, die zum Teil kürzer als 2 Wochen sind. Diese Rahmenbedingungen verdeutlichen einerseits, dass Laufzeiten von mehr als 2 Jahren aus Perspektive der IT-Sicherheit wenig sinnvoll erscheinen. Diese Frist sollte daher als maximale Gültigkeitsdauer angegeben und durch Zertifizierungen der Entwicklungs- bzw. Herstellprozesse begleitet werden. Hieraus lässt sich eine Verstetigung der Sicherheit der resultierenden Produkte erwarten.

Darüber hinaus werden in § 7 Hersteller lediglich verpflichtet, die erklärten Eigenschaften des Produktes zu aktualisieren, "sobald sie [beispielsweise Sicherheitslücken] ihm bekannt werden“. Im Sinne der Erhöhung der Sicherheit sollte hier stattdessen die aktive und kontinuierliche Gewährleistung der IT-Sicherheit bei den Herstellern eingefordert werden. Als Beleg hierfür eignen sich dabei nicht nur Dokumente, sondern auch die erneute und kontinuierliche Durchführung von (automatisierten) Prüfroutinen. Ferner sollten stichprobenartige Kontrollen der Prüfbehörden verankert werden.

Zu § 9 Verwendung des Sicherheitskennzeichens

Der Widerruf des Sicherheitskennzeichens für nicht physische Produkte ist unproblematisch durch Entfernung von Links, Grafiken etc. möglich. Herausfordernder hingegen ist die Handhabung von physischen Produkten (beispielsweise Retail-Versionen von Software). Diesbezüglich wird in § 9 Abs. 4 geregelt, dass der Hersteller "keine nach dem Erlöschen hergestellten Produkte mehr mit Etikett auf den Markt [bringen darf]“. Da der Zeitpunkt der Herstellung vielfach nur schwierig nachzuvollziehen sein wird, sollten auch hier Maximalfristen, die

sich nicht am Herstellungsdatum, sondern am Zeitpunkt des Entzugs des Kennzeichens orientieren, vorgegeben werden. Dies gilt insbesondere, da eine Orientierung am Herstelldatum kontraproduktiv wirken kann, da nach der Erteilung des IT-Sicherheitskennzeichens ein Anreiz zur schnellen und umfangreichen Produktion geschaffen wird. Ggf. anschließend erkannte Sicherheitslücken würden in diesem Fall erst nach dem Abverkauf der vorproduzierten Produkte geschlossen.

Zur Fälschungssicherheit des IT-Sicherheitskennzeichens

Aus dem Referentenentwurf sind keine Informationen zur Fälschungssicherheit des IT-Sicherheitskennzeichens ersichtlich. Gerade wenn es das Ziel ist, ein Kennzeichen zu entwickeln, welches durch erhöhtes Verbrauchervertrauen verkaufsfördernd wirkt, erscheint das Risiko zur unautorisierten Nutzung hoch. Daher sind Maßnahmen zu definieren, die die Echtheit des Kennzeichens bestätigen und Kopien sowie nicht legitimierte Nutzung ausschließen oder zumindest begrenzen.

Allgemein

Das IT-Sicherheitskennzeichen zielt auf Produkte für Endverbraucherinnen und -verbraucher ab. Es sollte nochmals klar definiert werden, dass höherwertige Prüfungen bzw. Zertifizierungen nicht geschwächt oder vom Markt verdrängt werden dürfen. Für diese höherwertigen Prüfungen bzw. Zertifizierungen ist das IT-Sicherheitskennzeichen nicht geeignet. Dies gilt insbesondere auch für die im IT-Sicherheitsgesetz adressierten Betreiber von kritischen Infrastrukturen.

Zusammenfassung

Ein Sicherheitskennzeichen, das das Vertrauen der Verbraucher genießen soll, setzt strenge Anforderungen an Hersteller. Wie den Ausführungen zu § 5 entnommen werden kann, sind diese möglicherweise nicht immer wirtschaftlich abbildbar, so dass über mögliche Abstufungen des IT-Sicherheitskennzeichens entschieden werden sollte. Eine einzig auf Dokumenten basierte Vergabe des IT-Sicherheitskennzeichens ist jedoch kritisch zu betrachten. Ferner ist die konkrete Handhabung des IT-Sicherheitskennzeichens – gerade im Kontext sehr kurzer Entwicklungszyklen – festzulegen. Neben stichprobenartigen Prüfungen der Produkte, wurden in den Ausführungen zu § 7 und § 8 automatisierte Prüfroutinen angeregt sowie die aktive und kontinuierliche Prüfung durch die Hersteller eingefordert. Zusätzliche und dauerhafte Sicherheit kann durch zertifizierte Entwicklungs- und Herstellprozesse gefördert werden. Letztlich sollten auch Maßnahmen zur Fälschungssicherheit des IT-Sicherheitskennzeichens festgelegt werden, da mit dessen Erfolg die Attraktivität für Fälschungen und unberechtigte Verwendung steigt.

Wir hoffen, mit dieser Stellungnahme einen Beitrag zur weiteren Ausgestaltung des IT-Sicherheitskennzeichens geleistet zu haben und unterstützen die Weiterentwicklung ausdrücklich. Eine Abstimmung der IT-Sicherheitsvorgaben mit den jeweiligen Branchen sollte insbesondere auch die IT-Sicherheit betreffende Klärungen mit dem Bundesverband IT-Sicherheit umfassen. Hierfür bieten wir unsere Unterstützung an.