bitkom

Stellungnahme

August 2024

Evaluierung des IT-Sicherheitskennzeichens

Zusammenfassung

Das BSI vergibt seit 2021 das IT-Sicherheitskennzeichen für digitale Produkte und Dienste. Auf diese Weise soll mehr Transparenz für erkennbare Cybersicherheit am Verbrauchermarkt geschaffen werden. Das Kennzeichen wird in diesem Jahr gesetzlich evaluiert. Der Bitkom begrüßt diese Evaluierung, um die Wirksamkeit und Akzeptanz des IT-Sicherheitskennzeichens zu überprüfen. Es ist im Interesse der Digitalbranche, dass die Kriterien und Standards klar definiert und auf die Bedürfnisse des Marktes abgestimmt sind. Wir freuen uns daher über die Gelegenheit, an dieser Evaluierung teilzunehmen und im Namen unserer Mitglieder einen Beitrag dazu leisten zu können.

Neben den Evaluationskriterien gemäß § 14 der Verordnung zum IT-Sicherheitskennzeichen – Produktkategorien, Anerkennung von Branchenstandards und Freigabekriterien für das Kennzeichen – möchten wir mit dieser Stellungnahme ein Augenmerk auf das Verhältnis zwischen dem IT-Sicherheitskennzeichen und dem Cyber Resilience Act (CRA) legen. Für die Evaluierung und Weiterentwicklung des Kennzeichens ist es zwingend notwendig einen realen Mehrwert gegenüber den Verpflichtungen des CRA zu schaffen. Eine Möglichkeit wäre es, die bestehenden Strukturen und die Rolle des BSI zu nutzen, um Unternehmen beim Konformitätsprozess des CRA zu unterstützen und begleiten.

Für die Produktkategorien, zugehörig zu den vorgegebenen Evaluationskriterien, vermerken wir, dass die aktuelle Anzahl mit nur fünf Kategorien, von denen lediglich zwei in zweistelliger Höhe vergeben wurden, nicht ausreichend ist. Die schnelle Integration weiterer Produktkategorien wäre sinnvoll gewesen, um dem Kennzeichen mehr Gewicht zu verleihen. Bei der Anerkennung von Branchenstandards zeigt sich ein mangelnder Transfer von bestehenden Standards in die Kriterien des IT-Sicherheitskennzeichens, was die bisher mangelnde Durchsetzung unter den Marktteilnehmenden reflektiert. Zu den Freigabekriterien für das IT-Sicherheitskennzeichen halten wir fest, dass viele Mitgliedsunternehmen aufgrund gebundener Ressourcen durch verpflichtende Gesetze und hoher Kosten für Konformitätsbewertung und -prüfung der Produkte keinen ausreichend signifikanten Nutzen sehen. Mitgliedsunternehmen, die den Prozess bereits durchlaufen haben,

haben jedoch durchweg positive Erfahrungen gemacht. Sie loben die aktive und engagierte Unterstützung des BSI sowie die effiziente Beseitigung von Hindernissen im Vergabeprozess.

Insgesamt ist festzuhalten, dass eine Weiterentwicklung des IT-Sicherheitskennzeichens vor dem Hintergrund der laufenden Evaluierung stark vom Zusammenspiel mit europäischen Vorgaben und Standards, insbesondere dem CRA, und der Marktakzeptanz abhängig gemacht werden muss. Unternehmen stellen ihre Produkte in der Regel nicht für einen abgeschlossenen nationalen Markt her, der sich mit einer deutschen Kennzeichnung abdecken lässt, sondern wollen diese auf dem internationalen Markt vertreiben können. Die Cybersicherheitsregulierung wird richtigerweise zunehmend auf europäischer Ebene harmonisiert, was bei der weiteren Ausgestaltung unbedingt berücksichtigt werden muss. Das deutsche IT-Sicherheitskennzeichen sollte sich in dieses europäische Rahmenwerk einfügen, um einen Mehrwert im internationalen Kontext zu generieren. Mit der aktuellen Verbreitung sind jedoch keine signifikanten Vorteile durch das Kennzeichen erkennbar. Deshalb ist es notwendig, zu prüfen, wie bestehende Ressourcen und Strukturen effizienter genutzt werden können, etwa durch eine unterstützende Beratung im Rahmen des CRA. So lässt sich eine positive Wirkung erzielen, die mit der gegenwärtigen Verbreitung des Kennzeichens nicht realisierbar ist.

Verhältnis zum Cyber Resilience Act

Die Europäische Kommission zielt mit dem CRA darauf ab, die Cybersicherheit und Widerstandsfähigkeit gegenüber Cyberangriffen in der EU zu stärken. Sie setzt harmonisierte Cybersicherheitsstandards für Produkte mit digitalen Elementen fest, indem sie unter anderem Berichte über Vorfälle und automatische Sicherheitsupdates vorschreibt. Die Verordnung befindet sich zum heutigen Stand im Corrigendum-Prozess, welcher im Herbst 2024 abgeschlossen sein soll, woraufhin mit einem baldigen Inkrafttreten zu rechnen ist. Der CRA sieht eine Übergangsfrist von 3 Jahren vor, bis Hersteller die Anforderungen an ihre Produkte vollständig erfüllen müssen.

Mit seinem Anwendungsbereich umfasst der CRA die bestehenden Produktkategorien des IT-Sicherheitskennzeichensund setzt Kriterien, die sich mit den technischen und organisatorischen Anforderungen des Kennzeichens decken bzw. darüber hinausgehen. Durch die Einführung des verpflichtenden CRA stellt sich daher die logische Frage nach der Rolle des danebenstehenden IT-Sicherheitskennzeichens. Während das IT-Sicherheitskennzeichen eine begrenzte Anzahl an Produktkategorien vorzuweisen hat, hat die europäische Verordnung einen wesentlich weitreichenderen Umfang mit allen Produkten, die digitale Elemente enthalten.

Außerdem ergibt sich in jetziger Form eine Redundanz zwischen freiwilliger Kennzeichnung für Sichtbarkeit am Verbrauchermarkt einerseits und der Erfüllung von gesetzlichen Vorgaben durch den CRA andererseits. Es ist in Frage zu stellen, inwiefern sich mit einem nationalen Kennzeichen werben lässt, dessen Kriterien ohnehin durch die EU vorgegeben werden.

Neben den beschriebenen Redundanzen ergibt sich ein weiteres Problem durch den CRA, selbst zu diesem frühen Zeitpunkt, an dem die Verordnung noch nicht greift. Da das IT-Sicherheitskennzeichen auf Freiwilligkeit basiert, müssen Unternehmen sorgfältig abwägen, inwieweit sie Ressourcen in die Konformität ihrer Produkte investieren. Die bestehende und bevorstehende Cybersicherheitsregulierung bindet erhebliche interne Ressourcen, die sowohl für laufende Auflagen und Meldepflichten als auch für die Vorbereitung auf die Konformität eingesetzt werden müssen. Dies wird besonders am CRA deutlich, da Unternehmen ihre Produktion so umgestalten müssen, dass sie nach der Übergangsfrist weiterhin ein CE-Kennzeichen erhalten können. Unsere Mitgliedsunternehmen berichten, dass sie derzeit bereits an ihrer Auslastungsgrenze arbeiten und deshalb keine Kapazitäten für freiwillige Kennzeichen haben. Diese Situation wird zusätzlich durch äußere Umstände wie den Fachkräftemangel verschärft.

Um sich klar vom CRA abzugrenzen, könnte das BSI die Anforderungen an ein neues IT-Sicherheitskennzeichen deutlich höher ansetzen als die des CRA. Ein deutlich höher angesetztes Niveau des IT-Sicherheitskennzeichens zur Abgrenzung vom CRA könnte zwar auf den ersten Blick eine schärfere Profilierung der Anforderungen suggerieren, würde jedoch in der Praxis kaum zur gewünschten Breitenwirkung führen. Angesichts der bisher niedrigen Verbreitung des IT-Sicherheitskennzeichens ist zu befürchten, dass höhere Hürden eher abschreckend auf Unternehmen wirken, da zu häufig wenig Ressourcen für Umsetzung und Auditierung vorliegen. Statt einer stärkeren Durchdringung des Marktes und einer breiteren Anwendung des Sicherheitskennzeichens würde eine solche Anhebung der Anforderungen wahrscheinlich genau das Gegenteil bewirken: Es würde die Anzahl der Unternehmen, die das Kennzeichen implementieren können oder wollen, weiter verringern und damit seine Relevanz und Wirksamkeit auf dem Markt schwächen.

Alternativ bietet es sich an, die bestehenden Kompetenzen im BSI zu nutzen, um die Ressourcen als Kompetenzstelle zur Vorbereitung auf den CRA zu bündeln. Angesichts der noch bestehenden längeren Übergangsfrist und der zahlreichen offenen Fragen in der Wirtschaft, stellt dies eine ideale Gelegenheit dar, um Unternehmen gezielt auf die neuen europäischen Anforderungen vorzubereiten. Hier könnte das BSI eine zentrale Rolle spielen, indem es die Firmen unterstützt und ihnen hilft, die zukünftigen Herausforderungen erfolgreich zu meistern. Mit dem bereits bestehenden Fachwissen und vorhandenen Ressourcen kann eine Plattform geboten werden, die für Rechtssicherheit und Zuverlässigkeit im Sinne einer harmonisierten Cybersicherheit sorgt.

Von herausragender Bedeutung ist außerdem, dass die bereits vorgegebenen Standards des IT-Sicherheitskennzeichens in den europäischen Standardisierungsprozess einfließen. Das BSI sollte seine umfangreiche Vorarbeit und Expertise unbedingt bei der Erarbeitung von Standards für den CRA einbringen. Dies würde nicht nur die Qualität und Sicherheit der Produkte erhöhen, sondern auch die internationale Wettbewerbsfähigkeit der deutschen Wirtschaft stärken.

Produktkategorien

Die aktuelle Anzahl der Produktkategorien für das IT-Sicherheitskennzeichen bleibt hinter den Erwartungen zurück. Nach aktuellem Stand gibt es nur fünf aktive Kategorien, von denen lediglich zwei in zweistelliger Höhe vergeben wurden. Insbesondere sind 18 E-Mail-Dienste und 34 Breitbandrouter mit dem IT-Sicherheitskennzeichen ausgezeichnet. Die Erweiterung des Kennzeichens auf Smartphones ist zu begrüßen, da dies eine Ausweitung des Angebots darstellt. Aus dem Feedback unserer Mitgliedsunternehmen geht hervor, dass die ursprüngliche Idee des IT-Sicherheitskennzeichens grundsätzlich auf positive Resonanz gestoßen ist. Sie hätten sich stärker eingebracht, konnten aber unter den Erweiterungen der Produktkategorien keine für ihre Produktpalette passende finden.

Aus unserer Sicht zeigt sich daher, dass die schnelle Integration weiterer Produktkategorien sinnvoll gewesen wäre, um dem Kennzeichen insgesamt mehr Gewicht zu verleihen. Vor dem Hintergrund von einzeln ausgearbeiteten Standards wird jedoch auch offensichtlich, wo die Schwierigkeit in dieser Erweiterung liegt. Für die Zukunft ergibt sich bei der Identifikation sinnvoller Produktkategorien eine große Chance, wenn Lücken gefüllt werden können, die durch Regulierungen wie CRA, CER und NIS2 entstehen. Insbesondere für kleine und mittelständische Unternehmen (KMUs) könnte das IT-Sicherheitskennzeichen dann als eine Art Leitfaden für mehr Informationssicherheit in ihren Produkten dienen. Dies könnte sich als Wettbewerbsvorteil erweisen, besonders für deutsche Softwarehersteller, die die deutsche öffentliche Verwaltung beliefern möchten.

Anerkennung von Branchenstandards

Bei der Überprüfung der Anerkennung von Branchenstandards im Zusammenhang mit dem IT-Sicherheitskennzeichen wird deutlich, dass der beabsichtigte Transfer bestehender Standards in die Kriterien dieses Kennzeichens bislang nicht erfolgreich umgesetzt wurde. Wir vermuten, dass dies auf die unzureichende Durchsetzung des Kennzeichens unter den Marktteilnehmenden zurückzuführen ist. Derzeit scheint es an einem effektiven Mechanismus zu fehlen, der sicherstellt, dass die bestehenden Branchenstandards tatsächlich Anwendung finden. Nur wenn dieses Problem gelöst würde, könnten Unternehmen aus eigenem Interesse vermehrt dazu bereit sein, ihre etablierten Standards in die Kriterien des IT-Sicherheitskennzeichens einzubringen. Dies schließt direkt an die bereits genannte Problematik der geringen Marktakzeptanz an.

Freigabekriterien für das Kennzeichen

Im Rahmen der Qualifizierung von Produkten für die Freigabekriterien des IT-Sicherheitskennzeichens stellt sich für Hersteller die Frage nach dem Verhältnis von Aufwand und Nutzen. Dies gilt selbstverständlich nicht nur für das IT-Sicherheitskennzeichen, sondern für alle freiwilligen Maßnahmen. Viele Mitgliedsunternehmen sehen bei der Evaluierung dieses Verhältnisses jedoch keinen

signifikanten Nutzen. Dies ist teilweise auf die durch verpflichtende Gesetze gebundenen Ressourcen zurückzuführen, wie bereits im Zusammenhang mit dem CRA beschrieben. Ein weiterer Faktor sind die Kosten für Konformitätsbewertung und -prüfung, die oft den potenziellen Gewinn durch eine positive Verbraucherwahrnehmung übersteigen. Zudem können Stichprobenüberprüfungen weitere Ressourcen im Unternehmen binden. Es wird auch berücksichtigt, dass Produkte möglicherweise ihr End-of-Life erreichen, bevor die zwei Jahre für das Kennzeichen abgelaufen sind, was die Kosten-Nutzen-Bilanz weiter verschlechtert. Solange Unternehmen keinen signifikanten Nutzen, etwa durch höhere Verkaufszahlen, im IT-Sicherheitskennzeichen sehen, wird sich dieses Problem nicht lösen lassen. Ein möglicher Vorschlag wäre eine neutrale Untersuchung unter Verbrauchern, um den tatsächlichen Effekt messbar zu machen.

Mitgliedsunternehmen, die einen Nutzen im Kennzeichen sehen und den Freigabeprozess bereits durchlaufen haben, berichten jedoch durchweg von positiven Erfahrungen. Die Freigabekriterien des Kennzeichens zeichnen sich durch die aktive und engagierte Unterstützung des BSI aus. Insbesondere hervorzuheben ist die Möglichkeit, offene Fragen und potenzielle Hindernisse direkt kommunizieren zu können. Diese werden vom BSI zeitnah und effizient ausgeräumt, was den gesamten Vergabeprozess erheblich erleichtert. Der stellt ein Alleinstellungsmerkmal für das Kennzeichen dar und sollte daher beibehalten werden.

Angesichts einer möglichen Ausweitung der Produktkategorien und einer Fokussierung auf CRA-Anforderungen ist es jedoch essenziell, dass die Skalierbarkeit der Prozesse bei der damit verbundenen Zunahme von Anfragen sichergestellt wird. Wir empfehlen daher, die Kapazitäten des BSI entsprechend zu optimieren. Auf diese Weise kann gewährleistet werden, dass die Unterstützung für Unternehmen auch bei steigendem Anfragevolumen in weiterhin hoher Qualität abläuft. Insgesamt sehen wir die aktive Unterstützung des BSI als einen wesentlichen Erfolgsfaktor des Kennzeichens und sprechen uns klar dafür aus, diesen Service beizubehalten, weiterzuentwickeln und auszubauen.

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. 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, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. 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 leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber

Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner

Felix Kuhlenkamp | Referent Sicherheitspolitik
T 030 27576-279 | f.kuhlenkamp@bitkom.org

Verantwortliches Bitkom-Gremium

AK Informationssicherheit