GESELLSCHAFT
FÜR INFORMATIK

Berlin, 26. August 2024

Stellungnahme

der Gesellschaft für Informatik e.V. (GI)

Zur Evaluation des IT-Sicherheitskennzeichens

GESELLSCHAFT
FÜR INFORMATIK

Hintergrund

Für das IT-Sicherheitskennzeichen für digitale Produkte und Dienste definiert das Bundesamt für Sicherheit in der Informationstechnik (BSI) unter Einbeziehung von Stakeholdern für bestimmte Produktkategorien (z. B. Breitbandrouter, E-Mail-Dienste) zu erfüllende Sicherheitseigenschaften. Diese Sicherheitseigenschaften richten sich nach geltenden Standards. Dienstleistungs- und Herstellungsunternehmen, die Produkte mit dem IT-Sicherheitskennzeichen versehen wollen, verpflichten sich, diese Sicherheitseigenschaften entsprechend einzuhalten. Sie führen dazu eine Konformitätsprüfung durch (oder beauftragen dazu eine Bewertungsstelle). Das BSI prüft die Vollständigkeit der bereitgestellten Angaben und vergibt entsprechend das IT-Sicherheitskennzeichen. Nach dessen Erteilung kann die BSI-Marktaufsicht anlassbezogen oder anlasslos stichprobenartig prüfen, ob die Unternehmen ihre Versprechen einhalten.

Das Bundesministerium des Innern und für Heimat (BMI) hat Fachverbände und Interessensvertreter*innen dazu aufgefordert, zu dem seit 2021 vergebenen IT-Sicherheitskennzeichen ihre Einschätzungen abzugeben. Die Gesellschaft für Informatik kommt dem mit dieser Stellungnahme nach.

Grundsätzliche Einschätzung

Wir als Gesellschaft für Informatik e.V. (GI) sehen die Ziele, die IT-Sicherheit von Verbrauchsprodukten zu fördern, diesbezüglich Vertrauen von Verbraucher*innen herzustellen und IT-Sicherheit als marktrelevantes Kriterium zu stärken, als sehr relevant für mehr Cyberresilienz in Deutschland an.

Für die IT-Sicherheit etablierte Standards, Normen und diesbezügliche Zertifizierungen sind für Verbraucher*innen wenig verständlich und transparent. Bis zur Etablierung des IT-Sicherheitskennzeichen gab es kein staatlich anerkanntes Kennzeichen, dass die IT-Sicherheit von Produkten für Verbraucher*innen sichtbar machte und als Kaufkriterium etablierte.

> *Wir bewerten das IT-Sicherheitskennzeichen insgesamt als wirksames Mittel, um die Cyberresilienz von Organisationen sowie das Vertrauen von Verbraucher*innen in IT-Produkte zu stärken. Wir sehen jedoch, dass das Kennzeichen eine deutlich größere Relevanz und Reichweite erhalten könnte und sollte.*

Im Folgenden erläutern wir diesbezügliche Aspekte und Verbesserungsmöglichkeiten des IT-Sicherheitskennzeichens.

Einschätzung zu den Freigabekriterien für das Kennzeichen

Mit dem freiwilligen IT-Sicherheitskennzeichen vertraut das BSI auf die Erklärung der Unternehmen, dass diese die definierten Sicherheitseigenschaften in der Praxis einhalten. Dies erkennen wir als ein kosteneffizientes Mittel an, um die anfangs genannten Ziele zu fördern. Wir kritisieren jedoch, dass dadurch eine systematische, verlässliche Vorgabe und Prüfung und unabhängige Bestätigung über die Einhaltung der Sicherheitskriterien fehlt. Die stichprobenartigen Überprüfungen der ausgezeichneten Unternehmen können dem zwar entgegenwirken. Leider liegen uns jedoch keine Vorgaben oder Zahlen vor, wie oft solche Überprüfungen tatsächlich stattfinden.

> *Um die Wirksamkeit der Umsetzung zu gewährleisten, fordern wir daher dazu auf, mindestens fünfzig Prozent der gekennzeichneten Produkte stichprobenartig zu überprüfen. Außerdem fordern wir ein transparentes öffentliches Berichtswesen zu den Überprüfungen, um das Vertrauen in das Kennzeichen zu stärken.*

Einschätzung zu den Produktkategorien

Innerhalb der drei Jahre, während der das IT-Sicherheitskennzeichen besteht, haben insgesamt neun Unternehmen das IT-Sicherheitssiegel erhalten. Insgesamt hat das BSI Sicherheitskriterien für fünf Produktkategorien aufgestellt. Wir als GI bedauern die geringe thematische Breite der mit dem Kennzeichen versehenen Produkte sowie das bisher verhaltene Interesse von Unternehmen am Kennzeichen, das sich in diesen Zahlen zeigt.

> *Wir ermutigen dazu, weitere Unternehmen für das Kennzeichen zu motivieren sowie eine höhere Produktabdeckung zu erreichen.*

Um mehr Unternehmen für das Kennzeichen zu gewinnen schlagen wir z. B. Kampagnen vor, in denen die Erfahrungswerte und Erfolge von schon teilnehmenden Unternehmen geteilt werden und stärker für die steigende Relevanz des Themas geworben wird.

Außerdem sollten die Produktkategorien deutlich erweitert werden. Wir empfehlen hierfür,

1. dass das BSI sich bei der Festlegung der Produktkategorien zukünftig daran orientiert, welche Produkte von Verbraucher*innen stark nachgefragt werden (z. B. Smartphones);

2. dass sich das BSI daran orientiert, für welche Produktkategorien es bereits Technische Richtlinien veröffentlicht hat, aus denen dann konkrete

Sicherheitsanforderungen abgeleitet werden können. (So gibt es zum Beispiel die TR-03161 für Anwendungen im Gesundheitswesen, aber keine Kategorie für entsprechende Produkte, die das IT-Sicherheitskennzeichen anstreben.);

3. dass alle Produkte, die Software-basierte Funktionen beinhalten und Kommunikationsbeziehungen über das Internet aufnehmen, mit einbezogen werden.

Einschätzung zur Anerkennung von Branchenstandards

Wir als GI befürworten den in §10 (5) der Verordnung zum IT-Sicherheitskennzeichen des Bundesamtes für Sicherheit in der Informationstechnik (BSI-ITSiKV) festgelegten Ansatz, den Bedarf für neue Technische Richtlinien nachfrageorientiert aus Herstellervorschlägen für Sicherheitsvorgaben zu motivieren. Auch der in §10 (4) festgelegte Prozess, durch den Konkurrentinnen und Konkurrenten konsensual einen Vorschlag für einen Standard vorschlagen müssen, werten wir als positive Entlastung des BSI.

In §11 (2) des BSI-ITSiKV ist festgelegt, dass das BSI sich bei der Aufstellung der Sicherheitsanforderungen um ein Gleichauf mit international etablierten Standards „bemüht".

> *Um das IT-Sicherheitskennzeichen zu stärken und international anschlussfähig zu halten, fordern wir dazu auf, den Passus §11 (2) des BSI-ITSiKV zu stärken und damit internationale technische Standards tatsächlich einzuhalten oder zu übertreffen.*

Letzteres ist umso relevanter, da zukünftig Dienstleistungs- und Herstellungsunternehmen von IT-Produkten mit dem Cyber Resilience Act (CRA) der Europäischen Union dazu verpflichtet werden, IT-Sicherheitsstandards während des gesamten Lebenszyklus ihrer vernetzten Produkte einzuführen und einzuhalten. Das Sicherheitskennzeichen (und die damit verbundene Honorierung von Unternehmen, die solche Standards bisher freiwillig befolgen) könnte somit obsolet werden. Um dem entgegenzuwirken, sollten die Anforderungen des IT-Sicherheitskennzeichens über die mit dem CRA eingeführten Mindeststandards deutlich hinausgehen.

> *Wir empfehlen daher, die in den Produktkategorien aufgestellten Sicherheitseigenschaften in Bezug auf die Anforderungen des CRA zu prüfen und entsprechend zu erhöhen.*

Bei der Erhöhung der Sicherheitsanforderungen sollten die verwendeten Programmiersprachen sowie Secure Coding Standards Bedeutung erhalten. Hierbei

sollte berücksichtigt werden, dass unterschiedliche Programmiersprachen auch eine sehr unterschiedliches Qualitätsniveau hinsichtlich der IT-Sicherheit bieten.

Sonstiges

Wir als GI sehen die Umsetzung eines QR-Codes, der Verbraucher*innen über die Kriterien der IT-Sicherheit des Produkts sowie deren Aktualität informiert, als guten kommunikativen Ansatz. Zum gegenwärtigen Zeitpunkt fehlen jedoch noch in das Konzept eingebundene, gebrauchstaugliche Anwendungen und Schnittstellen, um einen dauerhaften Überblick über eingescannte Produkte zu erhalten.

> *Wir regen an, möglichst automatisierte Informationen (z. B. E-Mail- oder Push-Benachrichtigung) über kritische Schwachstellen der Produkte einzuführen, um individuelle Schutzziele effektiv, effizient und zufriedenstellend zu unterstützen.*

Über die Gesellschaft für Informatik e.V. (GI)

Die Gesellschaft für Informatik e.V. (GI) ist die größte Fachgesellschaft für Informatik im deutschsprachigen Raum. Seit 1969 vertritt sie die Interessen der Informatikerinnen und Informatiker in Wissenschaft, Gesellschaft und Politik und setzt sich für eine gemeinwohlorientierte Digitalisierung ein. Mit 14 Fachbereichen, über 30 aktiven Regionalgruppen und unzähligen Fachgruppen ist die GI Plattform und Sprachrohr für alle Disziplinen in der Informatik. Weitere Informationen finden Sie unter www.gi.de.