Stellungnahme

IT-Sicherheitskennzeichen

09. April 2019

Zusammenfassung

Im Zuge der Erarbeitung des IT-Sicherheitsgesetzes 2.0 plant das Bundesministerium des Innern, für Bau und Heimat (BMI) ein IT-Sicherheitskennzeichen für mehr Transparenz für den Verbraucher einzuführen. Die Digitalwirtschaft steht einem IT-Sicherheitskennzeichen grundsätzlich positiv und offen gegenüber. Transparenz in der IT-Sicherheit für den Verbraucher als notwendigen Baustein der Vertrauensbildung unterstützen wir.

Die Anwender beeinflussen durch ihre Kaufentscheidung für sicherere Produkte das Angebot. Sie verhindern durch kluges Nutzungsverhalten, dass Einfallstore für Angreifer geschaffen werden. Das Vertrauen der Verbraucher wird zukünftig davon abhängen, wie sicher die Nutzer ihre Geräte einschätzen. In diesem Zusammenhang spielt die Sensibilisierung für IT-Sicherheit eine nicht zu unterschätzende Rolle. Hier kann das IT-Sicherheitskennzeichen positiv unterstützen. Damit ein Kennzeichen allerdings seine volle Wirkung entfällt – d.h. den Käufer positiv in seiner Kaufentscheidung beeinflusst und damit mehr sichere Geräte in den Umlauf bringt – sind aus Sicht des Bitkom einige wichtige Punkte zu beachten, auf die wir im Folgenden im Detail eingehen.

Darüber hinaus ist ein IT-Sicherheitskennzeichen nur als eine kleine Komponente eines umfassenden Konzeptes für mehr IT-Sicherheit zu verstehen. Das Ziel eines höheren IT-Sicherheitsniveaus kann nur erreicht werden, wenn Hersteller und Anwender, Infrastrukturbetreiber und Strafermittlungsbehörden gemeinsam darauf hinwirken und ihre jeweilige Verantwortung innerhalb des Ökosystems übernehmen. Dies muss bei der Ausgestaltung von Gesetzesvorhaben immer mit bedacht werden.

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

Teresa Ritter
Bereichsleiterin Sicherheitspolitik
T +49 30 27576-203
t.ritter@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Achim Berg

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Internationale und sektorielle Ausgestaltung

Da die Unternehmen der Digitalwirtschaft auf internationalen Märkten agieren, ist eine mindestens europaweit einheitliche Einführung eines IT-Sicherheitskennzeichens von höchster Priorität. Damit es innerhalb der EU zu keiner Fragmentierung von freiwilligen Kennzeichen, Labels oder Siegeln kommt, sollten Vorschläge europäisch etabliert werden. 28 verschiedene IT-Sicherheitskennzeichen, die nur in den jeweiligen Mitglieds-

staaten gelten, wären nicht nur ein bürokratisch höchst aufwendiges Konstrukt für die jeweiligen Hersteller. Eine solche Fragmentierung würde ebenso seine Wirkung beim Verbraucher, für mehr Transparenz und Übersicht beim Thema IT-Sicherheit zu sorgen, verfehlen.

Eine deutsche Lösung muss europäisch abgestimmt sein und das Potenzial haben, international skalierbar zu sein. Deshalb sollte Deutschland seine Vorstellungen und Vorarbeiten von Anfang an in den europäischen Prozess einbringen und sein Konzept von Beginn an als europäische Lösung vorstellen. In diesem Zusammenhang sind besonders die europäischen Bemühungen um den EU Cybersecurity Act zu beachten. Hier ist ein sogenannter Beipackzettel angedacht. Sobald der Beipackzettel auf europäischer Ebene etabliert ist, sollte er das IT-Sicherheitskennzeichen substituieren.

Betrachtung über den gesamten Lebenszyklus eines Produktes

Wir begrüßen auch den Ansatz, über eine dynamische Komponente im IT-Sicherheitskennzeichen den zunehmend kürzer werdenden Innovationszyklen insbesondere im IT- und Cyberbereich gerecht zu werden.

Das Update-Management des Herstellers spielt hierbei natürlich eine große Rolle. Wie lange Updates entwickelt bzw. bereitgestellt werden und in welchem Zeitraum sowohl die Entwicklung als auch die Bereitstellung geschehen muss, darf nicht für alle Produkte gleichermaßen festgelegt werden. Die Entwicklung von Updates nimmt naturgemäß unterschiedlich viel Zeit in Anspruch. Dabei empfiehlt es sich Reaktionszeiten an bestehenden, gängigen Maßen zu orientieren. Zudem sind die derzeitigen regulatorischen Entwicklungen zu berücksichtigen, die Einfluss auf Pflichten hinsichtlich Updates haben werden (insb. Digital Content Directive, ePrivacy Verordnung). Es gilt auch zu beachten, dass in der Sicherheitsarchitektur eines Produktes das Zusammenspiel einer Vielzahl von Komponenten die Sicherheit eines Produktes ausmachen und hierin elementarer Treiber von Innovation darstellt.

Gerade beim Thema Verbraucher- bzw. Betreiberverantwortung sehen wir beim vorliegenden Konzept erhebliche Lücken. In der Regel ist ein kontinuierliches Patch-Management ein großer Kostentreiber. Deshalb sollte sich eine dynamische Komponente beim IT-Sicherheitskennzeichen nicht auf einen passiven, Hersteller-fokussierten Ansatz beschränken, sondern sollte auch starke Motivatoren für Verbraucher und Betreiber beinhalten, Updates und Patches zeitnah zu installieren und somit die Sicherheit eines Produktes oder Systems über seinen gesamten Lebenszyklus hinweg zu gewährleisten.

Internationale Standards als Grundlage

Bei der Ausgestaltung von Standards und Normen ist es notwendig, dass die bereits europäisch anerkannten und bewährten Prozesse eingesetzt werden. Die Standards und Normen, auf Grundlage derer das Kennzeichen vergeben wird, müssen von den nationalen bzw. europäischen und internationalen Normungsorganisationen erarbeitet werden. Dadurch lässt sich sicherstellen, dass die Standards bzw. Normen europäisch anerkannt sind und keine nationalen Lösungen darstellen. Deshalb sollte vermieden werden, dass das IT-Kennzeichen ausschließlich auf Grundlage von Technischen Richtlinien des BSI, welche sich nicht auf internationale Standards beziehen, vergeben wird. Eine anschließende Internationalisierung würde sich dadurch äußerst schwierig gestalten.

Außerdem muss bedacht werden, dass Standards und Normen von unterschiedlichen Normungsorganisationen möglicherweise im Wettbewerb zu einander stehen könnten. Hier sollte es einen transparenten Prozess geben, der festlegt, wie in diesem Falle verfahren wird.

Unterschied an IT-Sicherheit muss erkennbar sein

Die Standards und Normen, die dem Kennzeichen zugrunde liegen werden, sind aller Voraussicht nach Mindestanforderungen. Es muss klar ersichtlich werden, welches Gerät diese Mindestanforderungen gerade so erfüllt und welche Geräte mit komplexeren Sicherheitsanforderungen ausgestattet sind. Ein Kennzeichen darf nicht zu Lasten der Hersteller gehen, die schon viel für die IT-Sicherheit ihrer Produkte machen. Möglich wäre ein abgestuftes Kennzeichen, welches auch höhere und anwendungsspezifischere Sicherheitsstandards abbilden kann und mit höheren Anforderungen an den Hersteller einhergeht. Im Zusammenhang mit der IT-Sicherheitsgesetz 2.0 könnte ggf. somit auch für den Nutzer ersichtlich sein, dass das jeweilige Produkt KRITIS-Fest ist. Dies sollte entsprechend der Sicherheitslevel „basic“, „substantial“ und „high“ des Cybersecurity Acts (CSA) erfolgen.

Ein Kennzeichen birgt außerdem die Gefahr, dass der Verbraucher sich durch den Kauf eines ausgezeichneten Gerätes in vollkommener Sicherheit wägt und einen sorgsamen Umgang mit dem Produkt nicht mehr gewährleistet ist. Dem Verbraucher muss klar gemacht werden, dass es sich hier nur um ein Mindestmaß an Sicherheit handelt und dass der richtige Umgang mit dem Gerät eine weitere unverzichtbare Komponente ist. Neben einem kontinuierlichen Patch-Management durch den Verbraucher ist ein regelmäßiges Überprüfen des aktuellen Sicherheitsniveaus unbedingt notwendig.

Produktdatenbank

Aus diesem Grund unterstützen wir die Idee einer Produktdatenbank, die in Echtzeit Auskunft darüber geben soll, in welchem Sicherheitszustand sich das Gerät befindet. D.h. unter anderem, ob der Betreiber weiterhin Updates zum Schließen von Lücken anbietet. Es wird sich über die Zeit herausstellen, ob dieses Konzept genügend skalierbar ist und so dynamisch wie nötig betrieben werden kann. Bei der Vielzahl an internetfähigen Produkten, muss das BSI personell stark aufstocken. Als Vorschlag zur Entlastung der Behörde könnte den Herstellern auferlegt werden, die Produktdatenbank für die eigenen Produkte zu pflegen. In diesem Zusammenhang sollte auch dem Endnutzer die Möglichkeit gegeben werden Sicherheitslücken, Fehler oder Probleme an zentraler Stelle an den Hersteller oder dem BSI zu melden.

Marktüberwachung

Damit das Konzept des IT-Sicherheitskennzeichens funktioniert, braucht es eine starke flächendeckende Marktüberwachung. Neben privatrechtlicher Durchsetzung im Markt muss der Staat in der Lage sein, diese Funktion zu übernehmen. Es gilt eine stete Überwachung der gekennzeichneten Produkte sicherzustellen, um Missbrauch des Kennzeichens zu verhindern.

Apps und andere Anwendungen

Es muss klar definiert werden, wo die Verantwortung des Herstellers endet. Apps und andere Anwendungen, die auf Produkte aufgespielt werden, können ebenfalls Sicherheitslücken aufweisen. Sie liegen aber nicht mehr im Verantwortungsbereich der Hersteller, sondern bedürfen eigenen Regelungen.