Referentenentwurf veröffentlicht – das freiwillige IT-Sicherheitskennzeichen kommt

Ein Beitrag von Stefan Hessel und Karin Potel

Durch das IT-Sicherheitsgesetz 2.0 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) den Auftrag erhalten, ein freiwilliges IT-Sicherheitskennzeichen zur Verbesserung der Verbraucherinformation einzuführen. Bereits Ende des Jahres sollen Verbraucher durch das Kennzeichen die Möglichkeit erhalten, sich leicht über vom Hersteller zugesicherte Sicherheitsfunktionen von Produkten und Diensten zu informieren. Das IT-Sicherheitskennzeichen soll als freiwilliges Label für IT-Produkte auf Basis des § 9c BSIG ausgestaltet werden. Es trifft jedoch keine Aussagen zum Datenschutz.

Das freiwillige IT-Sicherheitskennzeichen ist vergleichbar mit einer Cybersicherheitszertifizierung nach dem Cybersecurity Act, mit diesem jedoch nicht identisch. Es ist aber wahrscheinlich, dass das nationale IT-Sicherheitskennzeichen später in die europäische Cybersicherheitszertifizierung überführt wird. Das BSI deutet einen entsprechenden Übergang sogar bereits auf der Webseite an, sicher ist das jedoch keineswegs.

Relevanz für Unternehmen

Unternehmen sind durch die Kennzeichnung zukünftig in der Lage, die Sicherheitseigenschaften ihrer IT-Produkte leicht erkennbar zu machen, und können sich damit am Markt hervorheben. Aufgrund des steigenden Informationsbedürfnisses des Verbrauchers zu Cybersecurity-Aspekten kann die Kennzeichnung daher ein Verkaufsargument darstellen.

Antragsverfahren und Marktaufsicht

Eine Antragstellung soll im Laufe des Jahres für Breitbandrouter, die unter den Anwendungsgegenstand der BSI TR-03148 fallen, ermöglicht werden. Weitere Produktkategorien sollen folgen. Die eingereichten Herstellererklärungen werden einer Vollständigkeits- und Plausibilitätsprüfung unterzogen, für die das BSI regelmäßig eine Frist von sechs Wochen vorsieht.

Die Erteilung des Kennzeichens erfolgt in der Regel für mindestens zwei Jahre. Während dieser Zeit ist der Hersteller verpflichtet, die Konformität des Produktes aufrechtzuerhalten und dem BSI Änderungen

mitzuteilen. Das BSI ist zugleich berechtigt, die durch den Hersteller zugesicherten Anforderungen stichprobenartig oder anlassbezogen zu überprüfen.

Eine Ablehnung des Antrags kommt in Betracht, wenn Hinweise dafür vorliegen, dass das Produkt oder die mit dem Produkt ausgelieferte Software bekannte Sicherheitslücken enthält und bereits eine Warnung oder Information nach §§ 7, 7a BSIG erfolgt ist bzw. Maßnahmen nach § 9c Abs. 8 BSIG getroffen wurden. Liegt zu einem späteren Zeitpunkt ein Verstoß gegen die Herstellererklärung vor oder sind die gesetzlichen Voraussetzungen nicht erfüllt, so kann das IT-Sicherheitskennzeichen nach § 9c Abs. 8 BSIG entzogen werden.

Aktuelle Entwicklungen

Erst kürzlich hat das Bundesministerium des Innern, Bau und Heimat (BMI) den Entwurf einer Rechtsverordnung zum IT-Sicherheitskennzeichen des Bundesamtes für Sicherheit in der Informationstechnik veröffentlicht. Inhalt des Entwurfs ist die Gestaltung und Verwendung des IT-Sicherheitskennzeichens. Es soll aus der Herstellererklärung und der Sicherheitsinformation bestehen, auf die beide auf dem Etikett verwiesen wird. Darüber hinaus enthält der Entwurf Regelungen zu Antragsverfahren und -prüfung. Verbraucherinformationen zu Produkten mit Freigabe zur Nutzung sollen auf der Webseite des BSI veröffentlicht werden.

In diesem Zusammenhang ergeben sich weitere Fragestellungen in Bezug auf die Verpflichtung der Hersteller, dem BSI die für die produktspezifische Webseite notwendigen Informationen bereitzustellen (sog. dynamisches Informationsangebot). So enthält der neue § 327f BGB (PDF) (Inkrafttreten am 01.01.2022) für Verbraucherverträge über digitale Produkte die Verpflichtung, während der Nutzungsdauer Aktualisierungen, die zum Erhalt der Vertragsmäßigkeit des digitalen Produkts erforderlich sind, bereitzustellen und den Verbraucher hierüber zu informieren. Zu den Aktualisierungen zählen auch Sicherheitsupdates. Die Vorschrift dient der Umsetzung der EU-Richtlinie 2019/770 über "bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen" (kurz: Digitale-Dienste-Richtlinie). Die Dauer der Updatepflicht richtet sich bei einer dauerhaften Bereitstellung von digitalen Produkten nach dem Bereitstellungszeitraum und in anderen Fällen nach der vernünftigen Verbrauchererwartung. Ob sich jedoch ein Wechselspiel zwischen dem freiwilligen IT-Sicherheitskennzeichen und den Pflichten für Unternehmen nach § 327f BGB ergibt, lässt sich zum jetzigen Zeitpunkt nicht abschließend beurteilen.

Da Unternehmen über das dynamische Informationsangebot auch auf bestehende Sicherheitsprobleme oder Sicherheitsupdates hinweisen und Handlungsempfehlungen aussprechen können, dürfte im Fall von

entsprechenden Informationen wenigstens von einer Indizwirkung für die Erfüllung von § 327f BGB zugunsten des Unternehmens auszugehen sein. Eine vergleichbare Indizwirkung könnte dem IT-Sicherheitskennzeichen darüber hinaus bei der Erfüllung der datenschutzrechtlichen Anforderungen an die IT-Sicherheit aus Art. 32 DSGVO, die auch für Hersteller von Bedeutung sind, zukommen. Der Trend, dass sich die Datenschutzaufsichtsbehörden bei Fragestellungen zur IT-Sicherheit stark an den Vorgaben des BSI orientieren, könnte damit weiter verstärkt werden.

[August 2021]

Unternehmenskontakt: Melanie Schaumann I Head of Marketing & Communications I T > +49 30 / 2332895 0 I E melanie.schaumann@reuschlaw.de