



Bundesamt für Sicherheit in der Informationstechnik

Bekanntmachung der Allgemeinverfügung zur Einführung von Produktkategorien des freiwilligen IT-Sicherheitskennzeichens

Vom 22. Februar 2024

Gemäß § 9c Absatz 5 Satz 1 Nummer 1 des BSI-Gesetzes (BSIG) gibt das Bundesamt für Sicherheit in der Informationstechnik Produktkategorien per Allgemeinverfügung im Bundesanzeiger öffentlich bekannt, innerhalb derer das freiwillige IT-Sicherheitskennzeichen vergeben wird.

Hierzu erlässt das Bundesamt für Sicherheit in der Informationstechnik folgende

ALLGEMEINVERFÜGUNG

1. Die Kategorie „Videokonferenzdienste“ wird als zusätzliche Produktkategorie des freiwilligen IT-Sicherheitskennzeichens festgelegt.
2. Es wird von Amts wegen festgestellt, dass die DIN SPEC 27008 zur Nutzung mit dem IT-Sicherheitskennzeichen geeignet ist.
3. Für die zu Tenorpunkt 1 genannte Produktkategorie wird eine Laufzeit von vier Jahren ab Erteilung der Freigabe zur Nutzung des IT-Sicherheitskennzeichens festgelegt.

I.

Begründung

Zu Tenor 1.

1. Zur Information von Verbraucherinnen und Verbrauchern über die IT-Sicherheit von Produkten und Diensten des Verbrauchermarktes erteilt das Bundesamt für Sicherheit in der Informationstechnik auf Antrag ein freiwilliges IT-Sicherheitskennzeichen. Zu diesem Zweck werden Produktkategorien festgelegt, innerhalb derer Produkten die Freigabe zur Nutzung des IT-Sicherheitskennzeichens erteilt werden kann.

Eine solche Produktkategorie erfasst eine Gruppe von vergleichbaren informationstechnischen Produkten in einem eingrenzenden Bereich, vorliegend dem Bereich „Videokonferenzdienste“.

2. Die Festlegung der genannten Produktkategorie, für die das Bundesamt für Sicherheit in der Informationstechnik gemäß § 9c Absatz 1 BSIG zuständig ist, erfolgt auf Grundlage der §§ 9c Absatz 1 und 5 Nummer 1, 10 Absatz 3 BSIG in Verbindung mit § 11 der BSI-IT-Sicherheitskennzeichenverordnung (BSI-ITSiKV). Demnach legt das Bundesamt für Sicherheit in der Informationstechnik die Produktkategorien fest, für deren Produkte es die Freigabe des IT-Sicherheitskennzeichens erteilt.
3. Die vorliegende Allgemeinverfügung eröffnet die Antragstellung und Erteilung von IT-Sicherheitskennzeichen für „Videokonferenzdienste“. Erfasst sind damit für die Verwendung durch Verbraucherinnen und Verbraucher bestimmte
 - a) Dienste, die Verbraucherinnen und Verbrauchern einen zeitgleichen, interaktiven und wechselseitigen Informationsaustausch räumlich voneinander getrennter Gesprächspartner über Audio- und Videokanäle ermöglichen.
 - b) Sie können zusätzliche Funktionen, beispielsweise zur Übertragung von Bildschirmhalten, Dateien oder dem Nachrichtenaustausch in Echtzeit umfassen, dürfen diese aber nicht zum Hauptbestimmungszweck haben.
 - c) Ausdrücklich nicht erfasst sind Raumsysteme, Peripheriegeräte und ähnliche Hardwareprodukte für die Durchführung von Videokonferenzen.

4. Mangels gesetzlicher Eingrenzung entscheidet das Bundesamt für Sicherheit in der Informationstechnik nach eigenem Ermessen über die Auswahl relevanter Produktkategorien des IT-Sicherheitskennzeichens (vergleiche BT-Drucksache 19/26106, Seite 87). Ausgehend von dem gesetzgeberischen Ziel, die IT-Sicherheit von verschiedenen Verbraucherprodukten im IT-Bereich verständlich, transparent, einheitlich und aktuell darzustellen, leiten sich die maßgeblichen Aspekte für die Einführung neuer Produktkategorien ab. Entscheidungserhebliche Faktoren sind demnach unter anderem das Risiko- und Schutzpotenzial einer Produktgruppe, deren Marktdurchdringung und Verfügbarkeit am Verbrauchermarkt sowie das Vorliegen einschlägiger und geeigneter IT-Sicherheitsvorgaben.

Vor dem Hintergrund erscheint die Einführung der genannten Produktkategorie geeignet, zielführend und geboten. Videokonferenzen ermöglichen eine ortsunabhängige Echtzeitkommunikation für Verbraucherinnen und Verbraucher. Dies fördert soziale Verbindungen und ermöglicht die Pflege von Kontakten, was besonders in Zeiten von



räumlicher Trennung oder sozialer Distanzierung zu einer deutlich gestiegenen Marktdurchdringung geführt hat. Videokonferenzen haben sich zudem als unverzichtbares Werkzeug im Bildungsbereich etabliert.

Die Verbesserung des Security-Designs von Videokonferenzdiensten ermöglicht einen besseren Schutz der Verbraucherinnen und Verbraucher vor Cyber-Risiken. Die hier benannte Produktkategorie ist dabei mit einem besonderen Schadpotenzial verbunden, da Videokonferenzen oft sensible Informationen und persönliche Gespräche beinhalten. Videokonferenzdienste verarbeiten und übertragen Daten in Echtzeit. Eine unzureichende IT-Sicherheit könnte zu Datenlecks führen, bei denen Informationen unberechtigten Dritten zugänglich werden. Dies betrifft nicht nur die Videoinhalte, sondern auch Nutzerdaten, Anmeldedaten und andere sensible Informationen. Eine robuste IT-Sicherheit schützt die Privatsphäre der Benutzenden und stellt sicher, dass solche Informationen nicht gefährdet werden. Videokonferenzdienste können zudem das Ziel von Cyberangriffen sein, beispielsweise durch Distributed Denial of Service (DDoS)-Angriffe, Phishing-Versuche oder andere Arten von Malware. Eine gefestigte Sicherheitsinfrastruktur kann solche Angriffe erkennen, abwehren und im Falle eines erfolgreichen Angriffs angemessen darauf reagieren.

Zu Tenor 2.

- Um dies zu gewährleisten liegt mit der DIN SPEC 27008 bereits eine branchenabgestimmte IT-Sicherheitsvorgabe vor, deren Geeignetheit das BSI nach § 9c Absatz 3 Satz 1 BSIG in Verbindung mit § 10 Absatz 1 BSI-ITSiKV hiermit von Amts wegen feststellt. Die DIN-Spezifikation betrachtet die zugrunde liegende IT-Infrastruktur von Videokonferenzdiensten, insbesondere Software- und Hardwarekomponenten für den Aufbau, die Aufrechterhaltung und das Schließen des Kommunikationskanals zwischen den Konferenzteilnehmenden. Dazu gehören auch alle Software- und Hardwarekomponenten, die die Erzeugung, den Austausch, die Speicherung und die Rotation der Verschlüsselungsschlüssel gewährleisten, die zur Implementierung der sicheren Kommunikationskanäle benötigt werden. Die DIN SPEC 27008 ist damit geeignet, die gesetzlichen Anforderungen insbesondere im Hinblick auf Vertraulichkeit, Verfügbarkeit und Integrität der Benutzerdaten zu gewährleisten und mithin die Basisanforderungen für die Erteilung eines IT-Sicherheitskennzeichens abzubilden.
- Die verbindlichen Sicherheitsanforderungen der Produktkategorie werden gemäß § 11 Absatz 3 BSI-ITSiKV auf der Internetseite des Bundesamts für Sicherheit in der Informationstechnik veröffentlicht.

Zu Tenor 3.

- Die Festlegung der abweichenden Laufzeit der Allgemeinverfügung erfolgt auf Grundlage des § 10 Absatz 3 BSIG in Verbindung mit § 8 Absatz 1 Satz 3 BSI-ITSiKV. Demnach kann das BSI eine von der regelmäßigen Laufzeit (zwei Jahre) abweichende Laufzeit für Produktkategorien festlegen.

Anders als physische Geräte unterliegen Dienste in der Regel keinen absehbaren oder festen Produktlebenszyklen. Sie werden regelmäßig fortlaufend mit Updates versorgt, ohne dass sich die ursprüngliche Sicherheitsarchitektur grundlegend verändert. Mithin dürfen Verbraucherinnen und Verbraucher von vornherein von einer längeren Lebensdauer eines Dienstes ausgehen. Vor dem Hintergrund erscheint die Festlegung einer vom ordnungsgeberischen Regelfall abweichenden Laufzeit angemessen.

II.

Bekanntgabe

Diese Allgemeinverfügung wird mit Bekanntgabe wirksam und gilt an dem auf die Veröffentlichung im Bundesanzeiger folgenden Tag als bekanntgegeben, § 41 Absatz 4 Satz 4 Verwaltungsverfahrensgesetz.

III.

Rechtsbehelfsbelehrung

Gegen diese Allgemeinverfügung kann innerhalb eines Monats nach Bekanntgabe Widerspruch beim Bundesamt für Sicherheit in der Informationstechnik, Godesberger Allee 185 – 189, 53175 Bonn erhoben werden.

Bonn, den 22. Februar 2024

Bundesamt
für Sicherheit in der Informationstechnik

Im Auftrag
Sandro Amendola