FACHBEREICH
SICHERHEIT – SCHUTZ
UND ZUVERLÄSSIGKEIT

Berlin, 14. Mai 2021

Stellungnahme

des Fachbereichs Sicherheit – Schutz und Zuverlässigkeit – der Gesellschaft für Informatik e.V.

zum Referentenentwurf der zweiten Verordnung zur Änderung der BSI-Kritisverordnung

des Bundesministeriums des Inneren, für Bau und Heimat (BMI)

Ansprechpartner und Autor:
Bernhard C. Witt, Sprecher des GI-Fachbereichs „SICHERHEIT“, bcwitt@it-sec.de

Einleitung

Mit Schriftsatz vom 26. April 2021 hat das Bundesministerium des Inneren, für Bau und Heimat insbesondere Vertreter der Wissenschaft nach § 10 Absatz 1 Satz 1 BSIG dazu aufgerufen, Stellungnahmen zum Entwurf einer zweiten Verordnung zur Änderung der BSI-Kritisverordnung per Mail an CI3@bmi.bund.de einzureichen. Darin enthaltende personenbezogene Daten bedürfen einer Einwilligung der betroffenen Personen, die im Rahmen der Stellungnahme nachzuweisen sind.
Der Fachbereich Sicherheit – Schutz und Zuverlässigkeit – der Gesellschaft für Informatik e.V. nimmt diese Gelegenheit gerne wahr und nimmt zu dem Referentenentwurf vor allem zu geplanten Änderungen von § 1 und von Anhang 4 (Sektor Informationstechnik und Telekommunikation) Stellung und willigt hiermit ausdrücklich ein, dass diese Stellungnahme als auch die darin enthaltenen personenbezogenen Kontaktdaten des Sprechers veröffentlicht werden dürfen.

Zu § 1 Begriffsbestimmungen

Neu aufgenommen werden soll als Bestandteil der im KRITIS-Kontext zu betrachtenden Anlagen „Software und IT-Dienste, die für die Erbringung einer kritischen Dienstleistung notwendig sind“.
Der GI-Fachbereich Sicherheit begrüßt die Klarstellung, dass betriebsnotwendige IT-Systeme ausdrücklich Bestandteil der Anlage zur Erbringung einer kritischen Dienstleistung sind.
Allerdings sind aus Sicht des GI-Fachbereichs Sicherheit bei dieser Definition gleich mehrere Punkte nachschärfenswert:

1. Die Bezeichnung „Software und IT-Dienste“ ist unterspezifiziert und steht aus Sicht des GI-Fachbereichs Sicherheit nicht in unmittelbarem und begrifflich eindeutigem Sachzusammenhang mit den Legaldefinitionen aus dem BSIG: Dort sind dagegen IT-Systeme und IT-Komponenten gesetzlich normiert, nicht aber Software und IT-Dienste. Die Neufassung der BSI-KritisV bringt insoweit keine begriffliche Klarheit. Der GI-Fachbereich Sicherheit empfiehlt daher an dieser Stelle, „Software und IT-Dienste“ durch „IT-Systeme“ aus Gründen der Konsistenz mit dem BSIG zu ersetzen, da dieser Begriff als ausreichend trennscharf angesehen werden kann und den inneren Sachzusammenhang zugleich besser abbildet als durch ergänzende Hinzuziehung von IT-Komponenten, die i.d.R. sehr kleinteilig ausfallen und insoweit den Blick auf das Wesentliche verstellen würden. Ein IT-System besteht wiederum aus verschiedenen, miteinander kombinierten Bestandteilen, inkl. der auf der eingesetzten Hardware aufgespielten Betriebssoftware und der fachlichen Applikation bzw. den bereitgestellten IT-Diensten. Nur der Begriff „IT-System“ befindet sich insoweit auf gleicher Begriffshöhe wie Betriebsstätten (sprich der Räumlichkeiten) und Maschinen/Geräte bzw. oftsveränderliche Einrichtungen (sprich der Hardware), die in den anderen beiden Bestandteilen aus der Begriffsbestimmung zu „Anlagen“ bereits ausdrücklich bestimmt sind.

2. In der bisherigen Fassung ist unklar, ob diese „Software und IT-Dienste“ bzw. wie vom GI-Fachbereich Sicherheit vorgeschlagen „IT-Systeme“ dann nur unmittelbar oder sogar auch mittelbar für die Erbringung einer kritischen Dienstleistung notwendig sein sollen. Aus Sicht des GI-Fachbereichs Sicherheit sollte dies daher präzisiert werden. Als betriebsnotwendig gehören aus Sicht des GI-Fachbereichs Sicherheit sowohl die eigentlichen zur Funktionsfähigkeit der kritischen Dienstleistung eingesetzten IT-Systeme als auch die zugehörigen sicherheitstechnischen IT-Systeme (z.B. zur Netzwerksegmentierung, zur Anomalie- bzw. Angriffserkennung, zur Datensicherung und -wiederherstellung, zur Verwaltung relevanter Changes, etc.). Daher empfiehlt der GI-Fachbereich Sicherheit „notwendig sind“ zu ersetzen durch „unmittelbar notwendig sind (inkl. der zu deren Absicherung zugehörigen sicherheitstechnischen IT-Systeme)“.
3. Generell sollte aus Sicht des GI-Fachbereichs Sicherheit aufgrund der zusätzlichen Integration von „Software und IT-Dienste“ bzw. wie vom GI-Fachbereich Sicherheit vorgeschlagen „IT-Systeme“ in der Begriffsbestimmung anschließend im Anhang der Terminus „Anlage oder System“ bzw. „Anlage oder IT-System“ vereinfacht werden, da der zweite Bestandteil infolge der Erweiterung der Begriffsbestimmung nunmehr als entbehrlich angesehen wird.

Zu Anhang 4: Anlagenkategorien und Schwellenwerte im Sektor Informationstechnik und Telekommunikation

Im Referentenentwurf soll in Teil 3, Ziffer 2.2.1, Serverfarm (Hosting), neu „für Nutzer“ eingefügt werden.

Aus Sicht des GI-Fachbereichs Sicherheit ist dieser Terminus jedoch unterspezifiziert, da insbesondere auch administrative und sogar systemtechnische Funktionsuser als „Nutzer“ einzuordnen sind. Der GI-Fachbereich Sicherheit empfiehlt an dieser Stelle, den Begriff „Nutzer“ durch „Endnutzer“ zu ersetzen.

Grundsätzlich begrüßt der GI-Fachbereich Sicherheit jedoch, dass an dieser Stelle die Schwellenwerte gemäß Referentenentwurf heruntergesetzt werden sollen, da aus seiner Sicht die bestehenden Schwellenwerte (im Übrigen auch in anderen Sektoren) als zu starr und nicht ausreichend Sektorspezifika berücksichtigend angesehen werden. Aus Sicht des GI-Fachbereichs Sicherheit sind diese teilweise zu hoch und teilweise zu niedrig. Der GI-Fachbereich Sicherheit empfiehlt hier eine Überprüfung der jeweils berechneten Schwellenwerte, gibt aber selbst keine konkrete Empfehlung zur Anpassung einzelner Schwellenwerte an, da dies trotz seiner hohen Querschnittsfunktion nicht zur fachlichen Kernkompetenz des GI-Fachbereichs Sicherheit gehört, ermuntert aber andere Fachgesellschaften zu einer entsprechenden Kommentierung (ggf. dann auf Basis des zwischenzeitlich verabschiedeten IT-Sicherheitsgesetzes 2.0). Hierzu könnten auch die Erfahrungen über eingetretene Störungen aus den letzten Jahren geeignet einfließen.

Über den Fachbereich Sicherheit – Schutz und Zuverlässigkeit – der Gesellschaft für Informatik e.V.

Der GI-Fachbereich "Sicherheit -Schutz und Zuverlässigkeit" wurde im Februar 2002 gegründet und vernetzt zwei "Communities" miteinander: Während die „Safety-Community“ vor allem den Schutz der Umwelt vor IT-Systemen (beispielsweise Sicherheit des Menschen vor schwerwiegenden Systemfehlern in Flugzeugen, Kernreaktoren und Kraftwerken) sowie Fehlertoleranzmaßnahmen (z.B. Systemausfälle als Folge von Ermüdungserscheinungen, Softwarefehlern und Naturereignissen) im Blick hat, beschäftigt sich die „Security-Community“ hauptsächlich mit dem Schutz der IT-Systeme und ihrer Umgebung vor Bedrohungen von außen, insbesondere vor Gefahren, die von bösartigen Angriffen (durch Menschen) ausgehen. Der Fachbereich bietet ein Forum, in dem alle auf dem Gebiet der Sicherheit informationstechnischer Systeme arbeitenden Menschen ihr Fachthema, organisiert in Fachgruppen, wiederfinden. Neben der rein wissenschaftlichen Arbeit ermöglicht der Fachbereich einen fachlichen Austausch zwischen Wissenschaft und Praxis. Mehr Information über den Fachbereich Sicherheit der GI kann der Webseite https://fb-sicherheit.gi.de/ entnommen werden.

Über die Gesellschaft für Informatik e.V.

Die Gesellschaft für Informatik e.V. (GI) ist mit rund 20.000 persönlichen und 250 korporativen Mitgliedern die größte und wichtigste Fachgesellschaft für Informatik im deutschsprachigen Raum und vertritt seit 1969 die Interessen der Informatikerinnen und Informatiker in Wissenschaft, Wirtschaft, öffentlicher Verwaltung, Gesellschaft und Politik. 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.