GESELLSCHAFT
FÜR INFORMATIK

Berlin, 24. August 2023

Stellungnahme

der Gesellschaft für Informatik e. V. (GI)

zum Referentenentwurf eines Gesetzes zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen (KRITIS-Dachgesetz – KRITIS-DachG) vom 27. Juli 2023

Mit dem Schreiben vom 27. Juli 2023 hat das Bundesministerium des Innern und für Heimat den aktuellen Referentenentwurf zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen (KRITIS-Dachgesetz – KRITIS-DachG) versandt. Mit der CER-Richtlinie wurde ein einheitlicher europäischer Rechtsrahmen für die Stärkung der Resilienz kritischer Einrichtungen gegen Gefahren auch außerhalb des Schutzes der IT-Sicherheit im Binnenmarkt geschaffen. Das Ziel soll sein, einheitliche Mindestverpflichtungen für Betreiber kritischer Anlagen festzulegen und deren Umsetzung durch kohärente, gezielte Unterstützungs- und Aufsichtsmaßnahmen zu garantieren.

Zum vorliegenden Entwurf bezieht die Gesellschaft für Informatik (GI) im Folgenden Stellung. Anzumerken ist, dass der Entwurf noch nicht vollständig ist. Abschnitte zu Bußgeld, zu den Kosten und zum Erfüllungsaufwand fehlen.

Es ist zu begrüßen, dass der Entwurf des KRITIS-DachG parallel mit dem Referentenentwurf des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes (NIS2UmsuCG) entsteht. Wichtig wäre aus Sicht der GI, dass die Aktivitäten bzw. Arbeiten an den Gesetzen nicht nur zeitlich, sondern auch inhaltlich aufeinander abgestimmt sind.

Aus Sicht der GI muss insbesondere die Position des Bundesamtes für Sicherheit in der Informationstechnik (BSI) anerkannt und gestärkt werden. Dazu spricht die GI die folgende Kernempfehlung aus:

> Das BSI muss als zentrale Meldestelle für IT-Sicherheitsschwachstellen und -vorfälle gestärkt werden. Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) sollte an relevanten Schnittstellen einbezogen werden, um die CER-Richtlinie abzudecken.

Die folgenden Bemerkungen und Handlungsempfehlungen sollen dabei helfen, gemeinsame Nenner mit bestehender Regulierung zu identifizieren, das KRITIS-DachG zu vereinfachen und die Regulierung zu vereinheitlichen. Das übergeordnete Ziel ist eine für die Anbieter und die Zivilgesellschaft transparente, nachvollziehbare und prüfbare Grundlage für mehr Sicherheit und Resilienz.

Zu B. Besonderer Teil – zu § 1 (Zweck des Gesetzes), Absatz 3, S. 30

„Zudem wird erstmalig ergänzend zu den bereits existierenden Regelungen zum Cyberschutz von Kritischen Infrastrukturen im BSIG sowie in der BSI-Kritisverordnung, die die Gewährleistung der IT-Sicherheit bezwecken, ein All-Gefahrenansatz zugrunde gelegt, der alle über die Gefahren von Cyberangriffen hinausgehende Gefahren, von Naturkatastrophen bis hin zu von Menschen gemachten Gefahren, mit dem Ziel der Sicherstellung der Arbeitsfähigkeit der Wirtschaft berücksichtigt."

Eine „erstmalige" Zugrundelegung von entsprechenden Regelungen zum Cyberschutz von Kritischen Infrastrukturen trifft nicht zu. Beispielsweise existieren gemäß § 8 BSIG Meldepflichten für IT-Sicherheitsvorfälle, die ursächlich nicht ausschließlich auf Cyberangriffe zurückzuführen sind. Der sogenannte All-Gefahrenansatz ist durch die Meldepflichten gemäß BSIG bereits gedeckt.

Statt unnötig neue Regelungen und Strukturen zu schaffen, sollten bestehende Regelungen und Strukturen um das BSI genutzt werden. Dazu gehört die Erweiterung der Kapazitäten des BSI im Bereich der Meldung von Schwachstellen, auch außerhalb des Behörden- und Verwaltungsumfelds[1]. Es sollten außerdem, zwecks Erfüllung der Anforderungen aus der CER-Richtlinie, relevante Schnittstellen (bspw. zum BBK) aufgebaut werden – statt mit dem KRITIS-DachG eine weitere Meldestelle beim BBK zu errichten.

Zu § 1 - Zweck des Gesetzes sowie ad § 2 – Begriffsbestimmungen

„Dieses Gesetz legt Kriterien zur Identifizierung kritischer Anlagen und Verpflichtungen für Betreiber kritischer Anlagen fest […]"

Der Grundstein der KRITIS-Regulierung in Deutschland ist das BSI-Gesetz (BSIG), das im Jahr 2015 durch das IT-Sicherheitsgesetz und zuletzt im Jahr 2021 durch das IT-Sicherheitsgesetz 2.0 (ITSiG 2.0) konkretisiert und erweitert wurde. In diesem werden bereits viele für das KRITIS-DachG relevante Begriffe definiert.

Das BSIG reguliert die Sicherheit Kritischer Infrastrukturen (KRITIS) und legt Pflichten, Aufgaben und Befugnisse von KRITIS-Betreibern fest. Zu diesem Zweck werden im BSIG Grundbegriffe wie „Kritische Infrastrukturen" oder „Betreiber Kritischer Infrastrukturen" festgelegt. Gemäß § 2 Nr. 10 BSIG werden Kritische Infrastrukturen definiert und durch die Rechtsverordnung nach § 10 Absatz 1 BSIG (BSI-Kritisverordnung) konkretisiert (z. B. Schwellenwerte vorgegeben). Eine Ausnahme bilden Betreiber von Energieversorgungsnetzen und von Energieanlagen, für die entsprechende Pflichten gemäß EnWG und unabhängig von den in der BSI-KritisVO genannten Schwellenwerten gelten.

1 https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/Unternehmen/unternehmen.html?nn=133680&cms_pos=5

So wird beispielsweise im Telekommunikationsgesetz (TKG) auf eine wiederholte Definition von relevanten KRITIS-Begriffen verzichtet und auf die Definition im BSIG (bspw. „kritische Komponenten“ im § 2 Nr. 13 des BSI-Gesetzes) verwiesen.

Es ist weder zweckmäßig noch transparent, Begriffe wie „Kritische Infrastrukturen“ oder „Betreiber kritischer Anlagen“ im KRITIS-DachG erneut zu definieren, auch dann nicht, wenn es sich dabei (wie im Hinweis zu § 2 Nr. 10 erläutert) um ein Copy-and-Paste-Verfahren handelt („*Die nachfolgenden Begriffsbestimmungen dienen der Umsetzung der NIS-2-Richtlinie und sind dem Referentenentwurf des BMI für ein NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz entnommen.*“).

Es sollte und muss spezifiziert werden, welchen Weg der Gesetzgeber bei der Definition beschreiten möchte. Dazu müssen die notwendigen Schritte zur Vereinheitlichung des Definitorischen parallel (nicht nachgelagert) zum KRITIS-DachG eingeleitet werden. Diesbezüglich gibt es zwei Optionen:

Option 1: Das BSIG kann als Grundstein der KRITIS-Regulierung bestätigt werden, dabei kann man auf den darin (sowie in der BSI-KritisVO) enthaltenen Definition aufbauen. Dies macht lediglich eine Definition der bisher nicht vom BSIG erfassten Begriffe notwendig. Eine Änderung weiterer Gesetze und Verweise, wie etwa im TKG, ist dabei nicht notwendig.

Option 2: Die Begriffsbestimmungen ins KRITIS-DachG vollständig zu verlagern, bedeutet, relevante Abschnitte (Verweise und Definitionen) im BSIG, ITSiG 2.0, TKG und in einer Reihe weiterer relevanter Gesetze und Verordnungen zu entfernen und/oder anzupassen. Bedenkt man, wie viele Jahre das Auffinden und die Anpassung relevanter Gesetze nach dem Beschluss des ITSiG im Jahr 2015 in Anspruch genommen hatten, bedeutet dies einen erheblichen Aufwand.

Beide Optionen befriedigen den Anspruch gemäß Hinweis zu § 2 Nr. 10. („*Das KRITIS-DachG muss diese Begriffsbestimmungen enthalten, damit die Festlegung von Einrichtungsarten und Schwellenwerten nach BSI-Gesetz und Schwellenwerten nach KRITIS-DachG zukünftig in einer einzigen Rechtsverordnung (nach § 15 KRITIS-DachG) erfolgen kann.*“) Option 1 ist klar zu bevorzugen, um die Transparenz zu stärken und Aufwand zu sparen.

Zu § 15 – Ermächtigung zum Erlass von Rechtsverordnungen

„Das KRITIS-DachG muss diese Begriffsbestimmungen enthalten, damit die Festlegung von Einrichtungsarten und Schwellenwerten nach BSI-Gesetz und Schwellenwerten nach KRITIS-DachG zukünftig in einer einzigen Rechtsverordnung (nach § 15 KRITIS-DachG) erfolgen kann.“

Dieser Paragraf wäre dementsprechend anzupassen (beispielsweise durch BSI-KritisVO zu ersetzen).

Zu § 2 Nr. 6 – Begriffsbestimmungen sowie § 3 – Nationale zuständige Behörde für die Resilienz kritischer Anlagen

„[…] „Resilienz" die Fähigkeit des Betreibers einer kritischen Anlage, einen Vorfall zu verhindern, sich davor zu schützen, darauf zu reagieren, einen solchen abzuwehren, die Folgen eines solchen Vorfalls zu begrenzen, einen Vorfall aufzufangen, zu bewältigen und sich von einem solchen Vorfall zu erholen […]"

Im KRITIS-DachG fehlt die Definition weiterer relevanter Begriffe (wie „IT-Sicherheit", „Cybersicherheit", „IT-Notfall", „Notfall", „Krise" oder „Katastrophe", „Sicherheit", „Informationssicherheit" etc.) sowie ihre Abgrenzung zum Begriff „Resilienz". Durch deren Fehlen ist bisher nicht ersichtlich, warum das BBK und nicht das BSI – oder eine andere Behörde – die „nationale zuständige Behörde" für KRITIS-Resilienz sein sollte. Hierzu kann auf folgende bestehende Definitionen des BSI zur Unterscheidung von Störungen, Notfällen, Krisen und Katastrophen zurückgegriffen werden:

- Eine Störung ist dem Zustand vorenthalten, in dem Ressourcen einer Organisation nicht wie vorgesehen funktionieren und die dadurch entstehenden Schäden für die Unternehmen geringfügig sind.

- Ein Notfall tritt ein, wenn die Prozesse oder Ressourcen einer Institution nicht wie vorgesehen funktionieren und die Verfügbarkeit entsprechender Prozesse oder Ressourcen innerhalb einer geforderten Zeit wiederhergestellt werden kann. Der Geschäftsbetrieb wird im Notfall stark beeinträchtigt. Notfälle, welche die Kontinuität von Geschäftsprozessen beeinträchtigen, können eskalieren und sich zu einer Krise ausweiten.

- Unter einer Krise wird eine vom Normalzustand abweichende Situation verstanden, die trotz vorbeugender Maßnahmen eintreten, aber mit den üblichen Mitteln der Notfallbewältigung nicht bewältigt werden kann – und keine Auswirkungen auf das öffentliche Leben hat. Unter einer Krise wird dann ein verschärfter Notfall verstanden, bei dem die Existenz der Institution oder das Leben und die Gesundheit von Personen gefährdet sind.

- Die Bewältigung einer Katastrophe ist die Aufgabe des Katastrophenschutzes, der in Deutschland eine Aufgabe der Länder, die durch den Bund unterstützt und ergänzt werden, ist. Aus der Sicht einer Organisation allerdings stellt sich eine Katastrophe als Krise dar und wird intern durch die Notfallbewältigung der Institution in Zusammenarbeit mit den externen Hilfsorganisationen bewältigt.

Der Fokus des BBK liegt im Bevölkerungsschutz und in der Katastrophenhilfe – wobei eine „Katastrophe“ eine klar definierte und extreme Ausprägung des Begriffs „Vorfall“ gemäß § 2 Nr. 10 KRITIS-DachG darstellt. Ein Vorfall ist „*ein Ereignis, das die Erbringung einer kritischen Dienstleistung erheblich beeinträchtigt oder beeinträchtigen könnte*“ und somit noch keine Katastrophe. Laut KRITIS-DachG soll nun aber das für Bevölkerungsschutz und Katastrophenhilfe zuständige BBK für alle Formen der Vorfälle die „national zuständige Behörde“ werden.

Die Definitionen und Zuständigkeiten sollten auf Kompatibilität hin überprüft und ggf. angepasst werden, insbesondere die Kompatibilität der Zuständigkeiten der Behörden (Katastrophenhilfe) mit dem Wirkkreis des KRITIS-DachG (Resilienz, Vorfall).

Zu § 3 - Nationale zuständige Behörde für die Resilienz kritischer Anlagen, § 8 – Registrierung der kritischen Anlage sowie § 12 – Meldewesen für Störungen

Den Grundstein der KRITIS-Regulierung in Deutschland bildet das BSI-Gesetz (BSIG). § 8b BSIG definiert das BSI als zentrale Meldestelle für KRITIS-Betreiber. § 4 BSIG legt das BSI als zentrale Meldestelle für Bundesbehörden; § 4b BSIG als zentrale allgemeine Meldestelle für Sicherheit in der IT fest. Das BSI darf zur Abwehr von Gefahren Informationen sammeln und auswerten sowie sich mit anderen Behörden austauschen.

Anderslautend § 12 Abs. (1) ff. KRITIS-DachG:

„Betreiber kritischer Anlagen sind, unbeschadet anderer gesetzlicher Meldeverpflichtungen gegenüber zuständigen Behörden, verpflichtet, Vorfälle, die die Erbringung ihrer kritischen Dienstleistungen erheblich stören könnten, unverzüglich über ihre Kontaktstelle im Sinne von § 8 Absatz 3 an eine vom BBK im Einvernehmen mit dem BSI eingerichtete gemeinsame Meldestelle zu melden. Hierbei sind insbesondere Angaben zu Anzahl und Anteil der von der Störung betroffenen Nutzer, bisherige und voraussichtliche Dauer der Störung sowie das betroffene geografisches Gebiet der Störung, unter Berücksichtigung des Umstandes, ob das Gebiet geografisch isoliert ist, zu berücksichtigen.“

In den vergangenen Jahren wurde mit großem Aufwand ein deliberativer Prozess zwischen Behörden, dem Gesetzgeber, den KRITIS-Betreibern privatwirtschaftlicher Unternehmen und der Aufsicht erarbeitet. Aus diesen resultierte, dass nicht die BaFin oder die BNetzA als zentrale Meldestellen (parallel oder zusätzlich) zum BSI agieren, sondern dass das BSI diese Aufgabe übernimmt und diese Rolle inzwischen mit Erfolg ausfüllt. Entsprechend der CER-Richtlinie sollte es bei diesem Prozess belassen werden, statt die Akteure mit neuen Strukturen zu überfordern. Statt die Verantwortung an das BBK zu geben, ist eine Schnittstelle zu den bestehenden

Verfahren und Meldesystemen des BSI für die für das BBK interessanten und relevanten „Vorfälle“ hinreichend. Damit würden die Anforderungen der CER-Richtlinie erfüllt und zugleich der in den vergangenen Jahren erarbeitete Kompromiss gewürdigt werden.

Bei einer Neuregulierung der Meldepflichten für Sicherheitsvorfälle muss bedacht werden, dass die Umsetzung von Meldeprozessen, die Etablierung einer geeigneten Aufbau- und Ablauforganisation, die Freistellung kompetenter Ressourcen, die Definition der Zuständigkeiten und vieles mehr für die Organisationen einen nicht unerheblichen Aufwand bedeutet. Anders als zu Beginn des oben erläuterten Prozesses (2015) bestehen heute für alle Organisationen relevante Meldepflichten für sogenannte Data Breaches (gemäß Art. 33 DSGVO). Ein integrierter Ansatz wäre für meldepflichtige KRITIS-Betreiber und für Regulierer effektiver. Ein derartiger Ansatz sollte im KRITIS-DachG verankert werden.

Zu § 18 – Evaluierung

„Das Bundesministerium des Innern und für Heimat wird die Regelungen dieses Gesetzes regelmäßig, spätestens nach Ablauf von fünf Jahren nach Inkrafttreten des Gesetzes auf wissenschaftlich fundierter Grundlage evaluieren.“

Wissenschaftlich fundierte Kriterien sind wichtig, um die Wirksamkeit der bisherigen Regulierung des KRITIS-Bereichs (BSIG, TKG oder ITSiG 2.0) zu bewerten und zu beurteilen.

Sollte die Wirksamkeit der vorangehenden Regulierung negativ beurteilt werden, so muss im Rahmen einer Analyse eruiert werden, welche Ursachen dem Ergebnis zugrunde liegen, damit solche potenziellen Fehler im KRITIS-DachG oder NIS2UmsuCG vermieden werden können. Sollte die Wirksamkeit positiv bewertet werden und das Ziel von mehr Sicherheit für Bürger*innen mit der bestehenden Regulierung gut erreicht worden sein, so bestünde kein weiterer regulatorischer Handlungsbedarf. Mit den Worten von Charles Baron de Montesquieu ausgedrückt, sinngemäß: Wenn es nicht notwendig ist, ein Gesetz zu machen, dann ist es notwendig, kein Gesetz zu machen.

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.