GESELLSCHAFT
FÜR INFORMATIK

Berlin, 04. September 2025

Stellungnahme

der Gesellschaft für Informatik e. V. (GI)

zum Referentenentwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen vom 29. August 2025

GESELLSCHAFT
FÜR INFORMATIK

Mit dem Schreiben vom 29. August 2025 hat das Bundesministerium des Innern den aktuellen Referentenentwurf zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen (KRITIS-Dachgesetz – KRITIS-DachG) versandt. Mit der Richtlinie (EU) 2022/2557 (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.

Grundsätzliche Einschätzung

Die GI weist an diesem Punkt kritisch auf die sehr kurze Frist zur Stellungnahme hin. Eine Frist von vier Werktagen macht eine differenzierte Auseinandersetzung mit dem Referentenentwurf nahezu unmöglich. Wir verweisen auf unseren offenen Brief „Angemessene Fristen statt Scheinbeteiligung“[1], in dem wir uns bereits 2020 für angemessene Fristen zur Kommentierung von Gesetzentwürfen sowie eine bessere Informationsbereitstellung ausgesprochen hatten.

Die GI hatte zuletzt 2023 Stellung zum damaligen Referentenentwurf bezogen und die Entwicklung seitdem weiterverfolgt. Sie begrüßt, dass der KRITIS-DachG-Referentenentwurf auf den Referentenentwurf des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes (NIS2UmsuCG) verweist und sich inhaltlich mit diesem abstimmt.

Das übergeordnete Ziel der nationalen Umsetzung europäischer Vorgaben zu den KRITIS-Sektoren sei es, laut Bericht zur Cybersicherheit des Bundesrechnungshofes, mitunter „mehrfache Meldepflichten zu vermeiden und dem BSI zu einem vollständigen Lageüberblick zu verhelfen“ (Bericht Bundesrechnungshof 2025, S. 9)[2]. Die GI spricht sich nach wie vor für eine Stärkung der Position des Bundesamtes für Sicherheit in der Informationstechnik (BSI) aus, um eine Resilienz im digitalen Raum sicherzustellen. 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

[1] https://gi.de/meldung/offener-brief-ausreichende-fristen-fuer-verbaendebeteiligung
[2] https://www.politico.eu/wp-content/uploads/2025/07/02/88-Absatz-2-BHO-zur-Cybersicherheit.pdf

eine für die Anbieter und die Zivilgesellschaft transparente, nachvollziehbare und prüfbare Grundlage für mehr Sicherheit und Resilienz.

Kohärentes Meldewesen statt Doppelstrukturen (zu Begründung - A. Allgemeiner Teil, I. Zielsetzung, Absatz 2, S. 32)

Der Gesetzentwurf sieht vor, das KRITIS-Dachgesetz in Kohärenz mit dem BSI-Gesetz, dem NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz und der „DORA-Verordnung“ treten zu lassen (S. 32). Diese Gesetze befassen sich mit dem Schutz der IT-Sicherheit von KRITIS. Die GI begrüßt den Aufbau eines kohärenten Systems zum Schutz kritischer Anlagen und zur Umsetzung europarechtlicher Vorgaben.

Fehlende Begriffsbestimmungen (u.a. zu § 2 - Begriffsbestimmungen)

Bereits in der letzten Stellungnahme ging die GI darauf ein, dass viele für das KRITIS-DachG relevanten Begriffe bereits in vorangegangenen Gesetzen wie dem BSIG oder dem IT-Sicherheitsgesetz 2.0 (ITSiG 2.0) definiert wurden. 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 „Betreiber kritischer Anlagen“ im KRITIS-DachG erneut zu definieren. 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.

KRITIS-DachG in der Fassung vom 27.8.2025 spezifiziert außerdem „kritische Dienstleistungen“, indem das Spektrum um ausgewählte Bereiche der Daseinsvorsorge erweitert wird. Konkret heißt es im §2 Nr. 4: „[…] kritische Dienstleistung“ […] eine Dienstleistung zur Versorgung der Allgemeinheit in den Sektoren Energie, Transport und Verkehr, Finanzwesen, Leistungen der Sozialversicherung sowie Grundsicherung für Arbeitsuchende, Gesundheitswesen, Wasser, Ernährung, Informationstechnik und Telekommunikation, Weltraum oder Siedlungsabfallentsorgung, deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde“.

Die GI schlägt daher vor, das BSIG als Grundstein der KRITIS-Regulierung zu bestätigen. Dabei kann man auf die darin (sowie in der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV)) enthaltene 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.

Während das KRITIS-DachG Begriffe so doppelt definiert, 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 aus Sicht der GI weiterhin nicht verständlich, 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 GI spricht sich weiterhin dafür aus, die Definitionen und Zuständigkeiten auf Kompatibilität hin zu prüfen und ggf. anzupassen, insbesondere die Kompatibilität der Zuständigkeiten der Behörden (Katastrophenhilfe) mit dem Wirkkreis des KRITIS-DachG (Resilienz, Vorfall).

Zugang zu Resilienzstandards erleichtert (zu § 14 – branchenspezifische Resilienzstandards)

Positiv hervorzuheben ist die Entwicklung von branchenspezifischen Resilienzstandards in § 14 KRITIS-DachG. Diese sollen nach § 14 Abs. 2 Satz 5 auch durch die Betreiber kritischer Anlagen oder ihre Branchenverbände vorgeschlagen werden können. Der Entwurf sieht vor, dass diese auf der Internetseite des BBK kostenfrei zur Verfügung gestellt werden. Dies ist ein sinnvoller Schritt: Die Bereitstellung einer öffentlichen Leistung bedient ein öffentliches Interesse und darf daher nicht an zusätzliche Kosten gebunden sein.

BSI und BBK gemeinsam im Meldewesen integriert (zu § 18 – Meldewesen für Vorfälle)

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.

Die GI hatte zuletzt gefordert, das BSI als zentrale Meldestelle zu belassen und nicht das BBK hierfür einzusetzen. Wir begrüßen daher, dass der Referentenentwurf eine gemeinsame Meldestelle zwischen BSI und BBK vorsieht, und Vorfälle von dort aus an das BBK weitergegeben wurden. Die weitergehende Erklärung, damit „Behörden einen Überblick über die Vorfälle und mögliche Bedrohungen im gesamten Bundesgebiet zu ermöglichen“ und „diese Erkenntnisse […] dann in die nationalen Risikoanalysen und Risikobewertungen fließen [zu lassen]“ deckt sich mit unserer Forderung nach mehr transparenten und nachvollziehbaren Grundlagen für Risikoeinschätzungen.

Wir unterstützen zudem die vorgesehene Erweiterung des Online-Meldeportals des BSI für Störungen, „die den physischen Schutz von Betreibern kritischer Anlagen betreffen“. Physische Schäden und IT-Schäden gehen in vielen Fällen miteinander einher, sodass damit das Meldewesen effizienter gestaltet wird.

Wir regen an, diese Erweiterung nicht lediglich in der Begründung, sondern direkt im KRITIS-DachG unter § 18 fest zu verankern.

Darüber hinaus regen wir an, den Modus Operandi, i.e. „die Einzelheiten zur Ausgestaltung des Meldeverfahrens“ gemäß § 18 Abs. 2 nicht in einem gesonderten Verfahren und „unter Einvernehmen“ mit dem BSI, sondern direkt das Meldeverfahren des BSI inkl. Prozesse und Fristen, einzusetzen. Eine gesonderte Regelung schwächt die Erreichung des Ziels einer erheblichen Reduzierung des „Verwaltungsaufwandes sowohl für die beteiligten Behörden als auch der Betreiber“ (S. 69).

Die positive Entwicklung liegt dennoch noch unter den Erwartungen und Empfehlungen des Bundesrates bzgl. der Konsolidierung der Meldepflichten für Sicherheitsvorfälle mit den Meldepflichten für sog. Datenpannen (Data Breaches) gemäß DSGVO. Auch werden dadurch die Empfehlungen des Bundesrechnungshofes aus dem aktuellen Bericht zur Cybersicherheit nur teilweise berücksichtigt. Dort wird explizit eine „gemeinsame Datenbasis und ein einheitlicher strukturierter Datenaustausch“ zwischen BSI, BBK, BaFin und BNetzA für „eine effiziente bürokratiearme Zusammenarbeit“ gefordert (S.9). Konkret heißt es im Bericht: „Insgesamt muss [die Bundesregierung] die Arbeit von u. a. BSI, BBK, BaFin und BNetzA spätestens mit der Umsetzung der neuen europäischen Richtlinien besser strukturieren und koordinieren“ (S. 9)[3].

In der aktuellen Fassung des KRITIS-DachG ist diese Empfehlung noch nicht gewürdigt worden. § 18 Abs. 1 führt aus: „[…] Meldepflichten auf Grund sonstiger gesetzlicher Vorgaben bleiben unberührt“, bzw. „Die Störungsmeldung nach diesem Gesetz erfolgt unbeschadet anderer gesetzlicher Meldeverpflichtungen gegenüber weiteren zuständigen Behörden. Bereits bestehende Meldungsverpflichtungen der Betreiber gegenüber anderen Stellen, bleiben daher, sofern gegeben, bestehen. Eine unverzügliche und regelmäßige Weiterleitung der Meldung nach Absätze 1 und 2 an zuständige Behörden oder andere Behörden erfolgt nicht“ (S. 69, Begründung).

Evaluierung (zu § 25 – Evaluierung)

„Das Bundesministerium des Innern wird dieses Gesetz regelmäßig, erstmalig bis einschließlich 17. Oktober 2029 auf wissenschaftlich fundierter Grundlage evaluieren“ (§ 25 KRITIS-DachG, S. 28). Wissenschaftlich fundierte Kriterien sowie eine unabhängige Evaluierung 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

[3] https://www.politico.eu/wp-content/uploads/2025/07/02/88-Absatz-2-BHO-zur-Cybersicherheit.pdf

erreicht worden sein, sollte davon ausgegangen werden, dass vorerst kein weiterer regulatorischer Handlungsbedarf besteht.

Kontakt

Nina Locher
Senior Referentin Cybersicherheitspolitik
Gesellschaft für Informatik e.V. (GI)

Geschäftsstelle Berlin
Weydingerstraße 14-16
10178 Berlin

E-Mail: nina.locher@gi.de

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.