bitkom

Stellungnahme

Januar 2024

Bitkom zum KRITIS-DachG Referentenentwurf

Zusammenfassung

Grundsätzlich stellt der zweite Entwurf eine Verbesserung gegenüber seiner ursprünglichen Version dar. Wir begrüßen, dass es nun mit dem BBK eine zentrale Anlaufstelle für Unternehmen geben soll. Jedoch verweisen wir bei den Eckpunkten zum KRITIS-DachG sowie dem Positionspapier zum ersten Referentenentwurf vom August 2023. Insbesondere spricht sich der Bitkom deutlich für eine akzentuelle Änderung des Entwurfs aus, hin zu einem kooperativen, gemeinsamen Ansatz. Hier verweisen wir auf unsere Vorschläge aus vorherigen Positionspapieren, insb. die stärkere Einbindung der Wirtschaft & Einrichtung einer Sicherheitskommission.

Der vorliegende Referentenentwurf ist dem Ziel, größere Kohärenz und Vereinheitlichung der Fristen, Begrifflichkeiten, Prozesse etc. in KRITIS-DachG und NIS2UmsuCG ein Stück nähergekommen. Es sei denn noch einmal auf die Wichtigkeit verwiesen, hier möglichst große Einheitlichkeit und damit Überschaubarkeit und Vereinfachung für die betroffenen Unternehmen zu gewährleisten. Insgesamt bleibt es dabei, dass die Umsetzungsgesetze der CER- und der NIS2-Richtlinien nicht ausreichend aufeinander abgestimmt sind.

Zielsetzung

Das primäre Ziel des KRITIS-Dachgesetzes sollte sein, durch eine enge Zusammenarbeit zwischen Staat, Gesellschaft und Wirtschaft einen umfassenden und einheitlichen Schutz für die essenziellen Kritischen Infrastrukturen zu gewährleisten. Dieser Schutzschirm sollte sicherstellen, dass sicherheitsrelevante Vorfälle wie Sabotage, Terrorismus, Unfälle oder Naturkatastrophen lediglich zu kurzfristigen Störungen führen, jedoch nicht zu einem vollständigen und langanhaltenden Ausfall. Das KRITISDachgesetz sollte darauf abzielen, klare Zuständigkeiten zu definieren, Schutzpflichten zu harmonisieren, die Kooperation zwischen staatlichen Institutionen,

Wirtschaft und Gesellschaft in der Vorbeugung und im Ernstfall zu optimieren und hierfür umfassende Notfall- und Krisenmanagementverfahren einzuführen

Notwendige Klarheit und Kohärenz

Harmonisierung KRITIS-DachG und NIS2

Auch im neuen Entwurf gibt es Fragen zur Kohärenz, die eine sorgfältige Prüfung und mögliche Anpassung, auch im Zusammenspiel mit dem Nis2-UmsuCG. Die Überschneidungen beider Regulierungen müssen konsequent aneinander angeglichen werden. Schon der Begriff des KRITIS-Unternehmens ist an dieser Stelle irreführend und könnte als „wichtiges“ oder „besonders wichtiges“ Unternehmen referenziert werden.

Weiter gelten entsprechend der EU-rechtlichen Vorgaben gemäß § 4 Abs. 6 des Entwurfs die §§ 7-12 nicht für verschiedene Sektoren, zum Beispiel die Sektoren Informationstechnik und Telekommunikation. Übrig bleibt die Registrierungspflicht nach § 6 des Entwurfs. Diese findet sich aber bereits in der NIS2 sowie dem entsprechenden Umsetzungsgesetz. Die derzeitige teilweise Herausnahme aus dem Anwendungsbereich ist nicht unproblematisch. Es entstehen rechtliche Unklarheiten, die vermieden werden könnten. Zum Beispiel scheint die Überwachungspflicht des § 14 auch für den TK-Sektor zu gelten, obwohl eine Überwachung nach § 14 Abs. 1 den Vorgaben des § 10 erfolgen, der für TK-Unternehmen nicht anzuwenden ist. Gleiches gilt für § 16 Abs. 2: Diese Vorschrift enthält eine Verordnungsermächtigung zur Konkretisierung der Vorgaben des § 10, der keine Anwendung finden soll. Wir regen daher an, die Sektoren Informationstechnik und Telekommunikation aus dem Anwendungsbereich des KRITIS-Dachgesetz herauszunehmen.

Nach wie vor ist der Entwurf von begrifflichen Ungenauigkeiten geprägt. Während die CER- und die NIS-2-Richtlinie sich auf den Begriff „Einrichtungen“ fokussieren, stellt das KRITS-Dachgesetz auf „Anlagen“ ab (vgl. insb. § 4 Abs. 1). Darüber hinaus können nach § 4 Abs. 2 „weitere Betreiber“ festgelegt werden. Dieser terminologische Bruch im Gesetz ist nicht nachvollziehbar. Auch die Begriffsbestimmungen in Verbindung mit § 4 und § 16 ergeben in der derzeitigen Fassung keinen Sinn. Es sollten einheitlich und gesetzesübergreifend konsistent Betreiber kritischer Anlagen adressiert werden. Letztlich ist auch die Definition der kritischen Anlage in §2 sprachlich falsch verfasst (es müsste heißen: "eine Anlage, über die eine kritische Dienstleistung erbracht wird").

Risikobewertungen

Die in §9 eingeführten „*vertrauenswürdigen Informationsquellen*“ sind zu unbestimmt. Wir schlagen vor, diese durch „*...und andere, von ihnen als vertrauenswürdig eingeschätzte Informationsquellen*“ zu ersetzen.

Fokus der Bewertungen und Rechtsklarheit

Die Bewertungen sollen sich auf Risiken konzentrieren, die von den Anlagenbetreibern bewältigt werden können. Es bestehen Bedenken hinsichtlich der Einbeziehung von hybriden oder feindlichen Bedrohungen, da der Schutz vor solchen Risiken primär in den Verantwortungsbereich staatlicher Gewalt fällt. Die Forderung nach einer klaren Definition von »hybriden Bedrohungen oder anderen feindlichen Bedrohungen« (§ 9(1) und § 10(1)) wird erhoben, um Rechtsklarheit zu schaffen und Unsicherheiten zu beseitigen

Betroffene Sektoren

Das KRITIS-DachG wird keine sektoren- oder gar branchenspezifischen Regelungen treffen, sondern abstrakt vorgeben, dass in allen KRITIS-Sektoren geeignete und verhältnismäßige Maßnahmen zum physischen Schutz kritischer Anlagen zu treffen sind. Die umsetzungsorientierte Unterstützung der Betreiber ist mit Blick auf den Umsetzungsaufwand bis 2026 hierbei erfolgsentscheidend, ebenso wie eine schnellstmögliche Arbeits- und Lieferfähigkeit des BBKs (insb. bei Vorgaben der Risikobewertung und Resilienzpläne). Hier bleibt das Gesetz aber zu vage – so ist unklar, ob die bereitgestellten Vorlagen, Muster und Leitlinien durch das BBK für die Unternehmen verbindlich sind. Sollte das Gegenteil der Fall sein, kann hierauf im Sinne der Ressourcenschonung verzichtet werden.

Zur Vereinheitlichung und Spezifizierung der Anforderungen ist die Beibehaltung und teilweise Neuentwicklung von branchenspezifischen Standards (neben den horizontal wirkenden Standards) für die Umsetzung innerhalb und zwischen den Sektoren wichtig.

Darüber hinaus erscheint die in § 4 enthaltene Sektorenbezeichnung unvollständig oder unpräzise. Z.B. ist das "Bankwesen" nicht enthalten, obwohl in § 4 Abs. 6 eine Rückausnahme enthalten ist. Auch der "Digitalsektor" wird in der Gesetzesbegründung häufiger erwähnt, wird aber in § 4 Abs. 1 nicht genannt.

Erfüllungsaufwände

In den aufgeführten Erfüllungsaufwänden fehlt eine Angabe von Aufwänden für die Wirtschaft. Solange diese Aufwände nicht benannt werden können, sollte aus Sicht des Bitkom das Gesetz nicht in ein parlamentarisches Verfahren überwiesen werden. Es gilt hier, die finanziellen Auswirkungen auf betroffene Unternehmen abschätzen zu können und so das Gesetz auf seine Effizienz zu überprüfen. Als Kompromiss sprechen wir uns dafür aus, weitestgehend auf die Verlagerung von Regelungen in Rechtsverordnungen zu verzichten und diese im Gesetz direkt vorzunehmen. Somit wäre dann eine Abschätzung der Erfüllungsaufwände seriös darstellbar.

In diesem Kontext fordern wir auch eine Anpassung des Punktes F „Weitere Kosten“. Investitionen und Kosten der Wirtschaft für eine Erhöhung der Resilienz und Sicherheit sollten umlagefähig auf die Produkte und Dienstleistungen der betroffenen Unternehmen sein. Die bisherige Formulierung suggeriert, dass eine Erhöhung der Resilienz und Sicherheit keine Kosten verursacht.

KRITIS-Resilienzstrategie

Die Vorlage einer Nationalen KRITIS-Resilienzstrategie für Januar 2026 sehen wir als deutlich zu spät an. Eine solche Strategie sollte vor Festlegung von Regulatorischen Verpflichtungen für KRITIS Betreiber vorliegen. Daher spricht sich der Bitkom für die Erstellung einer KRITIS-Resilienzstrategie bis Sommer 2024 aus.

Um möglichst frühzeitig Klarheit und Planungssicherheit für die betroffenen Unternehmen zu schaffen, sollte außerdem auf Rechtsverordnungen weitestgehend verzichtet und die zentralen Regelungen bereits im Gesetz verankert werden.

Schulungen von Geschäftsleitern

Art. 14 nutzt die Begrifflichkeit des Geschäftsleiters anstelle des Geschäftsführers. Wir fordern hier eine Klarstellung, warum explizit nur die Geschäftsleitung genannt wird. Darüber hinaus ist zu überprüfen, inwiefern Art. 14 einen Eingriff in die Berufsfreiheit von Geschäftsleitern (Abs. 2) sowie in deutsches Haftungsrecht (Abs. 1) darstellt. Der Ausschluss eines Verzichts der Gesellschafter gegenüber der Geschäftsleitung ist nicht nachvollziehbar. Wir plädieren daher dafür, Art. 14 ersatzlos zu streichen.

Registrierungs- und Meldewesen

Zuständigkeiten

§3 des Entwurfs benennt das BBK als zentrale Anlaufstelle, §12 normiert eine gemeinsame Meldestelle von BBK und BSI. Allerdings werden in §3 weitere Bundes- und Länderbehörden, zudem in §7 die EU-Kommission als Adressaten von Meldungen bzw. Ersteller weiterer Anforderungen an kritische Anlagen/Erbringer kritischer Dienstleistungen genannt. Hier muss unbedingt sichergestellt werden, dass betroffene Unternehmen Meldungen an eine oder möglichst wenige Stellen und auf Basis einheitlicher Kriterien machen müssen – und bspw. nicht mit 16 unterschiedlichen, länderspezifischen Auslegungen einer Bundesregelung konfrontiert werden. Insbesondere für länderübergreifend tätige Unternehmen ist dies äußerst relevant. Wir weisen dringend darauf hin, dass einer drohenden Zersplitterung in Bundes- und Länderzuständigkeiten entgegengewirkt werden muss und sprechen uns für die Schaffung einer zentralen Stelle zur Harmonisierung und Koordinierung der den Ländern zustehenden Regelungsbereiche aus.

Dabei spielt auch ein medienbruchfreies Registrierungs- und Meldeportal eine wichtige Rolle. Das bedeutet, dass Meldungen digital eingereicht und automatisch die Bearbeitung durch die zuständige Behörde gewährleistet wird, ohne das weitere zutun des Unternehmens.

Meldepflichten

Die Formulierung in §12, Abs. 1 und 2., dass Vorfälle gemeldet werden müssen, die „erheblich stören könnten“ kann in der praktischen Abgrenzung erhebliche Probleme

bereiten. Wenn Vorfälle, die stören können, es aber letztendlich nicht tun, stellt sich die Frage, ob mit der Meldung solcher Vorfälle betroffene Unternehmen, Behörden und Meldewege nicht überfordert werden. Wir empfehlen daher, diesen Passus zu streichen oder zu präzisieren. Weiter ist eine in Abs. 2 geforderte Ursachenforschung binnen 24 Stunden in der Praxis schwer umsetzbar. Hier könnte die 24 Stunden Meldepflicht entschärft werden und auf 72 Stunden geändert werden.

Grundsätzlich sollte sichergestellt werden, dass die in § 6 enthaltene Registrierungspflicht gesetzesübergreifend einheitlich geregelt wird.

Nachweise

Um den Prüf- und Auditierungsaufwand betroffener Unternehmen zu minimieren, sollten Nachweise über Resilienzmaßnahmen und -pläne, Konzepte und Architektur sowie angewandtes Risikomanagement nach § 10 Anerkennung finden. Resilienzmaßnahmen lassen sich nach verschiedenen ISO-Standards (ISO 22316, 22320, 22301, 27001, 31000) sowie IEC 62443-2-1, 62443-3-2, und IEC 62443-3-3 zertifizieren und auditieren. Diese Standards eignen sich hierbei als Nachweise über ergriffene Maßnahmen. Außerdem ist sicherzustellen, dass die in §10 Abs. 3 genannten Maßnahmen lediglich beispielhaft zu verstehen sind, und eine auf die im betroffenen Unternehmen bzw. in der betroffenen Anlage vorliegende konkrete Situation abgestimmte Maßnahme der Auflistung in §10 Abs. 3 in jedem Fall vorgeht.

Weiterhin muss generell sichergestellt werden, dass Nachweise im Rahmen anderer Zertifizierungen und Genehmigungen auch im Rechtskontext des KRITIS-DG anerkannt, bzw. verwendet werden können und das BBK, das BSI bzw. die BNetzA sich auf etablierte Normen und Standards referenziert. Dies ist eine elementare Voraussetzung dafür, dass die Sicherheit zu erhöht wird, eine europäische Vergleichbarkeit hergestellt und die Kosten für die Antragsteller und Behörden in einem angemessenen Rahmen gehalten werden und Prozesse beherrschbar, wiederholbar und voraussagbar sind.

Kommunikation der Behörden

Es ist unabdingbar, dass die Abstimmung unter den Behörden zügig und nach klaren Regeln erfolgt, damit Betreiber kritischer Anlagen größtmögliche Sicherheit über ihre Pflichten erlangen und auf ein einheitliches Vorgehen vertrauen können. Dies schließt auch ein, dass in Behörden ein vergleichbares Schutz- und Resilienzniveau wie in den betroffenen Unternehmen sichergestellt wird, um vertrauliche Daten und Unternehmensgeheimnisse nach Übermittlung an die zuständigen Behörden nicht zu kompromittieren.

Der Referentenentwurf des KRITIS-DachG sieht an mehreren Stellen die Möglichkeit vor, dass das BBK Vorlagen, Muster oder anderweitige Vorgaben veröffentlicht, an denen sich betroffene Unternehmen orientieren können. Es ist sicherzustellen, dass diese Unterlagen möglichst frühzeitig vor Inkrafttreten der gesetzlichen Pflichten für die betroffenen Unternehmen veröffentlicht werden, um diesen eine ausreichende Zeit zur Vorbereitung und Implementierung zu ermöglichen. Dies gilt insbesondere für klare Kriterien, in welchen Fällen eine Meldung nach KRITIS-DachG zu erfolgen hat.

In diesem Kontext sollte auch die Bereitstellung eines Sicherheitslageberichts für den Geltungsbereich des KRITISDachG bedacht werden. Bisher wird der IT-Sicherheitslagebericht des BSI KRITIS-Betreibern, die unter das IT-Sicherheitsgesetz und KRITIS-Verordnung fallen, täglich bereitgestellt. Hier ist uns aktuell keine Entwicklung bzw. Diskussion zum Bereich der physischen Sicherheit bekannt.

Herausgeber
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner
Clemens Schleupner | Referent Vertrauensdienste & Digitale Identitäten
T 030 27576-424 | c.schleupner@bitkom.org

Verantwortliches Bitkom-Gremium
AK Informationssicherheit