bitkom

Stellungnahme zum KRITIS-Dachgesetz

Entwurf eines Gesetzes zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen

KRITIS-Dachgesetz

Ausgangslage

Das Bundesministerium des Innern und für Heimat (BMI) veröffentlichte am 17.07.2023 den Referentenentwurf zum KRITIS-Dachgesetz. Ziel dieses Gesetzes ist die Umsetzung der EU-Richtlinie über die Resilienz kritischer Einrichtungen (CER-Richtlinie). Das Gesetz beabsichtigt die Einführung neuer Vorgaben zur physischen Sicherheit kritischer Infrastrukturen, die parallel zu den bereits bestehenden IT-sicherheitsrechtlichen Regelungen, BSI-Gesetz sowie Gesetz zur Umsetzung der NIS-2-Richtlinie, gelten sollen.

Bitkom-Bewertung

Der Bitkom begrüßt die Absicht der Bundesregierung, den Schutz der Bevölkerung und die Versorgung in Krisensituationen zu stärken. Wir sind jedoch der Auffassung, dass eine praxistaugliche Umsetzung nur dann erfolgen kann, wenn die Wirtschaft frühzeitig und kontinuierlich in die Gestaltung der Regelungen einbezogen wird, insbesondere im Hinblick auf die geplante Rechtsverordnung. Aus diesem Grund fordern wir, dass auch bei der Verabschiedung von Rechtsverordnungen im Vorfeld die Expertise der Branchenverbände und der Unternehmen eingeholt wird. Der vorliegende Entwurf des KRITIS-Dachgesetzes bildet zudem lediglich einen Teil der angestrebten ganzheitlichen Sicherheitsarchitektur. Daher sollte eine Harmonisierung mit existierender und zukünftiger Regulierung, wie dem NIS-2-Umsetzungsgesetz, angestrebt werden.

Das Wichtigste

Im Bitkom sind neue Anbieter genauso wie Mitglieder mit großer Nähe zu den klassischen Diensten vertreten. Unser Papier zeichnet daher mögliche Kompromisslinien vor:

- **Anwendungsbereich & Rechtsverordnung**
  Der Referentenentwurf des KRITIS-DachG weist Unklarheiten auf. Die geplante Rechtsverordnung und Definitionsdifferenzen erfordern diesbezüglich Klärung. Physische Sicherheit und IT-Sicherheit sollten zudem ganzheitlich berücksichtigt werden.

- **Harmonisierung**
  Es müssen klare Regelungen zur Kompetenzverteilung etabliert werden und das KRITIS-Dachgesetz sowie das NIS-2-Umsetzungsgesetz inhaltlich zusammengeführt werden, um eine kohärente Gesetzgebung und einen umfassenden Schutz zu gewährleisten. Dies erfordert eine Abstimmung auf sowohl nationaler als auch europäischer Ebene, um die optimale Sicherheit für kritische Infrastrukturen sicherzustellen.

- **Kritische Komponenten**
  Der Bitkom kritisiert, dass der Artikel zu Kritischen Komponenten sowie bestehende Regelungen aus dem BSI-Gesetz im Referentenentwurf des KRITIS-Dachgesetzes nicht übernommen wurden. Damit könnten unternehmerische Risiken und negative Einwirkungen auf die Resilienz verringert werden.

Inhalt

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 KRITIS-Dachgesetz 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.

Anwendungsbereich & Rechtsverordnung

Ermächtigung und Konkretisierung

Der vorliegende Referentenentwurf zum KRITIS-DachG weist an einigen Stellen noch erhebliche Unklarheiten und Ungenauigkeiten auf. Dieser Umstand wird verstärkt durch die geplante Ermächtigung zur Schaffung einer Rechtsverordnung im Rahmen des Gesetzes. Diese Verordnung soll den Adressatenkreis sowie die damit verbundenen Pflichten festlegen. Hierbei ist es jedoch von wesentlicher Bedeutung, dass grundrechtsrelevante Aspekte im Gesetz selbst verankert sind, um Transparenz und Schutz zu gewährleisten. Zugleich sollte die Verordnung lediglich der Konkretisierung dienen und keine Möglichkeit bieten, über die gesetzlichen Vorgaben hinauszugehen. Das Gesetz sollte sich daher stärker an der CER-Richtlinie orientieren und die dort genannten Teilsektoren und Einrichtungskategorien direkt mit aufnehmen. Dadurch wäre der Adressatenkreis grundsätzlich bereits jetzt klar definiert.

Notwendige Klarheit und Kohärenz

Eine besondere Herausforderung liegt in der uneinheitlichen Definition von Begrifflichkeiten, Schwellenwerten und Zuständigkeiten zwischen dem KRITIS-DachG und dem NIS2-UmsuCG. Dies wirft Fragen zur Kohärenz auf und erfordert eine sorgfältige Prüfung und mögliche Anpassung beider Gesetzesentwürfe. Des Weiteren bedarf es dringend einer Klärung bezüglich der Unterschiede zwischen den Definitionen von »Informationstechnik und Telekommunikation (NIS-2-Umsetzungsgesetz)« und »Verwaltung von IKT-Diensten (Business-to-Business) (KRITIS-Dachgesetz)«. Diese Unklarheiten könnten zu Missverständnissen führen und sollten daher im Sinne der Digitalwirtschaft präzisiert werden. Ein Ausschnitt der unterschiedlichen Definitionen zwischen den genannten Gesetzesentwürfen findet sich im Anhang.

Ganzheitliche Sicherheitsbetrachtung

Die beträchtliche Relevanz der IT- und physischen Sicherheit wird im Referentenentwurf nicht in ausreichendem Maße berücksichtigt. Die fortschreitende Verschmelzung von Technologien macht deutlich, dass eine isolierte Betrachtung

18%

Digitaler Diebstahl, Spionage oder Sabotage auf Unternehmen haben um 18 % zugelegt, wobei analoge Angriffe derselben Art um 20 % gesunken sind.

Quelle: Bitkom Research, Wirtschaftsschutz 2022 (bitkom.org)

dieser Sicherheitsaspekte nicht zielführend ist. Insbesondere die vermehrte Verwendung von IT-Lösungen im Bereich der physischen Sicherheit erfordert klar abgestimmte Regelungen. Differenzierte Sicherheitsanforderungen, die sich an den jeweiligen Sektoren orientieren, sind dabei unerlässlich, um den individuellen Risiken gerecht zu werden. Daher sollte das beabsichtigte Gesetz eine umfassendere Perspektive auf die Digitalwirtschaft einnehmen und sicherstellen, dass alle relevanten Sicherheitsaspekte angemessen adressiert werden.

Für Betreiber kritischer Anlagen, welche gemäß den § 10, 12 & 13 des KRITIS-DachG in großen Teilen von dessen Geltungsbereich ausgenommen werden, entfallen die Verpflichtungen im Zusammenhang mit Risikomanagement, Meldewesen und Resilienzmaßnahmen gemäß dem KRITIS-DachG. Diese Angelegenheiten werden für die betroffenen Sektoren, Finanz- und Versicherungswesen sowie Informationstechnik und Telekommunikation, im NIS2-UmsuCG geregelt. Die Regularien des NIS2 betreffen ebenso digitale Dienste. Hierbei würde das KRITIS-DachG ebenfalls hinter dem NIS2-UmsG zurücktreten (§ 15 Nr.3). In Anbetracht dessen wäre es angemessen, wenn Unternehmen der betroffenen Branchen vollständig von den Anwendungsbestimmungen des KRITIS-DachG ausgenommen würden. Anforderungen an die physische Sicherheit dieser Unternehmen sollten ausschließlich aus den bereits bestehenden sektorspezifischen Vorschriften abgeleitet werden, um die Umsetzbarkeit für die Akteure zu gewährleisten.

Harmonisierung

Der Bitkom begrüßt die zeitnahe Umsetzung der CER-Richtlinie, um Planungssicherheit für die Unternehmen zu schaffen. Zur Sicherstellung einer einfachen Rechtsanwendung müssen jedoch die Vorgaben für kritische Infrastrukturen zur physischen Sicherheit im KRITIS-Dachgesetz und zur Informationssicherheit im NIS-2-Umsetzungsgesetz passgenau zueinander gestaltet werden und aufeinander abgestimmt. Einheitliche Begriffsdefinitionen sowie überschneidungs- und widerspruchsfreie Vorgaben sind dabei zentral. Einige Begrifflichkeiten sind im Anhang der Stellungnahme zu finden. Entsprechend muss vor der Inkraftsetzung dringend eine Konsistenzprüfung der verwendeten Begriffe/Definitionen und eine Prozessharmonisierung erfolgen.

Im Zuge der Ausgestaltung und Anpassung des gesetzlichen Rahmens für die physische Sicherheit und den Cyberschutz Kritischer Infrastrukturen sind zudem klare Regelungen in Bezug auf die behördliche Kompetenzverteilung erforderlich. Diese Regelungen müssen auch berücksichtigen, dass KRITIS-Unternehmen auch nach den für sie geltenden branchenspezifischen Regelungen, z. B. dem TKG oder der DORA, einer aufsichtsbehördlichen Kontrolle, z. B. durch die BNetzA oder der BaFin, unterliegen.

Daher sollten das KRITIS-Dachgesetz und das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz und die entsprechenden Verordnungen in einem gemeinsamen Gesetzgebungsverfahren gebündelt werden. Nur durch eine Bündelung kann Kohärenz – sowohl hinsichtlich der Anforderungen als auch in der Umsetzung – gewährleistet werden. Die Verhinderung von Doppelregulierung sowie die Einheitlichkeit, Widerspruchsfreiheit und Transparenz der Verpflichtungen für die Wirtschaft muss bei der Gesetzgebung zwingend sichergestellt werden. Eine

kohärente, abgestimmte Regelungslage national (ITSiG/Nationale Cybersicherheitsstrategie einerseits, KRITIS DG/Nationale Sicherheitsstrategie andererseits) wie europäisch (NIS/CRA einerseits, RCE andererseits) ist zwingend erforderlich, um den optimalen Schutz der Infrastruktur zu gewährleisten. Vor dem Hintergrund zahlreicher nationaler und europäischer Regulierungsinstrumente, die sich teilweise überlappen oder widersprechen, braucht es nicht nur auf Bundesebene eine verstärkte Koordinierung beim Schutz kritischer Infrastrukturen, sondern auch eine bessere Abstimmung zwischen deutscher und europäischer Politik.

Registrierungs- & Meldewesen

Wir begrüßen die geplante gemeinsame Registrierungsmöglichkeit durch das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe sowie das Bundesamt für Sicherheit in der Informationstechnik. Diese Maßnahme verspricht mehr Effizienz und einen vereinfachten Informationsfluss durch die Vereinheitlichung von Prozessen. Die Vermeidung paralleler und aufwändiger Meldestrukturen ist essenziell, weshalb eine präzise Abstimmung zwischen dem Meldewesen im Bereich der physischen Sicherheit und der Informationssicherheit erforderlich ist. Um den Aufwand für die Unternehmen zu reduzieren, sollten die Meldefristen möglichst einheitlich gestaltet werden.

Zeiträume und Störungsmeldungen

Die vorgesehene Registrierungsfrist im KRITIS-Dachgesetz sollte im Einklang mit dem dreimonatigen Zeitrahmen im NIS-2-Umsetzungsgesetz stehen, um Klarheit und Konsistenz zu gewährleisten. Die unterschiedlichen Störungsmeldungsdauern im KRITIS-DachG (24 Stunden/1 Monat) und im BSIG des NIS-2-Umsetzungsgesetz (24 Stunden/72 Stunden/1 Monat) werfen Fragen auf. Insbesondere die Erstmeldungsfrist von 24 Stunden erscheint im Vergleich zu 72 Stunden in vergleichbaren kritischen Sektoren wie dem Flugbetrieb nicht verhältnismäßig.

Digitale Meldungen und Schutzanforderungen

Die Möglichkeit digitaler Meldungen mit den notwendigen Informationen, die zur Erfüllung des Auftrags der Aufsichtsbehörden unerlässlich sind, ist zu begrüßen. Dabei ist eine einheitliche und anwenderfreundliche Gestaltung von Meldepflichten sowie der dazugehörigen Schnittstellen und digitalen Portale von großer Bedeutung. Diese Gestaltung sollte den Aufwand für Unternehmen reduzieren und gleichzeitig die Sensibilität der übermittelten Informationen angemessen schützen.

Unklarheiten und internationale Aspekte

Es besteht Unklarheit hinsichtlich der Definition und Festlegung von kritischen Anlagen von besonderer Bedeutung für Europa. Klarheit ist auch erforderlich in Bezug auf die Meldewege bei Sicherheitsvorfällen bei Tochtergesellschaften mit Sitz im EU-Ausland. Besondere Bedenken ergeben sich bei der Publikation der Liste wesentlicher Dienste, da dieser Prozess Unsicherheiten birgt und ein neues Publikationsmedium einführt. Es ist notwendig, diese Aspekte sorgfältig zu klären, um eine reibungslose und transparente Umsetzung zu gewährleisten.

Risikomanagementmaßnahmen & -bewertung

Technische und Organisatorische Maßnahmen

Die Digitalwirtschaft betont die Wichtigkeit der Vereinheitlichung von Technischen und Organisatorischen Maßnahmen (TOM), um ein effektives Schutzniveau zu erreichen. Diese Maßnahmen sollten im Einklang mit den Anforderungen des NIS2-UmsuCG und internationalen Standards stehen. Klare, einfache und umsetzbare Schutzziele sind unerlässlich, um eine effiziente Sicherheitsstrategie zu gewährleisten. Die vorgesehenen Sicherheitsstandards gemäß § 8a Absatz 2 BSIG sollen als Grundlage für Bedrohungsanalysen dienen, jedoch fehlt es im aktuellen Referentenentwurf an Klarheit bezüglich der Definition, Verantwortung und des Zeitrahmens für die Festlegung dieser Standards.

Risikobewertungen und Harmonisierung

Die gemeinsame Erarbeitung von Risikobewertungen für die Bereiche Kritischer Infrastrukturen durch Staat und Wirtschaft ist von großer Bedeutung. Eine behördenübergreifende und europäische Harmonisierung der Risikoszenarien ist notwendig, um Betreibern unterschiedlicher Sektoren unterschiedliche Risikoszenarien zu ersparen. Rechtzeitige Vorarbeiten seitens der öffentlichen Hand sind erforderlich, um Verzögerungen in den unternehmensindividuellen Risikoanalysen zu verhindern, wie sie in § 10 für eigene Risikoanalysen der Anlagenbetreiber festgelegt sind.

Die staatliche Risikoanalyse sollte zudem klare Regeln über die Priorisierung der Sektoren und der untergeordneten kritischen Anlagen im Krisenfall schaffen, z. B. im Falle eines Engpasses bei der Energieversorgung. Eine entsprechende Priorisierung ist in manchen Sektoren bereits gesetzlich verankert.

Sowohl KRITIS-DachG E in § 11 Abs. 5 als auch NIS-2-Umsetzungsgesetz E in § 30 Abs. 12 sehen die Möglichkeit vor, Branchenstandards für die geforderten Resilienz- bzw. Risikomanagement-Maßnahmen zu entwickeln. Auch hier sollte eine größtmögliche Übereinstimmung der Standards herrschen, um eine Parallelität mehrerer, in die gleiche Richtung zielender Standards zu vermeiden. Idealerweise sollten BSI und BBK eingereichte Branchenstandards gemeinsam prüfen, um Kohärenz sicherzustellen. Außerdem sollte klargestellt werden, wie in Fällen zu verfahren ist, bei denen betroffene Unternehmen oder Anlagenbetreiber mehreren Sektoren zuzuordnen sind.

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.

Stand der Technik

Sowohl KRITIS-DachG als auch NIS-2-Umsetzungsgesetz verweisen bei den geforderten Resilienz- bzw. Risikomanagement-Maßnahmen auf den Stand der Technik. Bei der Bewertung des Standes der Technik sollten immer der tatsächliche Schutzzweck und der tatsächliche Nutzen der zur Anwendung kommenden Technik herangezogen werden.

Der Stand der Technik sollte zudem kohärent mit den Anforderungen der NIS2 sein, dazu gehören u. a. die Verwendung von sicheren Multi-Faktor-Authentifizierungslösungen.

Kritische Komponenten

Der Bitkom bemängelt, dass ein zentraler Baustein des Gesetzes, Artikel 13 zu Kritischen Komponenten, der den Betrieb von kritischen Infrastrukturen maßgeblich beeinflusst und in die Geschäftsbeziehungen zu Herstellern und Lieferanten beeinflussen kann, zum Start der Verbändeanhörung nicht ausformuliert ist. Der Bitkom lehnt daher die aktuelle Ausgestaltung des Artikels (Leerstelle im Entwurf) ab.

Um die Pflicht der Bundesregierung der demokratischen Beteiligung zu erfüllen, muss die Wirtschaft in die letztliche Ausgestaltung des Artikel 13 miteinbezogen und konsultiert werden. Die zukünftige Formulierung des Artikel 13 sollte in keinem Fall über die aktuelle Regelung im BSI G hinausgehen.

Außerdem ist mit Verweis auf Nicht-IT-Produkte im Kapitel »Schutz von KRITIS« in der China-Strategie der Bundesregierung (S. 42) unklar, welche Ziele die Bundesregierung mit der Leerstelle im Referentenentwurf gegebenenfalls verfolgt.

Schon bei der Betrachtung von IT-Produkten als kritische Komponente galt: Der Schutzbedarf beim Betrieb von kritischen Infrastrukturen ist in erster Linie technisch-agnostisch und bedarf einer regel- und kritikalitätsbasierten Prüfung (und Zertifizierung).

Eine mögliche Ausweitung des Gesetzestextes auf Nicht-IT-Produkte stellt ein hohes unternehmerisches Risiko für die Betreiber dar. Sie ermöglicht einen zu großen Ermessensspielraum der Exekutive, insbesondere, wenn nicht klar ersichtlich ist, welche Produktgruppen mittel- bis langfristig in die Liste der kritischen Komponenten aufgenommen werden. Um die Resilienz der kritischen Infrastrukturen zu erhöhen, ist Investitions- und Rechtssicherheit zu gewährleisten. ´

Anhang

Die folgende Tabelle weist einige begriffliche Inkohärenzen im KRITIS-DachG und dem NIS2-UmsuCG auf. Diese Liste erhebt kein Anspruch auf Vollständigkeit.

Begrifflichkeiten	KRITIS-Dachgesetz	NIS2-UmsuCS	Kommentar
IT-Sicherheit vs. physische Sicherheit	Beim KRITIS-DachG und der damit verbundenen Umsetzung der CER-Richtlinie sowie bei der Umsetzung der NIS-2-Richtlinie durch das entsprechende Umsetzungsgesetz werden die Schnittstellen zwischen den Bereichen IT-Sicherheit und physischen Resilienzmaßnahmen von kritischen Anlagen berücksichtigt und angeglichen, bzw. – soweit möglich und sinnvoll – übereinstimmend geregelt.		*IT-Sicherheit umfasst mit den Schutzzielen Vertraulichkeit, Verfügbarkeit und Integrität auch physische Maßnahmen zu der Erreichung des Schutzziels. Die Abgrenzung von IT-Sicherheit und physischer Sicherheit bei Unternehmen, deren Kernkompetenz IT ist, führt zu Schwierigkeiten in der Abgrenzung.*
All-Gefahren-Ansatz	Die im KRITIS-DachG getroffenen Bestimmungen zu kritischen Anlagen orientieren sich an den bisherigen Regelungen zur IT-Sicherheit von Kritischen Infrastrukturen unter Berücksichtigung der geplanten Umsetzung der NIS-2-Richtlinie, um den Aufbau des Systems unter dem »All-Gefahren-Ansatz« auch für die Wirtschaft zu erleichtern.		*Der All-Gefahren-Ansatz wird heute schon für die IT von kritischen Infrastrukturen durch die BSI-Vorgaben gefordert. Auch hier fehlt die Klarstellung, dass sich die Aussagen auf den Nicht- IT-Bereich beziehen.*
Vorfälle	Ein »Vorfall« ist ein Ereignis, das die Erbringung einer kritischen Dienstleistung erheblich beeinträchtigt oder beeinträchtigen könnte.	Unterscheidet *Beinahevorfall Sicherheitsvorfall, erheblicher Sicherheitsvorfall.* Ein »Beinahevorfall« ist ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über informationstechnische Systeme, Komponenten und Prozesse angeboten werden oder zugänglich sind, beeinträchtigt haben könnte, dessen Eintritt jedoch erfolgreich verhindert wurde oder auf andere Weise nicht eingetreten ist;	*Es ist unklar, ob Vorfälle sich lediglich auf kritische Dienstleistungen beziehen und nicht auf kritische Anlagen.* *Warum unterscheidet das NIS2-UmsuCS bei Vorfällen, nicht aber das KRITIS-DachG?*

Begrifflichkeiten	KRITIS-Dachgesetz	NIS2-UmsuCS	Kommentar
		ein »erheblicher Sicherheitsvorfall« ist ein Sicherheitsvorfall, der a) schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann; oder b) andere natürliche oder juristische Personen durch erhebliche materielle oder im-materielle Schäden beeinträchtigt hat oder beeinträchtigen kann, soweit nach Absatz 2 keine weitergehende Begriffsbestimmung erfolgt; ein »Sicherheitsvorfall« ist ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über informationstechnische Systeme, Komponenten und Prozesse angeboten werden oder zugänglich sind, beeinträchtigt;	
Definition »Kritischer« Aspekte	»Kritische Infrastrukturen« sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der wirtschaftlichen Tätigkeit, der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden; eine »kritische Anlage« eine Anlage, die eine hohe Bedeutung für das Funktionieren des Gemeinwesens hat, da durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder	eine »kritische Anlage« eine Anlage, die von hoher Bedeutung für das Funktionieren des Gemeinwesens ist, da durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden; welche Anlagen im Einzelnen kritische Anlagen sind, bestimmt sich nach § 28 Absatz 3; »kritische Komponenten« IT-Produkte, a) die in Kritischen Anlagen eingesetzt werden,	Der Begriff »Kritische Dienstleistung« ist im NIS2-UmsuCS nicht vorhanden. *Eine einheitliche Verwendung von »kritische Anlage« oder »kritische Dienstleistung« ist wünschenswert.*

Begrifflichkeiten	KRITIS-Dachgesetz	NIS2-UmsuCS	Kommentar
	Gefährdungen für wirtschaftliche Tätigkeiten, die öffentliche Sicherheit oder Ordnung eintreten würden; welche Anlagen im Einzelnen kritische Anlagen sind, bestimmt sich nach § 4; eine »kritische Dienstleistung« eine Dienstleistung zur Versorgung der Allgemeinheit, deren Ausfall oder Beeinträchtigung zu einer Gefährdung von wirtschaftlichen Tätigkeiten, zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde; »Betreiber kritischer Anlagen« eine natürliche oder juristische Person oder rechtlich unselbstständige Organisationseinheit einer Gebietskörperschaft, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf eine kritische Anlage ausübt;	b) bei denen Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit Kritischer Anlagen oder zu Gefährdungen für die öffentliche Sicherheit führen können und c) die aufgrund eines Gesetzes unter Verweis auf diese Vorschrift aa) als kritische Komponente bestimmt werden oder bb) eine aufgrund eines Gesetzes als kritisch bestimmte Funktion realisieren, werden für einen der in § 57 Absatz 1 Nummer 1 genannten Sektoren keine kritischen Komponenten und keine kritischen Funktionen, aus denen kritische Komponenten abgeleitet werden können, aufgrund eines Gesetzes unter Verweis auf diese Vorschrift bestimmt, gibt es in diesem Sektor keine kritischen Komponenten im Sinne von dieser Nummer;	
Eine »wichtige Einrichtung« ist:	§ 2 (12) a) ein mittleres Unternehmen, das einer der durch Rechtsverordnung nach § 15 bestimmten Einrichtungsarten der Sektoren Energie, Transport und Verkehr, Finanz- und Versicherungswesen, Gesundheitswesen, Trinkwasser, Abwasser, Informationstechnik und Telekommunikation, Verwaltung von IKT-Diensten (Business-to-Business) oder Weltraum zuzuordnen ist,	§ 28 (7) 1. ein mittleres Unternehmen, das einer der durch Rechtsverordnung nach § 57 Absatz 1 bestimmten Einrichtungsarten der Sektoren Energie, Transport und Verkehr, Finanz- und Versicherungswesen, Gesundheitswesen, Trinkwasser, Abwasser, Informationstechnik und Telekommunikation, Verwaltung von IKT-Diensten (Business-to-Business) oder Weltraum zuzuordnen ist,	Definition enthält abweichend vom KRITIS-Dachgesetz bei der NIS2-UmsuCS zusätzlich »Vertrauensdiensteanbieter«

Begrifflichkeiten	KRITIS-Dachgesetz	NIS2-UmsuCS	Kommentar
	b) ein mittleres Unternehmen oder Großunternehmen, das einer der durch Rechtsverordnung nach § 15 bestimmten Einrichtungsarten der Sektoren Logistik, Siedlungsabfallentsorgung, Produktion, Chemie, Ernährung, verarbeitendes Gewerbe, Anbieter digitaler Dienste oder Forschung zuzuordnen ist, c) wer Güter im Sinne des Teils B der Kriegswaffenliste herstellt oder entwickelt oder vom Bundesamt zugelassene Produkte mit IT-Sicherheitsfunktionen zur Verarbeitung staatlicher Verschlusssachen oder für die IT-Sicherheitsfunktion wesentliche Komponenten solcher Produkte herstellt, d) wer Betreiber eines Betriebsbereichs der oberen Klasse im Sinne der Störfall-Verordnung in der jeweils geltenden Fassung oder nach § 1 Absatz 2 der Störfall-Verordnung einem solchen gleichgestellt ist,	2. ein mittleres Unternehmen oder Großunternehmen, das einer der durch Rechtsverordnung nach § 57 Absatz 1 bestimmten Einrichtungsarten der Sektoren Logistik, Siedlungsabfallentsorgung, Produktion, Chemie, Ernährung, verarbeitendes Gewerbe, Anbieter digitaler Dienste oder Forschung zuzuordnen ist, 3. Vertrauensdiensteanbieter, 4. wer Güter im Sinne des Teils B der Kriegswaffenliste herstellt oder entwickelt oder vom Bundesamt zugelassene Produkte mit IT-Sicherheitsfunktionen zur Verarbeitung staatlicher Verschlusssachen oder für die IT-Sicherheitsfunktion wesentliche Komponenten solcher Produkte herstellt, 5. wer Betreiber eines Betriebsbereichs der oberen Klasse im Sinne der Störfall-Verordnung in der jeweils geltenden Fassung oder nach § 1 Absatz 2 der Störfall-Verordnung einem solchen gleichgestellt ist,	
Kritische Anlage & besonders wichtige Unternehmen	§ 2 (11) »Besonders wichtige Einrichtung« a) ein Großunternehmen, das einer der durch Rechtsverordnung nach § 15 bestimmten Einrichtungsarten der Sektoren Energie, Transport und Verkehr, Finanz- und Versicherungswesen, Gesundheitswesen, Trinkwasser, Abwasser, Informationstechnik und Telekommunikation, Verwaltung von IKT-Diensten (Business-to-Business) oder Weltraum zuzuordnen ist,	analog	In der Definition von kritischen Anlagen (§ 28 NIS2-UmsuCS § 4 KRITIS-Dachgesetz) heißt der Sektor »Informationstechnik und Telekommunikation« bei wichtigen und wesentlichen Einrichtungen »Verwaltung von IKT-Diensten (Business-to-Business)«. *Wie grenzen sich die Begriffe ab und was passiert, wenn aufgrund der Tatsache, dass Betreiber kritischer Anlagen im IKT-Sektor auch*

Begrifflichkeiten	KRITIS-Dachgesetz	NIS2-UmsuCS	Kommentar
	§ 4 (1) Eine Anlage ist ab dem durch die Rechtsverordnung nach § 15 festgelegten Stichtag eine kritische Anlage, wenn sie einer der durch Rechtsverordnung nach § 15 festgelegten Anlagenarten in den Sektoren Energie, Transport und Verkehr, Finanz- und Versicherungswesen, Gesundheitswesen, Trinkwasser, Abwasser, Ernährung, Informationstechnik und Telekommunikation, Weltraum, öffentliche Verwaltung oder Siedlungsabfallentsorgung zuzuordnen ist und die durch Rechtsverordnung festgelegten Schwellenwerte erreicht oder überschreitet.		*wesentliche Einrichtung sind, diese nicht deckungsgleich sind?*
Registrierung	§ 8 (2) Wenn der Betreiber seine Pflicht zur Registrierung einer kritischen Anlage nicht erfüllt, kann das BBK die Registrierung im Einvernehmen mit der sonst zuständigen Aufsichtsbehörde des Bundes auch selbst vornehmen. (3) Jeder Betreiber einer kritischen Anlage muss dem BBK eine Kontaktstelle oder eine Person mit vergleichbarer Aufgabenstellung als Ansprechpartner benennen.	§ 32 Die Registrierung von besonders wichtigen Einrichtungen, wichtigen Einrichtungen und Domain-Name-Registry-Diensteanbieter kann das Bundesamt auch selbst vornehmen, wenn die Einrichtung oder der Anbieter ihre oder seine Pflicht zur Registrierung nicht erfüllt. (3) Betreiber kritischer Anlagen sind verpflichtet, spätestens bis zum ersten Werktag, der auf denjenigen Tag folgt, an dem die von ihnen betriebene Anlage erstmalig oder erneut als kritische Anlage gilt, die von ihnen betriebenen kritischen Anlagen beim Bundesamt zu registrieren, indem sie dem Bundesamt die folgenden Angaben übermitteln: 1. den Standort und die IP-Adressbereiche der von ihnen	§ 8 KRITIS-Dachgesetz sieht eine Registrierung durch BBK vor, § 32 NIS2-UmsuCS eine Registrierung durch das BSI falls der Betreiber seine Pflicht nicht erfüllt. Da kritische Anlagen gleichlautend in den Gesetzen definiert sind, ist unklar, durch wen die Registrierung durchgeführt wird, auch in dem Fall, dass dasselbe Meldewesen genutzt wird. Gleiches gilt für die Benennung einer Kontaktstelle, die doppelt erfolgen muss BBK und BSI (§ 8 (3) KRITIS-Dachgesetz bzw. § 32 (3)

Begrifflichkeiten	KRITIS-Dachgesetz	NIS2-UmsuCS	Kommentar
		betriebenen kritischen Anlagen, 2. Informationen zu einer jederzeit erreichbaren Kontaktstelle und 3. die für die von ihnen betriebenen kritischen Anlagen gemäß der Rechtsverordnung nach § 57 Absatz 1 ermittelte Anlagenkategorie und Versorgungskennzahlen. (4) Die Registrierung einer kritischen Anlage kann das Bundesamt auch selbst vor-nehmen, wenn der Betreiber seine Pflicht zur Registrierung nicht erfüllt. Nimmt das Bundesamt eine solche Registrierung selbst vor, informiert es die zuständige Aufsichtsbehörde des Bundes darüber. Der Betreiber kritischer Anlagen hat sicherzustellen, dass er über die Angaben nach Absatz 3 Nummer 2 oder durch das Bundesamt festgestellten Kontaktdaten jederzeit erreichbar ist.	

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

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

Ansprechpartner/in
Simran Mann | Referentin Sicherheitspolitik
T 030 27576-214 | s.mann@bitkom.org

Verantwortliches Bitkom-Gremium
AK Sicherheitspolitik