AG KRITIS

Kommentar zum Referentenentwurf des KRITIS-Dachgesetz (KRITIS-DachG)

22.08.2023

Die beiden Leiter der AG KRITIS, Manuel Atug und Johannes Rundfeldt zum von der AG KRITIS veröffentlichten Entwurfs des KRITIS-DG von Juni 2023:

Der geleakte Entwurf des KRITIS-Dachgesetz (KRITIS-DachG) wirkt auf den ersten Blick überschaubar, aber bei genauerem Hinsehen ist er sehr unabgestimmt und unvollständig und es gibt viel zu viele Ausnahmen und sehr späte Fristen, die erst in vielen Jahren initial greifen oder wirken werden. Zu viele Punkte sind leider ein Stillstand oder gar Rückschritt und halten bestehende Gefahren und Risiken über Jahre weiterhin offen.

Manuel Atug dazu: "Schade, mit den vielen Ausnahmen und Verantwortungsdiffusion wird das keine ganzheitliche Resilienz für Deutschland werden. Mit den späten Fristen wird da auch vor 2028 nicht wirklich viel wirken, daher passiert auf der aktuellen Basis erst mal 5 Jahre lang wenig bis gar nichts. Haben wir so viel Zeit und können wir so entspannt sein?"

Johannes Rundfeldt dazu: "Der vorliegende Entwurf, der direkt nach den Anschlägen auf Nordstream 2 angekündigt wurde, entpuppt sich, wie bereits befürchtet, als politischer Opportunismus. Das KRITIS-Dachgesetz wird den hochtrabenden Versprechungen des BMI nicht gerecht und ist unvollständig."

Inhalt

Inhaltsverzeichnis

Analyse und Kommentierung der AG KRITIS zum Entwurf des KRITIS-DachG:

Einleitung

Ein Dachgesetz soll, so sagt schon der Name, das gesamte Thema vollständig abdecken und einen verbindlichen regulatorischen Rahmen bilden. Die Ministerin hatte dazu erklärt: “Wir werden die besonders zu schützenden Bereiche definieren, Risiken und Bedrohungslagen besser erkennen und verpflichtende Schutzstandards festlegen.” Da durch die bevorstehende Umsetzung der NIS2 Direktive und der DORA Richtlinie in den kommenden Monaten doch noch einiges an Änderungen zu erwarten sind, definiert das KRITIS-DachG entgegen der Behauptungen das Thema höchstens vorläufig.

Bewertung von Sicherheitsrisiken, Bedrohungen und Vorfällen § 3 Abs 2

Das BBK soll zukünftig von BSI und der BnetzA u.a. Infos zu IT-Sicherheitsrisiken, -bedrohungen, -vorfällen erhalten. Derzeit ist jedoch für die sinnvolle Auswertung und Bewertung dieser Daten im BBK kein fachlich kompetentes Personal vorhanden - im BSI jedoch schon. Einen Personalaufwuchs beim BBK würden wir begrüßen, ob es aber sinnvoll ist, diese Daten dann zweimal, sowohl im BSI als auch im BBK zu bewerten erscheint vor dem Hintergrund des Fachkräftemangels im IT-Bereich wenig sinnvoll. Falls das BMI trotzdem nur einen Grund sucht, dem BBK ein erhebliches Aufstocken der Belegschaft zu ermöglichen, würden wir empfehlen dieses im Zuge des “Neustart im Bevölkerungsschutz” des BMI zu tun, der bisher leider eher einen Stillstand aufrecht hält.

Neudefinition der Sektoren - § 2 Abs 12b, § 4 Abs 1

Das KRITIS Dachgesetz definiert die Sektoren der kritischen Anlagen neu. Im KRITIS Dachgesetz ist die öffentliche Verwaltung erstmalig aufgenommen, nachdem diese bisher im BSIG nicht vorhanden war. Gleichzeitig wird der Sektor “Wasser” aufgeteilt in zwei Sektoren: “Trinkwasser” und “Abwasser”. “Weltraum” kommt als neuer Sektor hinzu. Auch im NIS2-Umsetzungsgesetz wird der Sektor “Weltraum” aufgenommen - der Sektor “öffentliche Verwaltung” ist jedoch nicht Teil der kritischen Anlagen. Der Sektor “Medien und Kultur”, unter den auch die Katastrophenschutzinformationssysteme der öffentlich-rechtlichen Medien fallen würden, ist weiterhin nicht definiert. Bemerkenswert ist außerdem, dass die Sektoren “Wissenschaft und Forschung” und “Chemie” fehlen. Diese sind nur unter der neuen Kategorie “wichtige Einrichtungen” zu finden, nicht aber unter “kritische Anlagen”. § 2 Abs 12b, § 4 Abs 1

Leider bleiben die neuen Kategorien der “wichtigen Einrichtungen” und der “besonders wichtigen Einrichtungen” für das KRITIS Dachgesetz irrelevant, da diese Kategorien dort gar nicht reguliert werden. (Begründung Teil B §2 zu Nr. 10)

Im Endeffekt betrifft das KRITIS Dachgesetz also nur eine Teilmenge der kritischen Infrastruktur, die sich zudem von der Teilmenge kritischer Infrastruktur im NIS2-Umsetzungsgesetz unterscheidet.

branchenspezifische Resilienzstandards - § 6 Abs 2

Betreiber von KRITIS können **branchenspezifische Resilienzstandards** (BSRS) erstellen, vergleichbar der branchenspezifischen Sicherheitsstandards (B3S in BSI-Gesetz § 8a Abs 2). Grundsätzlich ist dies eine gute Idee, allerdings wird es, genau wie bei den branchenspezifischen Sicherheitsstandards wieder viele Jahre dauern, bis diese neuen Resilienzstandards entwickelt und umgesetzt worden sind.

Registrierung beim BBK - § 8 Abs 1,2

Schon jetzt müssen KRITIS Betreiber sich beim BSI registrieren. Unsere Befürchtungen, dass eine doppelte Registratur notwendig wird, haben sich nicht bewahrheitet - Es wird eine gemeinsame Registrierung der KRITIS Betreiber bei BBK und BSI geben, statt einer separaten neue Registrierung beim BBK. Auch die Ersatzvornahme der Registrierung bei Verweigerung selbiger ist durch die gemeinsame Registrierung elegant gelöst. Die neue Regelung ist daher vergleichbar der BSI Ersatzvornahme B3S in BSI-Gesetz § 8b Abs 3. Die dringende Empfehlung der AG KRITIS, keine doppelten und parallelen Strukturen aufzubauen wurden hier offenbar erhört.

Erreichbare Kontaktstelle - § 8 Abs 3,4

Wir begrüßen ausdrücklich, dass die KRITIS Betreiber nun dem BBK eine jederzeit erreichbare Kontaktstelle benennen müssen. Hoffentlich wird das BBK stichprobenartige Kontrollen durchführen, um festzustellen, ob diese Kontaktstelle auch rund um die Uhr besetzt ist.

Betreiberliste im BBK - § 8 Abs 5

Zur Pflicht, die sich aus Absatz 5 ergibt, alle 4 Jahre eine Liste der KRITIS Betreiber im BBK zu erstellen fragen wir uns, wieso das nicht aus dem gemeinsamen Registrierungsportal von BSI und BBK extrahiert werden kann. Dies dürfte Arbeit sparen.

Sektorübergreifende Risikoanalysen und –bewertungen BBK - § 9 Abs 2

Das BBK wertet die durch die verantwortlichen Bundesministerien durchzuführenden Risikoanalysen und –bewertungen sektorübergreifend aus. Es wird also ein

sektorübergreifendes Lagebild erstellt. Dies sollte öffentlich verfügbar gemacht werden. Wenn es wieder mal ein Dokument ist, das in den zuständigen Behörden vergilbt und nur in Auszügen den Betreibern zur Verfügung gestellt wird, nützt das weder KRITIS Betreibern, noch der Versorgungssicherheit der Bevölkerung.

Sektorübergreifende Risikoanalysen und –bewertungen der Betreiber § 10 Abs 1

KRITIS Betreiber führen auf Basis der durchgeführten staatlichen Risikoanalysen und -bewertungen nach § 9 und anderer Informationsquellen initial 9 Monate nach Registrierung und dann spätestens alle 4 Jahre **Risikoanalysen und -bewertungen durch**. Inkl. *„Wirtschafsstabilität beeinträchtigenden, naturbedingten, klimatischen und vom Menschen verursachten Risiken berücksichtigen, darunter solche sektorübergreifender oder grenzüberschreitender Art, Unfälle, Naturkatastrophen, gesundheitliche Notlagen, sowie hybride Bedrohungen oder andere feindliche Bedrohungen, einschließlich terroristischer Straftaten“* sowie *„Wirtschafsstabilität beeinträchtigenden, Risiken berücksichtigen, die sich aus dem Ausmaß der Abhängigkeiten anderer Sektoren von der kritischen Dienstleistung, die von der kritischen Anlage - auch in benachbarten Mitgliedstaaten und Drittstaaten - erbracht wird“*. Das alles findet leider sehr spät und selten statt, aber immerhin soll was passieren.

Begrüßenswert ist, dass endlich auch eine Analyse der Abhängigkeiten zwischen den verschiedenen Sektoren selbst, sowohl durch die zuständigen Bundesministerien als auch durch die Betreiber durchgeführt werden muss. Wir halten zwar den Turnus von 4 Jahren für zu lang, begrüßen aber den grundsätzlichen Ansatz. Insbesondere möchten wir hier anmerken, dass der Vorschlag die Abhängigkeiten der Sektoren untereinander und mögliche Szenarien, bei denen kaskadierende Ausfälle verschiedene Sektoren gleichzeitig betreffen, von uns bereits 2019 im Rahmen des IT-SiG2 gemacht wurden. Damit diese Risiken nicht nur bei der physischen Sicherheit betrachtet werden, halten wir es für notwendig, dieselben Auflagen und Analysen auch in der NIS2-Umsetzung vorzugeben.

Ausnahmen von den Risikoanalysen und -bewertungen - § 10 Abs 3

Ausgenommen von den verpflichtenden Risikoanalysen und -bewertungen sind KRITIS Betreiber aus den Sektoren “Finanz- und Versicherungswesen” und “Informationstechnik und Telekommunikation”. Vier wesentliche Branchen werden vollständig ausgeklammert, was weder sinnvoll noch nachvollziehbar ist. Ein Dachgesetz, das nur für sechs von elf Sektoren anwendbar ist, kann vieles sein, aber kein Dachgesetz.

Stand der Technik – soll oder muss? § 11 Abs 1,2

KRITIS Betreiber müssen **innerhalb von 10 Monaten nach Registrierung** (§ 11 Abs 13) „geeignete und verhältnismäßige technische, sicherheitsbezogene und organisatorische Maßnahmen zur Gewährleistung ihrer Resilienz“ treffen. „Dabei **soll** der Stand der Technik eingehalten werden“ (nicht muss?!?). „Technische, sicherheitsbezogene und organisatorische Maßnahmen sind verhältnismäßig, wenn der Aufwand zur Verhinderung oder Begrenzung eines Ausfalls oder einer Beeinträchtigung der kritischen Dienstleistung zu den Folgen ihres Ausfalls oder ihrer Beeinträchtigung angemessen erscheint“. Dazu gibt es auch einen Anhang 1 mit mehr Details. Warum der Stand der Technik nur eingehalten werden soll, statt das verpflichtend vorzugeben erschließt sich uns nicht. Hier halten wir es für notwendig, den Stand der Technik als “Muss”-Vorschrift zu formulieren

Welche Maßnahmen zählen dazu? Solche, die erforderlich sind, um:

1. *das Auftreten von Vorfällen zu verhindern,*
2. *einen angemessenen physischen Schutz der Räumlichkeiten der kritischen Anlagen zu gewährleisten,*
3. *auf Vorfälle zu reagieren, sie abzuwehren und die Folgen solcher Vorfälle zu begrenzen,*
4. *nach Vorfällen die Wiederherstellung zu gewährleisten,*
5. *ein angemessenes Sicherheitsmanagement hinsichtlich der Mitarbeiter zu gewährleisten, einschließlich des Personals externer Dienstleister und*
6. *das entsprechende Personal für die unter den Nummern 1 bis 5 genannten Maßnahmen durch Informationsmaterialien, Schulungen und Übungen zu sensibilisieren.* § 11 Abs 3

Resilienzplan § 11 Abs 6

KRITIS Betreiber müssen die durchzuführenden Maßnahmen in einem **Resilienzplan** darstellen. Der ist dem BBK spätestens zu einem vom BBK (mit BSI abgestimmt) bei Registrierung festgelegten Zeitpunkt und anschließend alle 2 Jahre nachzuweisen.

KRITIS Betreiber müssen dem BBK **Dokumente zur Stärkung der Resilienz** zum festgelegten Zeitpunkt bereitstellen. Das BBK bestimmt dann, ob diese Maßnahmen dann vollständig oder teilweise den Verpflichtungen entsprechend gelten. Legt der KRITIS Betreiber Bescheide, Genehmigungen, Zertifizierungen oder ähnliche Nachweise zur Resilienzsteigerung von anderer zuständiger Behörde vor, gelten die darin beschriebenen Maßnahmen ohne weitere Überprüfung als erfüllt. § 11 Abs 7

BBK und zuständige Aufsichtsbehörde des Bundes können bei Verstößen gegen die Anforderungen KRITIS Betreiber anweisen, erforderliche und verhältnismäßige Maßnahmen zu ergreifen, um festgestellte Verstöße innerhalb einer angemessenen Frist zu beheben. Nach unserer Lesart des Gesetzes können hier auch Bußgelder nach § 19 verhängt werden. § 11 Abs 10

Ausgenommen davon sind KRITIS Betreiber aus den Sektoren “Finanz- und Versicherungswesen” und “Informationstechnik und Telekommunikation”. Vier wesentliche Branchen werden hier erneut vollständig ausgeklammert, was nicht sinnvoll ist. § 11 Abs 14

Meldepflicht für Vorfälle § 12 Abs 1,3

KRITIS Betreiber sind **spätestens 10 Monate nach Registrierung** verpflichtet, **Vorfälle**, die die Erbringung ihrer **kritischen Dienstleistungen erheblich stören könnten**, **unverzüglich** über ihre Kontaktstelle an eine gemeinsame BBK und BSI Meldestelle zu **melden**. Für tatdächlich stattgefundene Vorfälle muss eine erste Meldung bis spätestens **24 Stunden nach Kenntnisnahme** des Vorfalls übermittelt werden, es sei denn, dies ist in operativer Hinsicht nicht möglich. Spätestens **einen Monat danach** muss ein **ausführlicher Bericht** übermittelt werden. § 12 Abs 1,3

Ausgenommen davon sind wieder KRITIS Betreiber aus den Sektoren “Finanz- und Versicherungswesen” und “Informationstechnik und Telekommunikation”. Abermals werden hier vier wesentliche Branchen vollständig ausgeklammert. § 12 Abs 9

Verordnungsermächtigung für kritische Komponenten - § 13

Einsatz kritischer Komponenten: Die Verordnungsermächtigung wäre ein spannender Teil, der wird aber offenbar noch diskutiert. Der Paragraph ist daher noch komplett ohne Inhalt, weil derzeit noch unabgestimmt zwischen den Ressorts. § 13

In der hierzu kommenden – aber noch nicht existierenden – Rechtsverordnung können „Stichtage festgelegt und Teile der Bundesverwaltung als kritische Infrastruktur bestimmt“ werden. Dass hier wieder nur Teile der Bundesverwaltung KRITIS werden könnten und Kommunen und Bundesländerebene schon wieder nicht vorkommen zeigt, wie unvollständig das ganze durch all die vielen Ausnahmen und Abgrenzungen sein wird. § 15

Befreiung von den KRITIS-Pflichten - § 16 Abs 1

Das **BMI kann** auf Vorschlag von Bundeskanzleramt, BMVG oder auf eigenes Betreiben KRITIS Betreiber von Verpflichtungen nach diesem Gesetz **teilweise (einfacher Ausnahmebescheid)** oder **insgesamt (erweiterter Ausnahmebescheid) befreien**, wenn der KRITIS Betreiber gleichwertige Vorgaben einhält. Warum sollte sowas möglich sein? Und wieso können nicht alle KRITIS Betreiber den Nachweis durch Einhaltung des Stand der Technik bringen - der wirkungsvolle Alternativen ja bereits zulässt? Diese vielen unsinnigen Ausnahmeregelungen und alternativen Vorgehensweisen verkomplizieren die Umsetzung und Einhaltung enorm. Das BMI will anscheinend ein DACH mit Löchern und einem integrierten Wimmelbild der Verantwortungsdiffusion bauen. § 16 Abs 1

KRITIS Betreiber, die

1. in den Bereichen nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung, einschließlich der Ermittlung, Aufdeckung und Verfolgung von Straftaten (relevante Bereiche) tätig sind oder Dienste erbringen, oder
2. ausschließlich für Behörden, die Aufgaben in relevanten Bereichen nach Nummer 1 erfüllen, tätig sind oder Dienste erbringen,

können für diese Tätigkeiten oder Dienste von den Maßnahmen nach § 10 und § 11 und Meldepflichten nach § 12 **befreit** werden. Die Resilienz dieser Betreiber kritischer Anlagen muss in diesen Fällen anderweitig gewährleistet sein und beaufsichtigt werden. Es werden wieder große Teile kritischer Infrastruktur aus dem Sektor “Staat und Verwaltung” ausgeklammert, was aufgrund dieser vielen Ausnahmeregelungen keinem ganzheitlichen Resilienzansatz entspricht. Ebenso ist völlig offen, wie eine solche Beaufsichtigung umgesetzt werden soll. § 16 Abs 2

Evaluation - § 18

Das **BMI** wird das **Gesetz** regelmäßig, spätestens nach Ablauf von fünf Jahren nach Inkrafttreten des Gesetzes auf wissenschaftlich fundierter Grundlage **evaluieren**. Hier macht es sich das BMI wieder einfach, denn schon die Evaluierung des IT-SiG 2.0 war nicht wissenschaftlich und eher minderqualitativ. Dort wurden primär subjektive Einschätzung zur Maßnahmengüte, Effektivität und Komplexität der Umsetzung abgefragt, jedoch keine wissenschaftliche Evaluierung der Gesamtsituation vorgenommen. Eine seltene, erst in fünf Jahren stattfindende Evaluierung wird keinen effektiven Verbesserungsprozess gewährleisten. Stattdessen sollten die Kritierien für eine fortlaufende Evaluation schon mit der Verabschiedung des Gesetzes festgelegt werden. § 18

Bußgelder - § 19

Bußgeldvorschriften sind definiert, aber die Höhe der Bußgelder für die Ordnungswidrigkeiten ist noch nicht formuliert worden. Die Abstimmung mit dem BMJV läuft wohl noch und wird mit Spannung erwartet. § 19

Das Gesetz tritt am Tag der Verkündung in Kraft. Soweit sogut, wann auch immer das sein wird. Laut EU muss das spätestens im Oktober 2024 erfolgen, aber Frau Faeser hat ja angekündigt, dass das noch dieses Jahr kommen soll, weil es eilt. Wir sind gespannt.

Inkrafttreten

Alle **Maßnahmen und Vorgaben** sollen voraussichtlich am **01.01.2026** in Kraft treten. Diese ungewöhnlich lange Frist wird also weitere Jahre der Verzögerungen bei der Umsetzung verursachen.

Die **Bußgeldvorschriften** hingegen sollen erst am **01.01.2027** in Kraft treten. Hier wird es also noch ein Jahr oben drauf als Schonfrist gegeben, weil wir offenbar wirklich viel Zeit haben, diese wichtigen Maßnahmen zu ergreifen?

Anhang 1

(insbesondere zu berücksichtigende Maßnahmen nach § 11 Absatz 1):

Zu den bei einer Abwägung durch den Betreiber kritischer Anlagen zu berücksichtigenden Maßnahmen können insbesondere zählen:

a) um das Auftreten von Vorfällen zu verhindern:

- Maßnahmen der Notfallvorsorge

- Maßnahmen zur Anpassung an den Klimawandel

b) um einen angemessenen physischen Schutz ihrer Räumlichkeiten und Kritischen Infrastrukturen zu gewährleisten:

- Maßnahmen des Objektschutzes, u.a. das Aufstellen von Zäunen und Sperren

- Instrumente und Verfahren für die Überwachung der Umgebung

- Detektionsgeräte

- Zugangskontrollen

c) um auf Vorfälle zu reagieren, sie abzuwehren und die Folgen solcher Vorfälle zu begrenzen:

- Risiko- und Krisenmanagementverfahren und –protokolle

- vorgegebene Abläufe im Alarmfall

d) um nach Vorfällen die Wiederherstellung zu gewährleisten:

- Maßnahmen zur Aufrechterhaltung des Betriebs (z.B. Notstromversorgung)

- Ermittlung alternativer Lieferketten, um die Erbringung des wesentlichen Dienstes wiederaufzunehmen

e) um ein angemessenes Sicherheitsmanagement hinsichtlich der Mitarbeiter zu gewährleisten:

- Festlegung von Kategorien von Personal, das kritische Funktionen wahrnimmt,

- Festlegung von Zugangsrechten zu Räumlichkeiten, kritischen Infrastrukturen und zu sensiblen Informationen

- Berücksichtigung von Verfahren für Zuverlässigkeitsüberprüfungen und Benennung von Kategorien von Personal, die solche Zuverlässigkeitsüberprüfungen durchlaufen müssen; dabei bleiben die Vorschriften der Fachgesetze hinsichtlich der Zuverlässigkeitsüberprüfungen unberührt

- Festlegung angemessener Schulungsanforderungen und Qualifikationen

f) um das entsprechende Personal für die unter den Buchstaben a bis e genannten Maßnahmen zu sensibilisieren:

- Schulungen

- Informationsmaterial

- Übungen

Zur Unterstützung der KRITIS Betreiber stellt das **BBK Vorlagen und Muster** zur Verfügung. Die Maßnahmen sind eine Liste von Ideen, wir befürchten nur, dass sich genau an diesen ausgerichtet wird und alles andere kaum Berücksichtigung finden wird, schade. Wir bezweifeln nicht, dass diese Vorlagen und Muster letztlich hilfreich sein werden (wie auch beim BSI), jedoch wird die Entwicklung viel Zeit beanspruchen und Zeit haben wir in Fragen KRITIS einfach nicht mehr.

Und hier findet Ihr noch den von der AG KRITIS veröffentlichten Entwurfs des KRITIS-DG von Juni 2023.

AG KRITIS

Die AG KRITIS ist ein unabhängiger, ehrenamtlicher Zusammenschluss von Expertinnen und Experten, die sich täglich mit Kritischen Infrastrukturen (KRITIS) gemäß § 2 (10) BSI-Gesetz i. V. m. BSI-Kritisverordnung beschäftigen, z. B. durch Planung, Bau, Betrieb, Beratung oder Prüfung der beteiligten IT-Systeme und Anlagen. Die Arbeitsgruppe ist vollständig unabhängig von Staat und Wirtschaft und vertritt keine Interessen von Unternehmen oder