

24.01.2024

Stellungnahme zum 2. Referentenentwurf (12/2023) des Bundesministeriums des Innern und für Heimat (BMI) für das Gesetz zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz von Betreibern kritischer Anlagen (KRITIS-Dachgesetz – KRITIS-DachG)

Aufbauend auf der schriftlichen und mündlichen Stellungnahme zum ersten Referentenentwurf begrüßt die Allianz der Wissenschaftsorganisationen die deutlich positiven Entwicklungen des zweiten Entwurfs zur Umsetzung der Richtlinie (EU) 2022/2557. Nichtsdestotrotz sorgen insbesondere falsche Begrifflichkeiten sowie die noch unklare Angliederung an die Umsetzung der NIS2-Richtlinie für weiteren Kommentierungsbedarf. Wie zuletzt in der schriftlichen und mündlichen Stellungnahme gliedert sich die aktuelle Kommentierung in einen allgemeinen Teil im Sinne der Politikberatung und einen zweiten Teil aus Sicht der (eigenen) praktischen Umsetzung.

1. Allgemeine Anmerkungen

Fokus auf Organisationsebene ist sinnvoll

Der aus der Richtlinie (EU) 2022/2557 übernommene Fokus auf die Organisationsebene (Betreiber) ist sinnvoll, da diese Perspektive umfassender ist als die für einzelne Anlagen bzw. Dienste. Sie bezieht neben den lokalen ebenso angrenzende Faktoren sowie ggf. relevante prozedurale, organisatorische, personelle usw. Maßnahmen und Abläufe ein, womit auch der All-Gefahrenansatz zur Vorausschau von potentiellen Vorfällen besser berücksichtigt wird. Die Betreiber und insbesondere die Geschäftsführenden in die Verantwortung zu nehmen, wird sich sehr positiv auf die Umsetzungsqualität auswirken. Ggf. könnte man die Schulungsaufgaben etc. nicht verpflichtend an die Person des Geschäftsführenden binden, um eine Option mit einem permanenten (betriebserfahrenen) Mitarbeitenden offen zu lassen, die den Geschäftsführenden berät (ohne diesen aus der Haftung zu nehmen).

Verständnis und Verwendung von Begrifflichkeiten prüfen

Die Richtlinie (EU) 2022/2557, wie auch in großen Teilen des aktuellen Entwurfes übernommen, „legt Verpflichtungen für kritische Einrichtungen fest, die darauf abzielen, *ihre Resilienz und ihre Fähigkeit* zur Erbringung von Diensten ... im Binnenmarkt zu verbessern“.¹

Es geht in diesem Sinne nicht um die Resilienz des Betreibers, sondern seine *Fähigkeit, eine kritische Dienstleistung zu erbringen*. Damit ist bereits der Titel des Gesetzes „physische(n) Resilienz von Betreibern“ wie auch der Begriff „physische Resilienzmaßnahmen“ fachlich und inhaltlich inkorrekt.

So umfasst der Begriff Resilienz deutlich mehr als der Begriff „physischer Schutz“ suggeriert. Auch ist der Begriff „physisch“ keine ausreichende Umschreibung für alles, was nicht-IT/nicht-Cyber ist. Die Resilienzmaßnahmen dürfen daher nicht auf physische eingeschränkt werden. Die möglichen Maßnahmen zur Erhöhung der

¹ CELEX_32022L2557_DE_TXT

Resilienz in der Erbringung kritischer Dienste nach der Richtlinie (EU) 2022/2557 umfassen etwa auch Organisationsanweisungen an das Personal während einer Pandemie; vorsorgliche zusätzliche Kühlwassereservoirs zur Überbrückung bei Dürren oder besseren Versicherungsschutz bei Extremwetterereignissen, um den wirtschaftlichen Schaden zu begrenzen und den kritischen Dienst schnellstmöglich wieder bereitstellen zu können.

Weiterhin wurde der Begriff „physischer Schutz“ hier als Abgrenzung zum aufgeführten Begriff „Cyberschutz“ als Umschreibung der Cybersicherheit in der NIS2-Richtlinie² eingeführt. Bereits Cyberschutz ist jedoch ein nicht ausreichender Begriff für Cybersicherheit und kommt in der NIS2-Richtlinie und deren Umsetzung nicht vor. Im Englischen gibt es die sinnvolle Unterscheidung von *safety* und *security*. Die Richtlinie (EU) 2022/2557 nennt ebenfalls nicht den Begriff „physischer Schutz“, sie spricht maximal von „physischer Sicherheit“ im Gegenpart zur Cybersicherheit in der NIS2-Richtlinie. Allerdings umschreibt diese Formulierung nicht das Anwendungsfeld der Richtlinie (EU) 2022/2557, sondern weist nur darauf hin, dass man Komplementarität erreichen sollte.

Resilienz ist auch nicht unbedingt von Cyber-Elementen abstrahiert. Wie grundsätzlich im Vergleich Sicherheit zu Resilienz bezieht sich auch bei Systemen, Teilsystemen oder Komponenten, die Cyber-Elemente enthalten, der Bereich der Cyber-Resilienz auf die Fähigkeit, durch Cyber-Angriffe verursachte ungünstige Bedingungen *zu antizipieren, ihnen zu widerstehen, sich an sie anzupassen und sie wiederherzustellen*. Sie geht damit deutlich über den Begriff der Sicherheit hinaus. Die NIS2-Richtlinie begrenzt sich auf Cybersicherheit und schließt *bisher nicht* die Resilienz IT-relevanter Systeme mit ein. Somit sollte dies im KRITIS DachG mit abgedeckt werden, damit keine Regelungslücke entsteht.

Darüber hinaus gibt es keine positive Korrelation zwischen physischer Sicherheit und Resilienz. Das heißt, dass eine Erhöhung der physischen Sicherheit die Erbringung kritischer Dienste nicht zwangsläufig resilienter macht.

Einbettung und Abstimmung mit vorhandenen Regelungen

Neben dem vorherigen Punkt ist bisher die Schnittstelle bzw. notwendige gemeinsame Betrachtung der Anwendungsgebiete der beiden Richtlinien nicht ausreichend berücksichtigt. Wie bereits in der Stellungnahme zu dem ersten Referentenentwurf angemerkt, muss das Ziel sein, dass bundeseinheitliche und sektorenübergreifende Vorgaben für die Resilienz kritischer Infrastrukturen geschaffen werden. Diese vielfach berufene Komplementarität der Richtlinien scheint nicht (lückenlos) ausgereift. So ist unklar, in welcher Abschätzung die Risiken betrachtet werden, die aus den Verbindungen zwischen informationstechnischen und nicht-informationstechnischen Systemen entstehen können, um gemeinsamer Betroffenheit bzw. sich gegenseitig bedingende negative Auswirkungen optimal begegnen zu können. Es bleibt zu hoffen, dass die angesprochene Regelung zur „enge(n) Zusammenarbeit der beteiligten Behörden ... im BSIG und im KRITIS-DachG“³ hier ebenfalls zum Tragen kommt. Auch aus dieser Sicht ist es wesentlich, dass immer alle Sektoren abgebildet werden.

Es ist darüber hinaus zu prüfen, ob die Sektoren Bankwesen, Finanz- und Versicherungswesen und Informationstechnik und Telekommunikation von den sich ergebenden Pflichten per se ausgeschlossen sein sollen, um die Möglichkeit zur Erlangung eines höheren Maßes an Resilienz zu gewähren (siehe Artikel 8 Richtlinie (EU) 2022/2557 und etwa kommende und aktuelle Resilienzstrategien in Deutschland). Aufgrund der Unvorhersehbarkeit von in der Zukunft möglichen Risiken erscheint der Ausschluss dieser Sektoren von der Erfüllung der genannten Regelungen sehr gewagt. Es könnten dadurch Schutzlücken entstehen bzw. das maximal mögliche Maß an Resilienz nicht erreicht werden.

² Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz -NIS2UmsuCG) Microsoft Word - CI1_17002_41_22 3-16 (Referentenentwurf NIS2UmsuCG - 03-04-2023 09-00) (intra-pol.org)

³ Siehe aktueller Entwurf.

Meldepflicht und First Response

Die Verbindung zum Katastrophenschutz im Entwurf zum KRITIS-DachG ist nach wie vor kaum befriedigend ausgeführt. Die Informationskette und jeweiligen Schnittstellen zwischen den unteren Katastrophenschutzbehörden bzw. lokalen Behörden und Organisationen mit Sicherheitsaufgaben (BOS) mit den ansässigen Betreibern kritischer Anlagen sollten bundesweit verankert werden, etwa um einen schnellen Informationsfluss oder ein gemeinsames Lagebild sicherzustellen.

Sollte der Betreiber z.B. nicht selbst in der Lage sein, das BBK innerhalb der gesetzlich vorgesehenen Frist zu informieren, sollte die erste Behörde, die von einem Vorfall Kenntnis erlangt, das BBK informieren. Es sollte jedoch auch klar sein, dass die First Response auf einen Vorfall Priorität haben muss, d.h. dass lokale bzw. regionale Behörden noch vor dem BBK eingeschaltet werden, etwa um Evakuierungsmaßnahmen einzuleiten.

Darüber hinaus ist der Ansatz, die BSI-Plattform für Cyber-Vorfälle auf physische Vorfälle zu erweitern, zwar sehr positiv, aber es werden keine Vorfälle berücksichtigt, die entweder falsch klassifiziert werden oder bei denen zu einem späteren Zeitpunkt festgestellt wird, dass sie einen anderen Ursprung haben. Bei einem cyber-physischen Angriff beispielsweise sind die Auswirkungen auf das physische System sofort erkennbar (z. B. Stromausfall), aber die verursachende Malware muss möglicherweise erst forensisch analysiert werden, bevor sie identifiziert wird.

Bestimmung der Schwellenwerte

Die Schwellenwerte für die Identifikation einer kritischen Anlage sollten nicht nur an deren Leistung für eine bestimmte Anzahl zu versorgender Menschen orientiert werden, sondern auch an der von einer erheblichen Störung oder einem erheblichen Vorfall in dieser Anlage betroffenen Personen festgelegt werden (Bsp. Staudammbruch). Die Menge der betroffenen Personen (z.B. in ihrer Gesundheit) kann deutlich größer sein als die Menge der durch eine bestimmte Leistung versorgten Personen.

Auch sollte der pauschale Schwellenwert von 500.000 überdacht werden (siehe auch Richtlinie (EU) 2022/2557 § 7 Abs. 1). Ebenfalls ein Kriterium könnte die Betroffenheit der Souveränität der Bundesrepublik Deutschlands sein, auch wenn sich dies nicht in einer bestimmten Anzahl zu versorgenden oder betroffenen Personen niederschlägt.

Darüber hinaus kann das zusätzliche Kriterium der Abschätzung der Abhängigkeit verschiedener Infrastrukturen von anderen eine methodische Herausforderung darstellen, da diese sehr komplexe Rückkopplungsschleifen bilden können, die ohne sofortige Vereinfachungsannahmen nicht lösbar sind.

Einbezug der Wissenschaft

Wie bereits in der vorherigen Stellungnahme erläutert, erscheint es erforderlich, alle Bundesministerien einzubeziehen, um den Bedarf an Resilienzmaßnahmen abschätzen zu können bzw. das Gesetz in dieser Hinsicht umfänglich zu formulieren. Die Allianz regt daher insbesondere an, dass in § 16 Abs. 1 auch das Einvernehmen mit dem Bundesministerium für Bildung und Forschung hergestellt wird, nicht zuletzt, damit die Bedarfe und Interessen der Wissenschaftseinrichtungen hinreichend berücksichtigt werden können. Weitere detaillierte Vorschläge zur besseren Einbindung von Wissenschaftsorganisationen finden sich in Teil 2 der Stellungnahme.

Fazit

Zusammenfassend lässt sich festhalten, dass der Entwurf dem Ziel einer übergreifenden Regelung im Hinblick auf die Resilienz von Betreibern in der Erbringung kritischer Dienste für alle Sektoren sowie aus wirtschaftlicher und gesellschaftlicher Sicht näherkommt. Ein besseres Verständnis und eine entsprechende Verwendung von Begrifflichkeiten wie „physisch“, „Schutz“, „Sicherheit“ und „Resilienz“ ist notwendig. Der Ausschluss der IT-bezogenen Maßnahmen und die Komplementarität zu entsprechenden Regelungen (etwa BSIG und NIS2 Umsetzung) ist nicht zuletzt mangels parallelen aktuellen Entwurfs der Umsetzung der NIS2 noch nicht

abschließend zu beurteilen. Dies gilt ebenso für die Einbettung in die existierende und kommende weitere Regulierungs-/Richtlinienlandschaft aus dem Bereich, die in der Gesamtheit für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen oder wirtschaftlicher Tätigkeiten im europäischen Binnenmarkt und in Deutschland relevant sind.

2. Konkrete Anmerkungen aus Sicht betroffener Allianz-Organisationen

Es sollte sowohl bei der Umsetzung als auch im untergesetzlichen Regelwerk (Rechtsverordnungen) des KRITIS-DachG kritisch geprüft werden, ob es im Sinne der Richtlinie (EU) 2022/2557 bzw. des KRITIS-DachG ist, dass Einrichtungen/Anlagen, die zu Forschungseinrichtungen gehören (z.B. Anlagen zur Stromerzeugung, Abwasserbehandlung, Wasserstoffherzeugung/-speicherung, Flughäfen, Cloud-Computing-Dienste, Rechenzentrumsdienste), unter das KRITIS-DG fallen sollen. Ob dies der Fall ist, liegt an der Einstufung des jeweiligen Mitgliedsstaates in eine Kategorie (Spalte 3) im Anhang der Richtlinie (EU) 2022/2557 und damit im nationalen Ermessen. Diese Einstufung kann gem. Referentenentwurf des KRITIS-DachG durch den Bund bzw. die Länder erfolgen.

Kritische Anlagen unterliegen einem deutlich höheren Aufwand, sowohl administrativ als auch technisch, durch zusätzlich zu erstellende Risikoanalysen und Risikobewertungen, Meldepflichten und Umsetzung von Resilienzmaßnahmen.

Es ist bei der Ausgestaltung der zu erlassenden Verordnungen darauf zu achten, dass den Betreibern aus den Bereichen Forschung/Wissenschaft, sofern diese durch eine entsprechende Einstufung (s.o.) betroffen sind, zielführende Auflagen gemacht werden. Hier kann durch eine Nichteinstufung von Anlagen, die zu Forschungseinrichtungen gehören, oder das Setzen entsprechend hoher Schwellenwerte, ab dem Anlagen als kritische Anlagen eingestuft werden, eine nicht adäquate Einstufung als kritische Einrichtung vermieden werden. Falls dennoch eine Einstufung getroffen wurde, sollte analog zu den Wirtschaftsverbänden ein entsprechendes Anhörungsrecht erteilt werden.

Daraus folgt, wie bereits in den allgemeinen Anmerkungen aufgeführt, dass die Wissenschaftsorganisationen (Ergänzungsvorschläge in *kursiv*) im Rahmen der im KRITIS-DachG beschriebenen Anhörungen neben den Wirtschaftsverbänden explizit berücksichtigt werden sollten:

§ 10 Resilienzmaßnahmen der Betreiber kritischer Anlagen; Resilienzplan

(4) ... Die betroffenen Betreiber kritischer Anlagen, *die betroffenen Wissenschaftsorganisationen* und die betroffenen Wirtschaftsverbände sind anzuhören.

§ 11 Nachweise; behördliche Anordnungen

(4) ... nach Anhörung von Vertretern der betroffenen Betreiber kritischer Anlagen, *der betroffenen Wissenschaftsorganisationen* und der betroffenen Wirtschaftsverbände...

§ 12 Meldewesen für Vorfälle

(4) ... nach Anhörung der betroffenen Betreiber kritischer Anlagen, *der betroffenen Wissenschaftsorganisationen* und der betroffenen Wirtschaftsverbände und ...

In § 16 „Ermächtigung zum Erlass von Rechtsverordnungen“ sollte konkretisiert werden, wer mit „Vertretern der Wissenschaft“ gemeint ist. Hier wäre die Formulierung „Vertretern der Wissenschaftsorganisationen“ vorzuziehen:

§ 16 Ermächtigung zum Erlass von Rechtsverordnungen

(1) „Das Bundesministerium des Innern und für Heimat bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, nach Anhörung von Vertretern der *Wissenschaftsorganisationen*, der betroffenen Betreibern kritischer Anlagen und Einrichtungen der Bundesverwaltung und Wirtschaftsverbände im Einvernehmen...“

Die Allianz der Wissenschaftsorganisationen ist ein Zusammenschluss der bedeutendsten Wissenschaftsorganisationen in Deutschland. Sie nimmt regelmäßig Stellung zu wichtigen Fragen der Wissenschaftspolitik. Im Jahr 2024 übernimmt die Max-Planck-Gesellschaft die Sprecherrolle für die Allianz. Weitere Mitglieder sind die Alexander von Humboldt-Stiftung, der Deutsche Akademische Austauschdienst, die Deutsche Forschungsgemeinschaft, die Fraunhofer-Gesellschaft, die Helmholtz-Gemeinschaft, die Hochschulrektorenkonferenz, die Leibniz-Gemeinschaft, die Nationale Akademie der Wissenschaften Leopoldina und der Wissenschaftsrat.