Positionspapier zum Referenten-Entwurf des BMI zum KRITIS Dachgesetz vom 21.12.2023

UP KRITIS

Die Wirtschaftsvertreter des UP KRITIS begrüßen weiterhin die nationale Implementierung der CER-Richtlinie. Mit diesem Gesetzesvorschlag die CER-Richtlinie umzusetzen und gleichzeitig für Deutschland einen Start für die Regulierung des sektorübergreifenden und sektorspezifischen physischen Schutzes zu finden, ist nun deutlicher zu erkennen (z.B. kleinerer Scope als im NIS2UmsuCG, Themen wie „Komponentenbeschaffung“ sind entfallen). Es sollten jedoch unbedingt bis zur ersten Evaluierung des Gesetzes noch weitere Anpassungen vorgenommen werden, um gemeinsam mit dem Thema zielführend und auch praxisgerecht zu starten und erst danach Verbesserungen anzugehen. Hier bietet es sich dringend an, uns noch mehr an dem erfolgreichen Beispiel zur Einführung des IT-Sicherheitsgesetzes zu orientieren. Um dieses Ziel zu erreichen, weist der UP KRITIS in dieser Stellungnahme auf einige Themen hin, bei denen Verbesserungspotential erkannt wurde.

Übergreifend ist immer noch festzustellen, dass Voraussetzungen noch nicht geschaffen sind, um eine vollständige Bewertung (inhaltlich und monetär) des Gesetzesentwurfes vorzunehmen. Zum Beispiel fehlt die nationale Risikoanalyse bzw. die Kenntnis auf welcher Detailtiefe welche Themenstellungen in dieser adressiert werden und somit auch die zu betrachtende Szenarien für die betrieblichen Risikoanalyse und deren Maßnahmenableitung und Kostenabschätzungen. Auch das die Rechtsverordnung nach § 16 noch nicht vorliegt, erschwert eine Gesamtbeurteilung. Der UP KRITIS trifft die Annahme, dass dieses Gesetz die KRITIS Betreiber betrifft, die mehr oder weniger zur Zeit von der IT-Sicherheitsgesetzgebung betroffen sind (ca. 2.000 Unternehmen). Der UP KRITIS bietet an, gemeinsam steuerbare Risiken und auch betroffene Branchen und kritischen Dienstleistungen zu identifizieren.

Der UP KRITIS bedauert, dass der Kommentierungs-Entwurf zum NIS2UmsuCG immer noch nicht vorliegt, um erkennen zu können, ob diese beiden Gesetze zum Thema nationaler Sicherheit ineinandergreifen, sich ergänzen und nicht doppelt regulieren.

Es gibt keine Angaben zu den Bußgeldhöhen, wodurch hierzu keine detaillierte Betrachtung durch den UP KRITIS erfolgen kann. Den Ansatz, erst zu einem späteren, noch nicht endgültig definierten Zeitpunkt Bußgelder einzuführen, kann der UP KRITIS nachvollziehen, sieht aber Verbesserungspotential.

Der UP KRITIS verzichtet hier auf Formulierungsvorschläge, da diese auch von Branchenverbänden eingereicht werden und versucht mit dieser Stellungnahme das Thema grundsätzlich zu betrachten. Wir übersenden unsere Detail-Hinweise in der angehangenen Tabelle und einen uns wichtigen Vorschlag zur Zeitschiene und Abhängigkeiten insbesondere im Bezug zu Vorgaben und Auswahl geeigneter Schutzmaßnahmen nach §10 (1) mit dieser Stellungnahme zur weiteren Verwendung.

Zur effektiven und kosteneffizienten Erhöhung der sektorübergreifenden physischen Sicherheit, weisen wir auf folgende Verbesserungsmöglichkeiten hin und hoffen auf eine praxistaugliche nationale Umsetzung unter Einbeziehung der Wirtschaft unter anderem auch durch einen Anhörungstermin zu diesem Referentenentwurf.

Themenschwerpunkte

1. **Berücksichtigung von inhaltlichen und zeitlichen Abhängigkeiten sowie der betrieblichen Praxis bei der Auswahl und Festlegung von Maßnahmen zur Resilienz nach Artikel 1, §10 (1)**
   Die angehangene „Zeitschiene“ mit den Abhängigkeiten zeigt sehr deutlich, dass die Umsetzung des Gesetzes in der vorliegenden Fassung in der betrieblichen Praxis nicht möglich ist. Die Rechtsverordnungen und Kataloge von Mindeststandards aus §10 (4) und (5), sollten im Artikel 2 ausgelagert werden und später deren Notwendigkeit bei der Evaluierung des Gesetzes geprüft werden. Die Einführung des IT-Sicherheitsgesetzes hat gezeigt, dass die Wirtschaft mit Ihren Branchenverbänden im ersten Schritt auch ohne derartige Rechtsvorgaben oder Mindeststandards von behördlicher Seite geeignete Maßnahmen und Prozesse etablieren konnten. Dieser Weg ist mit dem in §10 (6) angedachten branchenspezifischen Mindeststandards ermöglicht und würde einen risikobasierten Ansatz ermöglichen. Leitplanken zur Orientierung hierzu sind nach Sicht des UP KRITIS im §10 (1) und (3) ausreichend vorgegeben.

2. **Erfüllungsaufwand für die Wirtschaft**
   Trotz der noch unklaren konkreten Ausführung zu Betroffenheit von Unternehmen und Detailtiefe, welche Themenstellungen in den Regelungen wie adressiert werden, haben die Wirtschaftsvertreter auf den Erfahrungen des IT-Sicherheitsgesetzes und den bisherigen Gesprächen mit dem BMI zum KRITIS-DachG erste vorsichtige Kostenschätzungen vorgenommen.
   Im Verhältnis zu den unter E3 für die Verwaltung mit „erheblichen Erfüllungsaufwand“ bezeichneten Kosten entstehen jedem betroffenen Unternehmen mindestens ein ähnlicher Kostenaufwand, so dass unter E2 zur klaren Information des Gesetzgebers im Minimum ebenfalls von „erheblichem Erfüllungsaufwand für alle betroffene Unternehmen“ zu sprechen ist. In dieser Betrachtung sind noch keine etwaig notwendigen technischen, baulichen Maßnahmen enthalten.

3. **Zuständigkeiten in der Durchsetzung und Aufsicht**
   Im vorliegenden Gesetzesentwurf sind die Behördenzuständigkeiten zum Thema Durchsetzung und Aufsicht nicht eindeutig geregelt bzw. lassen die Vermutung zu, dass betroffene Unternehmen (insb. „Verbundunternehmen“) im Rahmen der Bundes- und Landeshoheit verschiedenen Regelungen z.B. bei der „Nachweiserbringung“ befolgen müssen. Hier ist eine Harmonisierung dringend erforderlich.

4. **Vermeidung von Mehrfachregulierung: Harmonisierung der gesetzlichen Regelungen**
   Wir empfehlen die ausschließliche Regulierung von physikalischen Sicherheitsthemen. Eine Harmonisierung der Gesetzlichen Regelungen bzgl. Begriffsbestimmungen und deren Anwendung ist zwingend erforderlich.

5. **Identifizierung von betroffenen Unternehmen**
   Wir begrüßen, dass im Gesetz die Rahmenbedingungen zur Rechtsverordnung nun festgeschrieben sind. Beteiligung der Wirtschaft bei der Ausgestaltung der Rechtsverordnung ist weiterhin gewünscht.

6. **Risikobetrachtung**
   Es sollte auf die KRITIS-Verordnung referenziert werden und nur die Versorgungssicherheit als Kriterium herangezogen werden. Wir begrüßen die sektorspezifischen nationalen Risikoanalysen. Diese sollten unter Beteiligung der Wirtschaft erstellt werden.

7. Registrierungspflicht, Benennung Kontaktstelle

Es soll ein gemeinsames Online-Portal (bestenfalls gleichzeitig auch als Meldeportal für Störungen und Portal um alle notwendigen Nachweise zu erbringen) für das NIS2UmsuCG und das KRITIS DachG betrieben werden. Aufgrund der Sensibilität der Daten muss dieses Portal besonderen Sicherheitsanforderungen genügen. Hier sollten auch alle zukünftig zuständigen Behören ihren notwendigen Zugriff erhalten. Diese Daten dürfen nur zum Zwecke der Gefahrenabwehr genutzt werden.

8. Zu ergreifende Maßnahmen

Den Wirtschaftsvertretern des UP KRITIS ist nicht klar, was mit einem „Resilienzplan“ adressiert werden soll. Dies sollte konkretisiert werden. Es sollte darauf hingewiesen werden, dass bereits eine zielführende und praxisgerechte Planung von notwendigen Maßnahmen und deren entsprechende spätere Umsetzung ausreicht, um dem Ziel dieses Gesetzes gerecht zu werden. Bauliche Maßnahmen können Monate/Jahre in Anspruch nehmen.

9. Meldewesen

Es sollte weiterhin der Grundsatz „Ein Vorfall - Eine Meldung“ gelten. Daneben ist anzumerken, dass ein Informationsfluss vom BBK an die Betreiber der kritischen Anlagen weiterhin nicht angedacht ist.

10. Bußgeldvorschriften

Der UP KRITIS schlägt vor, zumindest bis zur ersten regulären Evaluierung des Gesetzes, den Ansatz zur Bußgeldhöhe des IT-SIG 1.0 zu wählen und nicht den des NIS2UmsCG.

Weitere Detailhinweise

1. Berücksichtigung von zeitlichen und inhaltlichen Abhängigkeiten sowie der betrieblichen Praxis bei der Auswahl und Festlegung von Maßnahmen zur Resilienz nach Artikel 1 §10 (1)

Die angehangene „Zeitschiene“ mit den Abhängigkeiten zeigt sehr deutlich, dass die Umsetzung des Gesetzes in der vorliegenden Fassung in der betrieblichen Praxis nicht möglich ist. Die dort aufgezeigten Abhängigkeiten machen klar, das betriebliche Notwendigkeiten bei der Gesamtausgestaltung zu berücksichtigen sind (Risikoidentifizierung, Maßnahmenidentifizierung und -planung, Budgetierung, Ausschreibungsverfahren, Beantragung von etwaigen baulichen Genehmigungen, bis zur Umsetzung). Erschwert wird das Thema in der augenblicklichen Fassung insbesondere durch die fehlende Planungssicherheit, die die angedachten, aber noch nicht existierenden behördlichen Vorgaben zur Ausgestaltung der Resilienzmaßnahmen nach §10 (1) mit sich bringen!

Aus Sicht des UP KRITIS, sollten somit die Rechtsverordnungen und Kataloge von Mindeststandards aus §10 (4) und (5), in den Artikel 2 ausgelagert und die Inkraftsetzung in Abhängigkeit zur Evaluierung gesetzt werden. Somit kann später deren Notwendigkeit im Rahmen der Evaluierung des Gesetzes geprüft werden. Dieses ist zurzeit schon für die sektorspezifischen Rechtsverordnungen der Länder so vorgehsehen und sollte auf Bundesvorgaben ausgeweitet werden. Somit würde das Thema der Ausgestaltung des §10 (1) für die Länder und den Bund in der ersten Fassung gleichbehandelt werden und dort keinen bis kaum Aufwand erzeugen.

Die Einführung des IT-Sicherheitsgesetzes hat nachweislich gezeigt, dass die Wirtschaft mit ihren Branchenverbänden auch ohne derartige Rechtsvorgaben oder Mindeststandards von behördlicher Seite geeignete Maßnahmen und Prozesse (branchenspezifischen Sicherheitsstandards) etablieren konnte. Bis auf die Rechtsverordnung zur Bestimmung von KRITIS Betreibern nach BSI-KRITIS VO wurde im Rahmen der Einführung des IT-Sicherheitsgesetzes auf die Nutzung dieses Rechtsmittels zur Vorgabe von Maßnahmen in den letzten 8 Jahren verzichtet und wir konnten im europäischen Vergleich in Deutschland ein sehr hohes Sicherheitsniveau erreichen. Es ist zusätzlich davon auszugehen, dass die zukünftig betroffenen Unternehmen auch schon Heute, u.a. aufgrund von bereits existierenden rechtlichen Rahmenbedingungen (aus IT-SIG oder UVV, etc.), insbesondere, auch im eigenen Interesse und nach Risikoabwägungen, ein geeignetes Maß an physischen Maßnahmen etabliert haben.

Es kann auf weitere Vorgaben zu Resilienzmaßnahmen von behördlicher Seite aus Sicht des UP KRITIS auch verzichtet werden, da mit den in §10 (6) angedachten zu entwickelnden branchenspezifischen Mindeststandards, unter Berücksichtigung der „Leitplanken“ aus §10 (1) und (3) ein praxisnaher und vor allem risikobasierten Ansatz ermöglicht würde.

Sollte das Instrument der Rechtsverordnung trotz unserer dringenden Empfehlung weiter angedacht sein, ist die Wirtschaft mit ihren Branchenverbänden zwingend in deren Erstellung einzubeziehen, damit deren Erfahrung hier einfließen kann und praxistaugliche Vorgaben zur Ausgestaltung des §10 (1) entstehen können. Zudem sollte dieser Eingriff das letzte Mittel der Wahl sein. Des Weiteren ist auf der Zeitachse diese Einflussnahme in die betrieblichen Abläufe zu berücksichtigen und angemessene Umsetzungsfristen zur Berücksichtigung dieser Vorgaben vorzusehen. Dieses kann bei baulichen Maßnahmen sehr schnell mehrere Jahre in Anspruch nehmen.

2. Vermeidung von Mehrfachregulierung: Harmonisierung der Gesetzlichen Regelungen

Hierzu müssen Begrifflichkeiten in allen deutschen Gesetzen einheitlich gewählt und genutzt und nicht doppelt definiert werden. Eindeutige, einheitliche und konsistente Verwendung ist hier zwingend erforderlich. Doppelung von Pflichten (z.B. Registrierungs-, Nachweis- und Meldepflichten sowie die Umsetzung von Maßnahmen) aus den unterschiedlichsten nationalen Gesetzen wie dem BSIG, EnWG, TKG,

KRITIS DachG usw. und europäischen Regulierungsvorgaben müssen vermieden werden. Zudem dürfen spezialrechtliche Normen und Bescheide von Fachbehörden sowie deren Zweckmäßigkeit durch das BBK nicht in Frage gestellt werden.

Eine Doppelung von Bußgeldern für den gleichen Sachverhalt muss ausgeschlossen sein.

Da das NISUmsuCG noch nicht vorliegt, besteht hier die große Gefahr, dass die Bestimmungen der Gesetze auseinanderlaufen und die Betreiber/Unternehmen hier in naher Zukunft bei der Umsetzung Probleme bekommen.

Die Behördenzuständigkeit muss klar geregelt und für die Wirtschaft erkennbar sein. Auch hier dürfen keine sich überschneidenden Zuständigkeiten geschaffen werden und die zuständige Behörde muss in die Lage versetzt werden diesen Pflichten nachzukommen. Nicht zuletzt, damit behördliche Prozesse, von denen die Betreiber abhängen, auch frist- und sachgerecht abgearbeitet werden können (z.B. nationale Risikoanalyse).

Für Unternehmen, die zukünftig sowohl nach NISUmsuCG als auch nach KRITIS DachG den Nachweispflichten unterliegen, muss eine Behörde mit der Aufgabe der Gesamtkoordination benannt werden, welche bei etwaigen Überschneidungen, die sich ggf. auch bei sehr guter gesetzlicher Regelung der Zuständigkeiten nicht vollständig vermeiden lassen, eine für alle Seiten bindende Entscheidung treffen darf. Die Erbringung von Nachweisen durch Audits muss in Form von „Gesamtaudits“ für Anforderungen nach NISUmsuCG und nach KRITIS DachG möglich sein.

3. Identifizierung von betroffenen Unternehmen

Die Wirtschaftsvertreter des UP KRITIS sehen bei der Identifizierung von kritischen Anlagen auch die Notwendigkeit die öffentliche Bundesverwaltung, insbesondere rund um die öffentliche Sicherheit, mit einzubeziehen (auch hier sollten der gleiche Maßstab angesetzt werden, wenn eine Bundesverwaltung für mehr als 500.000 Mitbürger zuständig ist, sollte diese im Scope des Gesetzes sein). Des Weiteren sind die Betreiber kritischer Anlagen im Falle einer großflächigen Krise, welche durch das BBK koordiniert werden soll, auch von dem BBK abhängig. Für solche Fälle muss das BBK auch in die Lage versetzt werden dieser Verpflichtung nachzukommen und nicht selbst durch sicherheitstechnische Probleme handlungsunfähig sein. Somit sieht der UP KRIITS den § 17 (Ausnahmebescheid) als sehr kritisch an.

4. Risikobetrachtung

Regelungsinhalte wie "oder andere dramatische Folgen eintreten würden" oder "erhebliche Störungen der wirtschaftlichen Tätigkeit" sind nicht eindeutig (jedes Unternehmen wird darunter was anderes verstehen). Bisher wurde die Versorgungssicherheit adressiert. Hier fehlen die Kriterien wann etwas erheblich oder dramatisch ist.

Wir begrüßen, dass auf betrieblicher Ebene die Wirtschaftlichkeit bei der Auswahl der Maßnahmen mitberücksichtigt wird. Dies sollte nicht nur in der Gesetzesbegründung, sondern auch im Gesetzestext vermerkt sein. Die Wirtschaftlichkeit ist die Vorrausetzung, dass ein Unternehmen eine Dienstleistung anbietet.

Wir begrüßen die sektorspezifischen nationalen Risikoanalysen, um die Besonderheiten des jeweiligen Sektors berücksichtigen zu können. Bei den nationalen Risikoanalysen und -bewertungen sollten die Wirtschaftsverbände beteiligt werden, um die behördliche Sicht mit den Praxiserfahrungen zu spiegeln und sektor- und branchenspezifische Risiken zu ergänzen. Dieses wird auch von der CER-Richtlinie vorgesehen.

Bestimmte durch die nationalen Risikoanalysen und -bewertungen identifizierte Risiken (z.B. Sabotageakte, die durch terroristische Vereinigungen oder durch Drittstaaten verübt werden) können durch die Betreiber kritischer Anlagen in ihren Resilienzplänen nur bedingt berücksichtigt werden. In diesen Fällen sollten Bund und Länder auch im Sinne der EU-Richtlinien zum Schutz Kritischer Infrastrukturen (CER-Richtlinie) die Betreiber kritischer Anlagen bzw. die kritischen Anlagen angemessen schützen.

Problematik: Berücksichtigung von Abhängigkeiten bei den betrieblichen Risikoanalysen. Im Energiesektor z.B. würden die Risiken ins unendliche reichen (Blackout Kaskadeneffekt auf Europa)! Beim ITSiG wurden diese Effekte mit gutem Grund ausgeblendet, da sonst keine wirtschaftliche Betrachtung der Risiken und der zu ergreifenden Maßnahmen möglich sind. Sicherheitsmaßnahmen müssen für die betroffenen Unternehmen wirtschaftlich vertretbar sein.

Die Risikobetrachtung ist bisher sehr statisch. Es muss die Möglichkeit bestehen, Anpassungen an aktuelle Risikolagen vorzunehmen und unbürokratisch Maßnahmen zu implementieren. Ein Hinweis, das auch abweichend von dem Risiko-Life-Cycle relevante kritische Sachverhalte geeignet Berücksichtigung finden sollten, sind mit aufzunehmen.

5. Zeitliche Abfolge

Die angedachten Stichtage und Zeiträume bei der Implementierung des Gesetzes müssen zwingend überarbeitet werden (siehe mitgelieferte „Zeitschiene“). Zum Beispiel können die betrieblichen Risikoanalysen erst nach den nationalen Risikoanalysen durchgeführt werden. Dann braucht es die Resilienzstandards, um geeignete Maßnahmen zu identifizieren, die diesen Risiken entgegenwirken. Im Anschluss müssen diese Maßnahmen implementiert werden. Dieser Zusammenhang muss durch den Gesetzgeber berücksichtigt werden.

Die übermittelte „Zeitschiene“ lässt klar erkennen, dass es hier noch einer Justierung bedarf. Der UP KRITIS hat einen ersten Vorschlag erarbeitet (Siehe Anlage KRITIS-DachG-Vers1.xls „Vorschlag „Timeline““), um hier eine praxistaugliche Umsetzung zu gewährleisen und steht für einen intensiveren Austausch zu dem Thema zur Verfügung.

6. Registrierungspflicht, Benennung Kontaktstelle

Es soll ein gemeinsames Online-Portal (bestenfalls gleichzeitig auch als Meldeportal für Störungen und Portal um alle notwendigen Nachweise zu erbringen) für das NIS2UmsuCG und das KRITIS DachG betrieben werden. Hierbei muss sichergestellt werden, das Unternehmen auch in geeigneter Art und Weise Daten einpflegen können (z.B. nicht nur Online in „Echtzeit“, sondern auch vorbereitend die notwendigen Datenabfragen zur Verfügung gestellt werden). Da es sich um sehr sensible Daten handelt, muss dieses Portal IT-technisch sicher betrieben und den betroffenen Unternehmen ein geeigneter Zugang eingerichtet werden. Listen, die das BBK aus diesem Portal entnimmt (z.B. Liste aller Betreiber kritischer Anlagen) müssen vertraulich (Vertraulichkeit, Geheimhaltung) behandelt werden und dürfen nicht veröffentlicht werden und zweckgebunden sein. Das BBK/BSI muss entsprechende Schutzmaßnahmen ergreifen, um die Vertraulichkeit zu gewährleisten.

Auf Unternehmensseite sollte keine Personen als Kontakt definiert werden können, sondern Funktionen (24/7 Erreichbarkeit).

7. Zu ergreifende Maßnahmen

Hier wird bei zukünftig zu implementierenden Maßnahmen auch auf den Stand der Technik verwiesen, somit u.a. die zukünftigen branchenspezifischen Resilienzstandards. Hierbei ist zwingend ein Bestandsschutz der bereits etablierten Sicherheitsmaßnahmen unter dem Aspekt der Wirtschaftlichkeit und Funktionalität zu berücksichtigen. In der Regel ist es Betreibern nicht möglich, zeitnah großflächig Sicherheitsinfrastruktur auszutauschen.

Den Wirtschaftsvertretern des UP KRITIS ist nicht klar, was mit einem „Resilienzplan“ adressiert ist. Sind damit,

a) Maßnahmen die bereits implementiert sind, oder

b) ergänzende und neue Maßnahmen die zukünftig implementiert werden sollen, da noch Maßnahmen fehlen, oder

c) Beides (a) und b)) adressiert.

Wichtig hierbei ist, dass die Identifizierung und angemessene zeitliche Planung von notwendigen Maßnahmen (unter Berücksichtigung der betrieblichen Praxis wie z.B. die Budgetplanung, Ausschreibungsprozesse/-fristen, Einholung von Baugenehmigungen, etc…) als ausreichende Erfüllung der Anforderungen anerkannt werden muss.

Die gewählte Detailtiefe in den Resilienzplänen, die evtl. der zuständigen Behörde als Nachweis zur Verfügung gestellt werden müssen (inklusive Informationen aus der Risikoanalyse, die zu der Auswahl der Maßnahme führten), sind für Maßnahmenpläne weder praxisüblich noch notwendig. Die anforderungsgemäß enthaltenen Informationen können je nach Detailtiefe äußerst sensibel sein.

8. Meldewesen

Auch hier verweisen wir auf das zentrale Portal, welches auch als „Meldeportal“ fungieren soll.

Neben den Meldungen im dem zentralen Meldeportal an das BBK/BSI, welche bei Bedarf an die BNetzA (auch für Meldeprozesse, die es diesbezüglich in Richtung Versorgungssicherheit schon gibt, z.B., EnWG §52), dem BKA oder dem Verfassungsschutz weitergegeben werden, wäre es wünschenswert auch weitere behördliche Meldeprozesse bei Sicherheitsvorfällen hierüber zu unterstützen (z.B. Datenschutzbehörden, sonstige Aufsichtsbehörden). Im Finanzsektor ist dieses durch DORA bereits umgesetzt.

Ein Vorfall - Eine Meldung!

Es fehlt ein Informationsfluss vom BBK an die Betreiber der kritischen Anlagen. Hier müssen zeitnah Warnungen über nationale/europäische physikalische Störungen/Bedrohungen/Risiken vom BBK an die Betreiber fließen. Dieses ist auch im BSIG bzw. NIS2UmsuCG so geregelt und hilft den Betreibern sich gegen dolose Handlungen zu schützen, bzw. diese bei Ihren Risikobetrachtungen zu berücksichtigen.

9. Bußgeldvorschriften

Der UP KRITIS schlägt vor, zumindest bis zur ersten regulären Evaluierung des Gesetzes, den Ansatz zur Bußgeldhöhe des IT-SIG 1.0 zu wählen und nicht den des NIS2UmsCG. Die maßnahmenbezogenen Bußgeldvorschriften erst einzuführen, nachdem es branchenspezifische Resilienzstandards gibt, scheint dem UP KRITIS zielführend. Hier muss jedoch eine Umsetzungsfrist eingeplant werden, damit diese Standards bei Risikoanalysen, Maßnahmenplanungen und -umsetzungen berücksichtigt werden können.

10. Besondere Behandlung von Betreibern kritischer Anlagen

Mit diesem Gesetz sollte klar definiert werden, dass Kritische Infrastrukturen einen besonderen Status bei der Bewertung von Vorfällen haben. Z.B. bei einer Pandemie müssen trotz Ausgangssperren, Mitarbeiter von Betreibern kritischer Anlagen noch Zutritt zu den Anlagen ermöglicht werden. Bei Hochwassersituationen sollten Betreiber kritischer Anlagen bevorzugt unterstützt werden, damit die Kritische Infrastruktur vorrangig wieder in Betrieb genommen werden kann bzw. geschützt bleibt.

Bei Verwaltungsentscheidung sollten Maßnahmen zur Steigerung der notwendigen Resilienz bei Betreibern von kritischen Anlagen mit besonderem Gewicht berücksichtigt werden (z.B. Sicherheit vor Denkmalschutz oder Sicherheit vor Transparenzpflichten).

11. Personalüberprüfung

Zurzeit sind personelle Sicherheitsüberprüfungen nur sehr eingeschränkt möglich (außer Telekommunikation/ÜNB/teilweise VNB). Nur die Nutzung von Terrorlisten/Sanktionslisten bei

Bestandspersonal und polizeiliche Führungszeugnisse bei Einstellung sind Möglichkeiten, das Thema abzudecken.

Unternehmen sollte die Möglichkeit eingeräumt werden, Personal mit sicherheitskritischen Aufgaben zu überprüfen/überprüfen zu lassen bzw. in die Lage zu versetzen, sich mit Sicherheitsbehörden auszutauschen. Hierzu sollte der Staat in diesem Gesetz eine Grundlage für Unternehmen schaffen. Ohne gesetzliche Grundlage sind „Überprüfungsmaßnahmen“ nach DSGVO untersagt.

Gleichzeitig unterstützen wir, dass entsprechende bereits existierende Vorschriften über Zuverlässigkeitsüberprüfungen unberührt bleiben.

12. Evaluierung

Wenn wir den Gesamtzeitablauf sehen, scheinen 5 Jahre für eine Evaluierung angemessen, insbesondere wenn zu diesem Zeitpunkt über die Notwendigkeit der Einführung zu weiteren Vorgaben bzgl. implementierender Maßnahmen entschieden werden soll. Es sollte jederzeit die Möglichkeit bestehen auf veränderte Sicherheitslagen unter Einbeziehung der Wirtschaft zu reagieren. Hiermit soll sichergestellt werden, dass die Auswirkungen auf die Wirtschaft berücksichtigt werden und für die Betreiber der Kritischen Anlagen Planungssicherheit gegeben ist.

Zum regulären Evaluierungszeitpunkt können auch die Kosten der Umsetzung (einmalig und fortlaufend (CAPEX/OPEX) benannt werden. Wir empfehlen eine zentrale Abfrage über das Bundesamt für Statistik.

13. Inkrafttreten

Der UP KRITIS schlägt dringend vor, §10 (4) und (5) des Artikel 1 in den Artikel 2 zu überführen. Hier ist auch das Thema der sektorspezifischen Rechtsverordnungen zur Ausgestaltung des §10 (1) angesiedelt. Beide Absätze sollten im Artikel 3 erst nach der Evaluierung des Gesetzes (2029/30) in Kraft gesetzt werden. Zu diesem Zeitpunkt kann geprüft werden, ob diese Verordnungen und Mindeststandards notwendig sind, um das Ziel zu erreichen und etwaige zusätzliche Regelungen können in der betrieblichen Praxis im Risiko-Life-Cycle berücksichtig werden.