

Stellungnahme

Zum Entwurf eines Gesetzes zur Umsetzung der CER-Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz von Betreibern kritischer Anlagen

Im Allgemeinen

Der Schutz der IT-Sicherheit von Kritischen Infrastrukturen ist derzeit im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) geregelt. Durch die Umsetzung der NIS-2-Richtlinie mit dem NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) werden die Regelungen zum Cyberschutz von Kritischen Infrastrukturen und weiteren wichtigen Einrichtungen weiterentwickelt. Das KRITIS-DachG soll neben diese Regelungen treten und den physischen Schutz kritischer Anlagen regeln.

Es wäre wünschenswert gewesen, die beiden Referentenentwürfe aufgrund der inhaltlichen Zusammenhänge zumindest parallel zur Diskussion zu stellen. Wir hätten daher ein gemeinsames Gesetzgebungsverfahren als sinnvoller erachtet. Da dies nun bedauerlicherweise nicht der Fall ist, sollte mindestens auf eine Harmonisierung der Regelungen geachtet werden. Wir sehen vor allem Bedarf bei den verwendeten Begriffen und Definitionen, in Bezug auf die Umsetzungsprozesse und die Kompetenzen der beteiligten Behörden. Mit der parallelen Behandlung physischer und cybersicherheitsrelevanter Verpflichtungen in zwei unterschiedlichen Gesetzgebungsverfahren besteht von Natur aus die Gefahr von Doppelregulierung und Inkonsistenzen. Die parallelen Gesetzesvorschläge führen zu einer komplexen Vorgabesystematik, deren wechselseitige Abhängigkeiten und Zuständigkeiten der einzelnen Behörden eine Umsetzung für Unternehmen unnötig erschweren. Dabei sollten – im Gegenteil – der Dokumentationsaufwand und zusätzliche bürokratische Belastungen minimiert werden, um nicht unnötig Kapazitäten zu binden, die die Unternehmen in die Verbesserung ihrer Sicherheitsvorkehrungen investieren könnten. Die Aufteilung in zwei getrennte Gesetzgebungsverfahren erschwert es den Unternehmen zusätzlich, die eigene Betroffenheit überhaupt festzustellen, die jeweils relevanten Anforderungen abzuleiten und rechtskonform umzusetzen.

Insbesondere vor dem Hintergrund, dass mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zwei unterschiedliche Aufsichtsbehörden für die Umsetzung des KRITIS-DachG und des NIS2UmsuCG verantwortlich zeichnen, die sich wiederum mit weiteren sektorspezifischen Aufsichtsbehörden vernetzen müssen, sollten die Prozesse der Zusammenarbeit zwischen den Behörden klar definiert werden. Nur so lässt sich Doppelaufwand für die Unternehmen, z. B. durch Mehrfachmeldungen, verhindern und effektive Warnhinweise an die Unternehmen gewährleisten. Alle Maßnahmen müssen darauf hinwirken, das Schutzniveau der Unternehmen zu verbessern und deren eigene

Sicherheitsbemühungen zu unterstützen. Eine angemessene personelle Ausstattung der Behörden ist dafür eine weitere Voraussetzung.

Der vorgeschlagene Regelungsrahmen insgesamt (inkl. NIS2UmsuCG) erhöht für potenziell betroffene Unternehmen die Komplexität der zukünftig beachtlichen Pflichten zur Umsetzung und Dokumentation von betrieblichen Maßnahmen. Wiederum werden wesentliche Inhalte, die über die Betroffenheit bestimmen, in nachrangige Rechtsakte mit geringeren Beteiligungsmöglichkeiten für die Wirtschaftsverbände verlagert.

Grundsätzlich weisen wir an dieser Stelle darauf hin, dass sich die Kommentierung des Gesetzentwurfs aufgrund der fehlenden Rechtsverordnung insgesamt als schwierig gestaltet, weil so für die Unternehmen ihre tatsächliche Betroffenheit schwer abschätzbar ist.

Darüber hinaus gilt, dass die Geschäftsprozesse der Unternehmen nicht ohne konkreten Anlass disruptiv verändert werden dürfen und dass die gesetzlich veranlassten Maßnahmen die Fortführung unternehmerischer Prozesse zulassen bzw. ermöglichen müssen. Dies betrifft unter anderem Aspekte wie die Cybersicherheit, Verhaltensregeln für Mitarbeitende, robuste analoge Ersatzprozesse und die Schadensminimierung im Angriffsfall bis zur Herstellung einer dauerhaften und hinreichenden Robustheit aller relevanten unternehmensinternen und -übergreifenden Prozesse.

Hier wäre ein konsistenter Ordnungsrahmen hilfreich, der den Unternehmen verlässliche Orientierung gibt und größtmögliche Transparenz über die rechtlichen Verpflichtungen herstellt.

Im Einzelnen

§ 4 Abs. 1

Positiv ist zu bewerten, dass die Systematik zur Bestimmung von KRITIS grundsätzlich beibehalten werden soll und auch im Gesetzentwurf explizit festgehalten wurde.

§ 4 Abs. 2

Behörden können nach entsprechendem Ermessen zukünftig einseitig die Identifizierung als Betreiber kritischer Anlagen vornehmen. Dies ist als problematisch zu bewerten. Hierfür maßgebliche Kriterien sind zwar im Referentenentwurf aufgeführt, jedoch erscheinen diese weder als abschließende Aufzählung noch sind sie spezifisch, da beispielsweise sowohl „Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten“ (Nummer 3) als auch der „Marktanteil des Betreibers“ (Nummer 4) nicht näher eingegrenzt werden.

Die dem Bundesinnenministerium zugebilligte Befugnis zur Festlegung weiterer Betreiber kritischer Anlagen unter Berücksichtigung der nationalen Risikoanalysen und Risikobewertungen nach § 8 erscheint ohne Kenntnis der Rechtsverordnung nach § 16 als

zu weitgehend. Soweit eine Anlehnung an den bestehenden Rahmen der BSI-KritisV beabsichtigt sein sollte, sollte dies klar formuliert sein. Derzeit ist unklar, welche Erwägungen überhaupt dafür maßgeblich sein könnten, den Anwendungsbereich in Abweichung von den Regelschwellenwerten auszuweiten.

Vielmehr sehen wir die Möglichkeit, dass eine Freiheit des Bundesinnenministeriums oder anderer Behörden, Festlegungen zu treffen, zu Lasten eines konsistenten, an klaren Maßstäben ausgerichteten Regelungsrahmens ginge und zudem Raum für eher opportunistische (also tagespolitischen Erwägungen folgende) Vorschläge zur Ausdehnung der Regulierung schafft.

§ 4 Abs. 7 und 8

Unklar sind uns bisher die Folgen des Verhältnisses anderer Regelungen zum vorliegenden Gesetz. Offenbar bleiben die Pflichten zur gesonderten Dokumentation der getroffenen Maßnahmen weiter bestehen (es reicht nicht der einfache Verweis auf bestehende Auditierung beispielsweise nach dem LuftSiG) ebenso wie alle sonstigen Vorschriften des KRITIS-DachG.

§ 8

Die Betreiber kritischer Anlagen sollen diese über ein gemeinsames Online-Meldeportal von BBK und BSI registrieren und eine Kontaktstelle bzw. eine Ansprechperson benennen, die jederzeit erreichbar ist. Das BBK erstellt eine Liste der Betreiber kritischer Anlagen.

Für die Unternehmen ist häufig ein größerer Rechercheaufwand erforderlich, um ihre Betroffenheit durch das KRITIS-DachG als auch durch das NIS2UmsuCG festzustellen. Ein gemeinsames Portal für die Registrierung ist auf jeden Fall hilfreich. Das Portal sollte auch Prüfmöglichkeiten enthalten, anhand derer die Unternehmen ihre Betroffenheit vor der Registrierung als Self-Service einfach selbst überprüfen können.

§ 9

Die Pflichten nach dem Gesetz scheinen mit einem hohen bürokratischen Aufwand verbunden zu sein. Die Intervalle (vier Jahre) zwischen den planmäßig durchzuführenden staatlichen Risikoanalysen halten wir für zu lang. Eine vierjährige Aktualisierung wird den sich sehr dynamisch entwickelnden Bedrohungsszenarien sowie den technologischen Rahmenbedingungen und Entwicklungen nicht gerecht.

§ 10

In praktischer Hinsicht sind die gesetzlich geforderten Resilienzmaßnahmen mit den bestehenden Strukturen, wenn auch mit erheblich wachsendem materiellem Aufwand, darstellbar. Umso bedauerlicher ist es, dass der Gesetzgeber keine orientierenden Informationen zu den fehlenden Rechtsverordnungen geben kann, die für die Ermittlung des Aufwandes unverzichtbar sind.

§ 12

Für bürokratiearme Prozesse sollte nur eine Meldung über das Portal des BSI erforderlich sein, deren Umfang klar definiert werden muss. Es wäre ein klarer Beitrag zu bürokratiearmer Regulierung, wenn Meldeverpflichtungen gegenüber anderen Stellen, die nach derzeitigem Stand bestehen bleiben sollen, und gegenüber dem BKK, aufgehoben werden würden. Über das Portal sollten die Meldungen an andere Behörden weitergeleitet werden. Dafür sind effektive technische und organisatorische Prozesse zu definieren und auf ein angemessenes Schutzniveau sensibler Informationen zu achten.

Der Umgang mit den Informationen muss im Sinne des Geheimsschutzes erfolgen (analog zu BSIG § 5 Abs. 4 und 5).

§ 14

Bemerkenswert ist die zuletzt (im Vergleich zu früheren Entwürfen) neu eingeführte Verpflichtung von Geschäftsleitern. Das folgt dem Beispiel bei der Neufassung der Vorschriften zur Cyberabwehr (Umsetzung von NIS2). Eine solche Regelung wird jedoch in vielen Fällen ins Leere gehen bzw. unbillige Haftungsrisiken für Leiter nationaler Unternehmensteile begründen. In internationalen Konzernunternehmen werden IT-Systeme in der Regel zentral betrieben und überwacht. Nationale Geschäftsleiter haben typischerweise keinen Einfluss auf wesentliche Aspekte des Risikomanagements. Auch bei der Abwehr physischer Gefahren bestehen in der Regel unternehmensweite Standards oder aber es kommen bereits gesetzliche Vorschriften zur Umsetzung (die nach § 4 Abs. 7 des Referentenentwurfs unberührt bleiben). Es erscheint daher sowohl unrealistisch als auch eigenartig unflexibel, wenn Geschäftsleiter Maßnahmen billigen müssen oder zu überwachen haben, für die eine rechtliche Verpflichtung besteht. Dies ist nach unserer Auffassung die Aufgabe der Aufsichtsbehörde. Desgleichen ist eine undifferenzierte Pflicht der Geschäftsleistungen zur Schulung nach § 14 Abs. 2 fragwürdig. Vielmehr beruhen effiziente Unternehmensstrukturen wesentlich auf einer arbeitsteiligen Organisation mit spezialisierten Fachabteilungen. Die Funktion von Geschäftsleitern ist es, diese Fachabteilungen zu steuern. Dieser Aufgabe können sie nicht nachkommen, wenn sie sämtliche spezialgesetzlichen Obliegenheiten persönlich nachhalten müssten. Pragmatischer wäre daher allenfalls eine Unterrichtungspflicht als Instrument zur expliziten Einbindung der Unternehmensleitung.

Der Bundesverband Paket und Expresslogistik:

Der 1982 gegründete Bundesverband Paket und Expresslogistik (BIEK) vertritt die Interessen der Kurier-, Express- und Paketbranche (KEP) in Deutschland. Rund 4.000 Unternehmen sorgen für eine flächendeckende Zustellung von der Hallig bis zur Alm, in der Stadt und auf dem Land. Die gesamte Branche realisiert in Deutschland derzeit jährliche Umsätze in Höhe von 26 Milliarden Euro, beschäftigt rund 258.000 Mitarbeiterinnen und Mitarbeiter und befördert ca. 4,15 Milliarden Sendungen pro Jahr.

Berlin, im Januar 2024