



RefE KRITIS-DachG - geänderte Fassung

Sehr geehrte Frau Polzin,
sehr geehrte Damen und Herren,

wir bedanken uns für die Übersendung des geänderten Referentenentwurfs des KRITIS-Dachgesetzes und die Gelegenheit zu den Änderungen Stellung zu nehmen. Gerne machen wir von dieser Möglichkeit Gebrauch. Aus Sicht des Lebensmittelhandels haben wir die folgenden Anmerkungen:

1.) § 3 Zuständigkeiten

Nach wie vor ist es für den Handel sehr wichtig, dass eine einheitliche Auslegung des Gesetzes gewährleistet ist. Auch die Ausweitung von Zuständigkeiten auf die Länder darf nicht dazu führen, dass Rechtsanwender mit 16 unterschiedlichen Auslegungen einer Bundesregelung konfrontiert werden.

In § 3 Abs. 4 und 5 fehlt aus unserer Sicht eine eindeutige Zuteilung, in welchen Fällen die entsprechende Bundes- oder Landesbehörde zuständig ist. Eine genauere und detailliertere Beschreibung der Zuständigkeiten wäre hilfreich.

Nicht klar ist weiterhin, zu welcher kritischen Dienstleistung der LEH zuzuordnen ist, so dass die zuständige Behörde für den Lebensmittelhandel nicht erkennbar ist.

§ 3 Abs. 7 bestimmt verschiedene Zuständigkeiten. Fehlend ist die Information, welche der Behörden für eine kritische Dienstleistung als Single Point of Contact zuständig ist, damit eine doppelte Meldung als kritische Dienstleistung verhindert werden kann.

2.) § 4 Anwendungsbereich

Die Ausrichtung des Schwellenwertes von 500.000 ist nicht plausibel, da sich z.B. in der NIS-2 Richtlinie auf den jeweiligen branchenspezifischen Standard bezogen (Diskussionspapier, NIS2-Richtlinie in Deutschland, § 57 Abs. 4, Stand: 27.09.2023) wird und der jeweilige Schwellenwert als Bezugsrahmen genutzt wird. Eine solche differenzierte Ausrichtung sollte ebenfalls genutzt werden. Darüber hinaus ist die Messbarkeit des angegebenen Schwellenwertes für den LEH nicht anwendbar und kann nicht valide gemessen werden. Angesichts der teilweise erheblichen Verpflichtungen, die aus dem KRITIS-DachG entstehen können, sollten die Kriterien, ob ein Unternehmen als kritische Anlage einzustufen ist oder nicht, per Gesetz geregelt werden und nicht in erst in einer Rechtsverordnung.

3.) § 6 Umsetzungsfristen

Wir hatten bereits in unserer ursprünglichen Stellungnahme darauf hingewiesen, dass die im Gesetz angesetzten Fristen in vielen Teilen sehr herausfordernd sind und an einigen Stellen nicht realistisch sind. Wir möchten an diesen Stellen insbesondere noch einmal auf die folgenden Punkte hinweisen:



a) § 6 Abs.6 (Verpflichtungen nach § 9 (9 – 10 Monate))

Die angegebenen Zeithorizonte sind für die Umsetzung der entsprechenden Anforderungen nicht umsetzbar:

- (§ 9) Der angegebene Zeithorizont für die Durchführung und Bewertung von Risikoanalysen in der vorgegebenen Zeitspanne von neun Monaten ist nicht haltbar. Die Durchführung einer umfassenden Risikoanalyse entsprechend des Risikozyklus ist standardgemäß auf 12 Monate anzusetzen. Für die Planung, Durchführung sowie Analyse wird ein deutlich größerer Zeitraum benötigt, um eine valide Analyse zu ermöglichen.
- (§ 10) Der angegebene Zeithorizont für die Fertigstellung von Resilienzplänen in Abhängigkeit der in §10 Abs. 6, S.2 aufgeführten Anforderungen, sind nicht umsetzbar. Eine Umsetzungszeit von einem Monat nach Fertigstellung der Risikoanalysen wird nicht abbildbar sein, um Resilienzmaßnahmen entsprechend der Risikoanalysen zu entwickeln und anschließend Resilienzpläne zu schreiben. Darüber hinaus ist die Plausibilität der Zeitspanne von einem Monat zu hinterfragen.
- (§ 11 Abs.2) Eine zeitliche Frist von sowohl 10 Monaten zur Erfüllung der verpflichtenden zu den erbringenden Informationen als auch weiterer Informationen/ Nachweise, ist nicht erfüllbar, da eine Übergangsfrist benötigt werden würde, um entsprechende weitere benötigte Informationen zu erstellen und anschließend den entsprechenden Behörden bereitstellen zu können.

b) zu § 6 Abs.1 (Kontaktstelle „jederzeitige Erreichbarkeit“)

Eine durchgängige Erreichbarkeit einer Kontaktstelle im Unternehmen kann nicht abgebildet werden, da eine nationale Erreichbarkeit 24/7 für den Geschäftsbetrieb nicht erforderlich ist und aktuell nicht erfolgt. Eine Umsetzbarkeit der Kontaktstelle ist zu prüfen und benötigt Vorlaufzeit in der Einrichtung.

c) Schließlich ist in § 6 Abs.1 unklar, ob eine erneute Registrierung mittels der gemeinsamen eingerichteten Registrierungsmöglichkeit notwendig ist, wenn die Organisation bereits als kritische Anlage bei dem BSI gemeldet ist (aufgrund des BSI-Gesetzes). Andernfalls müsste ein Austausch der bereits registrierten kritischen Dienstleistungen durch die jeweiligen Behörden erfolgen.

4.) § 10 Nachweis über getätigte Resilienzmaßnahmen

Resilienzmaßnahmen lassen sich nach verschiedenen ISO-Standards (z.B. ISO 22316, 22320, 22301, 31000) zertifizieren und auditieren. Es sollte sichergestellt werden, dass diese Standards als Nachweise über Resilienzmaßnahmen bzw. Resilienzpläne nach § 10 Anerkennung finden, um den Prüf- und Auditierungsaufwand in den betroffenen Unternehmen zu minimieren. Weiter sollte klargestellt werden, dass die in § 10 Abs. 3 genannten Maßnahmen lediglich beispielhaft zu verstehen sind, und eine auf die im betroffenen Unternehmen bzw. in der betroffenen Anlage vorliegende konkrete Situation abgestimmte Maßnahme der Auflistung in § 10 Abs. 3 in jedem Fall vorgeht.



Bezgl. § 10 Abs. 4 fehlen zeitliche Angaben, zu welchem Zeitpunkt die Mindestanforderungen bekannt gegeben werden und innerhalb welcher Fristen sie umgesetzt werden sollen. Die Fristen zwischen Anhörung und Umsetzung sollten angemessen und umsetzbar sein.

5.) § 12 Meldepflichten

Die Meldepflichten aus § 12 Abs.1 (Vorfälle, die „erheblich stören könnten“) sind zu unkonkret und aus unserer Sicht zu überdenken.

Die Formulierung kann in der Praxis in der Abgrenzung erhebliche Probleme bereiten. Wenn etwas stören kann, letztlich aber nicht stört, stellt sich die Frage, ob mit der Meldung solcher Vorfälle betroffene Unternehmen, Behörden und Meldewege nicht völlig überfordert bzw. unnötig beschäftigt werden.

In Abs. 2 heißt es: „Die Meldungen müssen die verfügbaren Informationen enthalten, die erforderlich sind, damit Art, Ursache und mögliche, auch grenzüberschreitende, Auswirkungen und Folgen des Vorfalls nachvollzogen und ermittelt werden können.“

Eine fundierte Ursachenforschung wird binnen 24 Stunden nicht möglich sein. Insbesondere bei Vorfällen mit IT-Bezug dürfte dies nicht realistisch sein. Zu beachten ist auch, dass die Ursachenforschung in solchen Fällen nicht im Vordergrund steht, sondern die Wiederaufnahme des Betriebes Priorität haben muss.

Bzgl. §12 Abs.2

Eine Einschätzung von Anzahl und Anteil der von der Störung betroffenen ist dem LEH nicht möglich. Es sollte eine andere Messgröße herangezogen werden, um die Betroffenheit valide darstellen zu können.

In § 12 Abs. 3 werden Betreiber kritischer Anlagen verpflichtet, binnen eines Monats einen ausführlichen Bericht zu übermitteln. Unklar ist, welche Informationen der ausführliche Bericht beinhalten sollte. Für eine erste Meldung wird dies durch § 12 Abs. 2 klargestellt. Sofern innerhalb des ausführlichen Berichtes bereits eine Lösung des Vorfalls beschrieben werden sollte, ist der Zeithorizont von einem Monat kritisch zu betrachten, da je nach Umfang eines Vorfalls, ggfls. auch nach einem Monat noch keine Lösung gefunden werden konnte. In diesem Fall wäre die Problemlösung weiterhin prioritär vor dem Bericht an die Behörde.

§ 12 Abs. 9 beinhaltet eine Offenlegung eines Vorfalls an die Bevölkerung. Anzumerken ist, dass die Offenlegung ggf. einen Reputationsschaden bei der entsprechenden kritischen Anlage erzeugen könnte, daher sollten Kategorien dargestellt werden, ab welchem Ausmaß, ein Vorfall der Öffentlichkeit zu melden ist.

6.) Allgemeine Anmerkungen

Kommunikation unter den Behörden:

Für den Handel ist es unabdingbar, dass die Abstimmung unter den Behörden zügig und nach klaren Regeln erfolgt, damit Betreiber kritischer Anlagen größtmögliche Sicherheit über ihre Pflichten erlangen und auf ein einheitliches Vorgehen vertrauen können. Dies schließt auch ein, dass in Behörden ein vergleichbares Schutz- und Resilienzniveau wie in



den betroffenen Unternehmen sichergestellt wird, um vertrauliche Daten und Unternehmensgeheimnisse nach Übermittlung an die zuständigen Behörden nicht zu kompromittieren.

Rechtzeitige Veröffentlichung von Vorgaben, Vorlagen, Mustern etc.:

Der Referentenentwurf des KRITIS-DachG sieht an mehreren Stellen die Möglichkeit vor, dass das BBK Vorlagen, Muster oder anderweitige Vorgaben veröffentlicht, an denen sich betroffene Unternehmen orientieren können. Es ist sicherzustellen, dass diese Unterlagen möglichst frühzeitig vor Inkrafttreten der gesetzlichen Pflichten für die betroffenen Unternehmen veröffentlicht werden, um diesen eine ausreichende Zeit zur Vorbereitung und Implementierung zu ermöglichen. Dies gilt insbesondere für klare Kriterien, in welchen Fällen eine Meldung nach KRITIS-DachG zu erfolgen hat.

Schulungspflicht von Geschäftsleitern, § 14 Abs. 2:

Eine regelmäßige Schulungspflicht des Geschäftsleiters ist in Abhängigkeit der Größe des Unternehmens zu hinterfragen, respektive sollte insbesondere bei großen Unternehmen die spezifische zuständige Abteilung bzw. die verantwortliche Person der zuständigen Abteilung verpflichtend geschult werden. Eine Zuordnung, der zu verpflichtend zu schulenden Person, sollte in Abhängigkeit der Unternehmensgröße erfolgen sowie näher spezifiziert werden, welche Person zu schulen ist.

7.) Kohärenz KRITIS-DachG/NIS2UmsuCG

Der vorliegende Referentenentwurf ist dem Ziel, größere Kohärenz und Vereinheitlichung der Fristen, Begrifflichkeiten, Prozesse etc. in KRITIS-DachG und NIS2UmsuCG ein Stück nähergekommen. Es sei dennoch noch einmal auf die Wichtigkeit verwiesen, hier möglichst große Einheitlichkeit und damit Überschaubarkeit und Vereinfachung für die betroffenen Unternehmen zu gewährleisten.

Wir bitten um Verständnis, dass wir uns aufgrund der Kürze der Frist vorbehalten müssen, weitere Anmerkungen nachzureichen.

Berlin, 24. Januar 2024

Bundesverband des Deutschen Lebensmittelhandels.