Übersicht Regulierung KRITIS und Kommentar zum geplanten KRITIS-Dachgesetz

von Franziska Englert
02. Januar 2023

**Ausgangslage**
Die Verschärfung der Bedrohungslage kritischer Infrastruktur in den vergangenen Jahren und der Ausblick auf die weitere Zunahme und Diversifizierung von Gefahren, führt auf EU- und nationaler Ebene zu einer kontinuierlichen Anpassung und Ausweitung der Regularien.

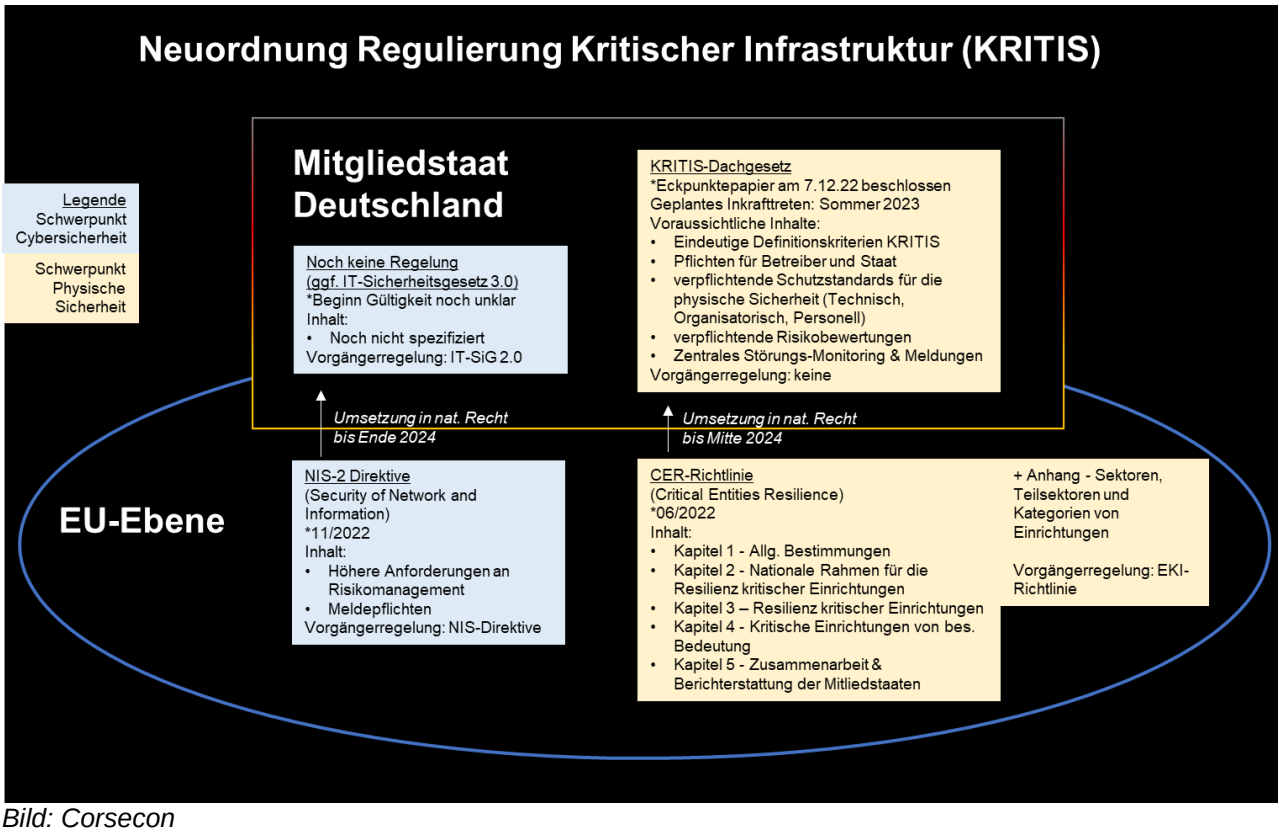

*Bild: Corsecon*

Ziel ist die Stärkung der Widerstandsfähigkeit kritischer Infrastrukturen. Dieses Ziel wird auch von der NATO verfolgt und ist Bestandteil des Koalitionsvertrages.
Engere staatenübergreifende Zusammenarbeit ist aufgrund der Abhängigkeiten zwischen den verschiedenen Sektoren im Schadensfall ebenso vorgesehen, wie die akteursübergreifende Kooperation zwischen Betreibern und staatlichen Behörden von Bund und Ländern in Deutschland.

Der Fokus lag bisher vorwiegend auf digitaler Sicherheit; mit der neuen CER-Richtlinie und dem in Folge geplanten KRITIS-Dachgesetz zur Umsetzung in nationales Recht wird dieser um den Bereich physische Sicherheit erweitert.

Durch die Umsetzung staatlicher Risikoanalysen soll ein Risikomonitoring etabliert werden. Die Vorgabe von Sicherheitsstandards zwingt Betreiber zur Ergreifung verbesserter Schutzmaßnahmen und Meldepflichten ermöglichen die schnelle Koordination von Reaktionsmaßnahmen zwischen Sektoren und über Ländergrenzen hinweg.
Die Betreiber Kritischer Infrastrukturen erwartet damit umfangreiche Anforderungen aus dem geplanten Gesetz.
Der Staat schafft eine zuständige Behörde und ein Meldewesen. Ergänzt werden diese Maßnahmen durch Beratung und Unterstützung für die Betreiber im Rahmen der Umsetzung der Anforderungen (z.B. mit Leitfäden des BBK). Diese vorgesehene Kooperation und Teilung der Verantwortlichkeiten soll die Zusammenarbeit der, am Schutz kritischer Infrastrukturen beteiligten Akteure verbessern.

**Bisherige Regularien in Deutschland**
Bisher gab es kein sektoren- und gefahrenübergreifendes Gesetz zum Schutz Kritischer Infrastrukturen. Vielmehr mussten Betreiber diverse gesetzliche Regelungen berücksichtigen.
Mit explizitem Bezug zum physischen Schutz spezifischer Kritischer Infrastrukturen gelten einzelne Fachgesetze mit unterschiedlicher Regelungstiefe. Behördenbefugnisse, Vorgaben und die verfolgten Ziele sind unterschiedlich definiert.
Zusätzlich fördert eine Vielzahl weiterer
gesetzlicher Regelungen, Normen und Standards (u.a. KAS – Kommission für Anlagensicherheit) mittelbar auch den physischen Schutz, wie etwa bautechnische Vorschriften, das Raumordnungsgesetz (ROG) oder das Gesetz über den Zivilschutz und die Katastrophenhilfe des Bundes (ZSKG) .

**Vorgaben auf EU-Ebene**
Die EU hat 2006 das Europäische Programm für den Schutz kritischer Infrastrukturen (EPSKI) ins Leben gerufen und 2008 die Richtlinie über kritische europäische Infrastrukturen (EKI- 2008/114/EG - Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der
Notwendigkeit, ihren Schutz zu verbessern) verabschiedet, die für die Sektoren Energie und Verkehr gilt. Diese wird künftig durch die 2022 geschaffene CER-Richtlinie ersetzt.

**Ziele des Dachgesetzes**
- Eindeutige Identifizierung von KRITIS-Betrieben
- Stärkung der Resilienz des Gesamtsystems
- Verpflichtende Schutzstandards
- Einführung eines staatlichen Rahmens wie einer übergreifend zuständigen Behörde, ein Meldewesen zu Sicherheitsvorfällen, Sicherheitskontrollen und Unterstützung der Betreiber
- Berücksichtigung der Auswirkungen auf das Gesamtsystem im Fokus, Schutz als ressortübergreifende Querschnittsaufgabe
- Betreiber sind für Prävention, Abwehr, Detektion und Reaktion zur Schadenbegrenzung und Rückführung in den Normalbetrieb verantwortlich
- Auf administrativer Ebene ist das Dachgesetz der neue Ansatz für den physischen Schutz von KRITIS, der durch eine Behörde koordiniert werden soll.

Erklärtes Ziel des Bundes ist, bei der in den kommenden Monaten anstehenden Erarbeitung des national geltenden Gesetzes, die Harmonisierung der künftig geltenden Vorgaben zu Cyberschutz und physischem Schutz.

**Inkrafttreten**
Das KRITIS-Dachgesetz wird bereits im Sommer 2023 erwartet.

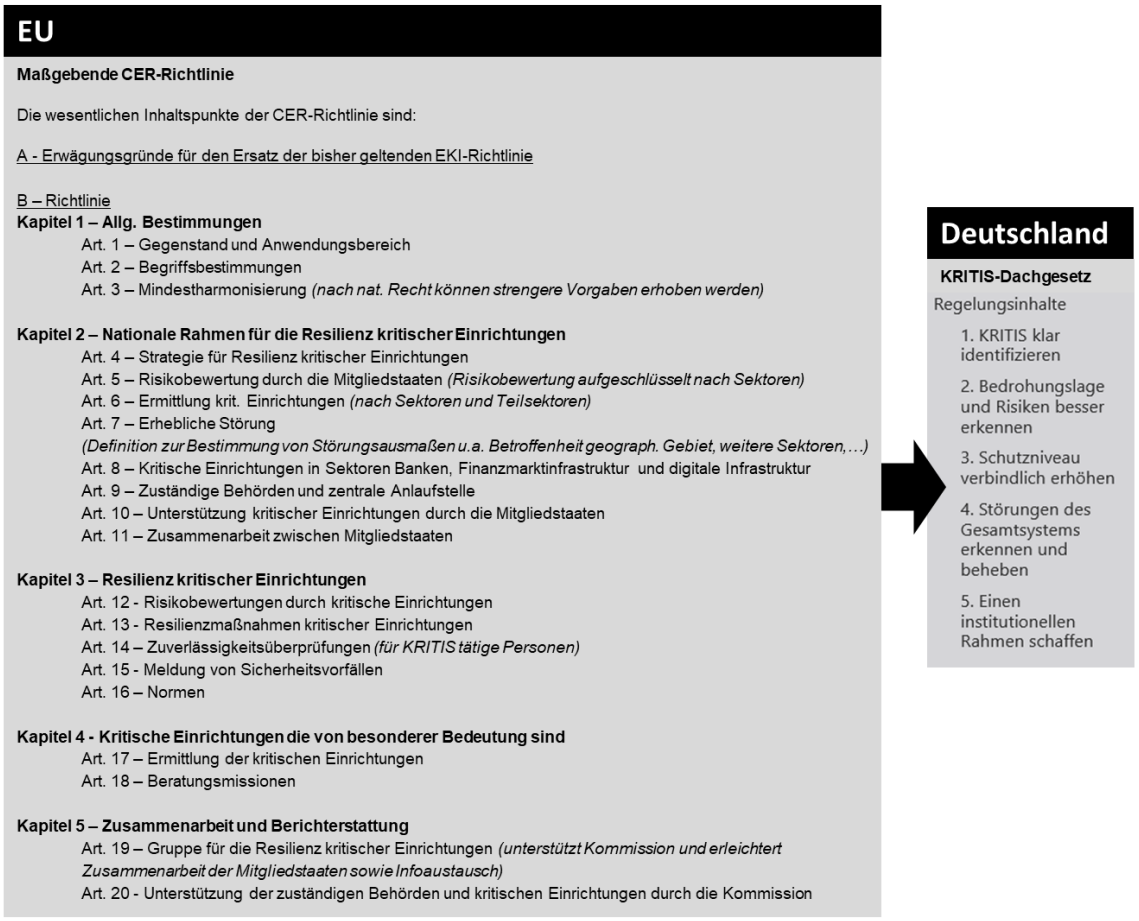


Bild: Zusammenfassung der Inhalte der CER-Richtlinie und des KRITIS-Dachgesetzes

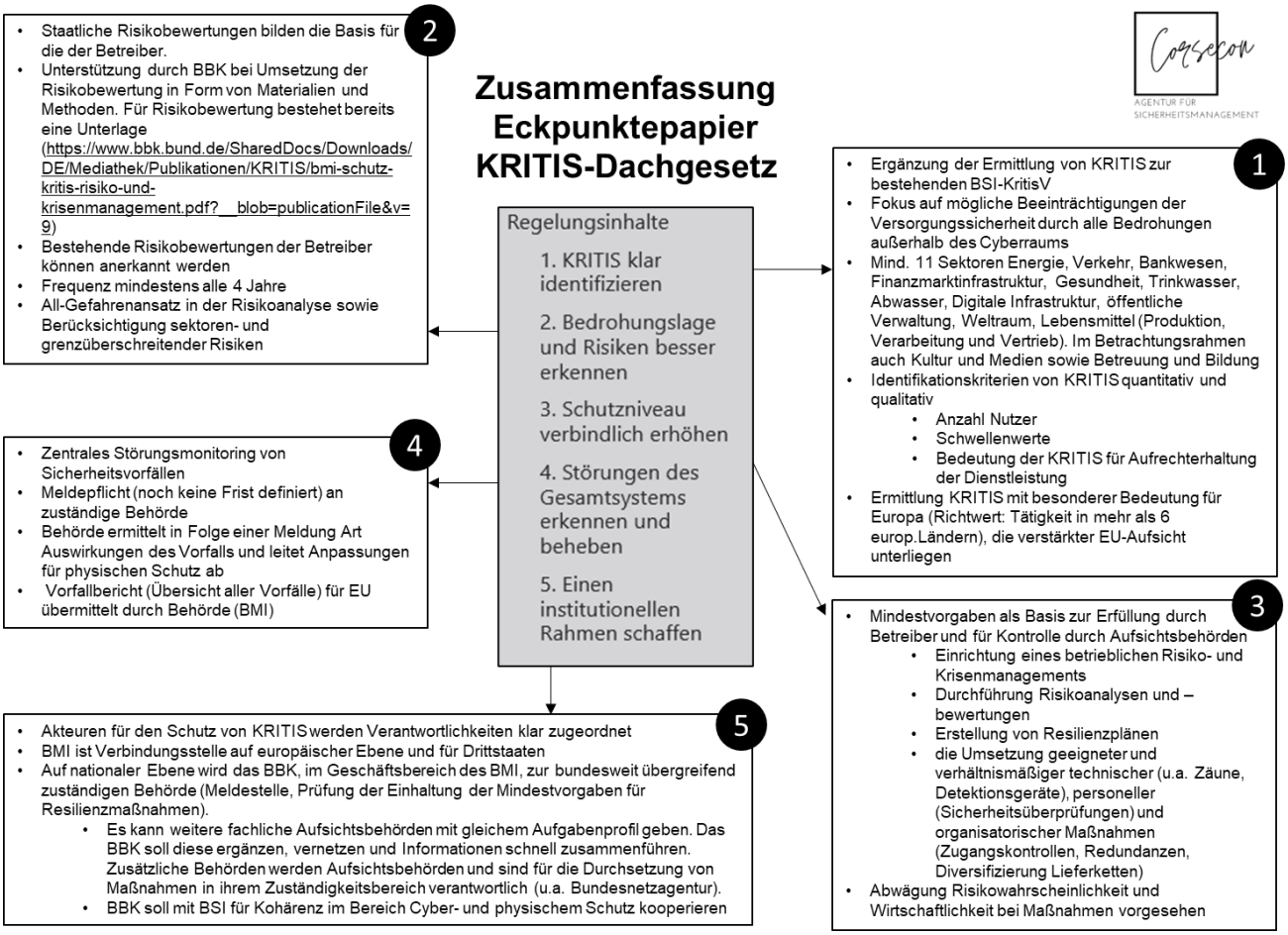

Bild: Auszug aus Eckpunktepapier & Zusammenfassung Corsecon

**Kommentar zum Eckpunktepapier und geplanten KRITIS-Dachgesetz**
Die Forcierung ganzheitlicher Lösungen in der Sicherheitsarchitektur der EU und einzelnen Mitgliedsstaaten ist zu begrüßen.
Insbesondere die Weitung des Blickwinkels über digitale Risiken hinaus war für mehr Resilienz überfällig, da die Vielzahl an Gefahren, deren Schadenpotenzial und die daraus resultierenden Kaskadeneffekte bisher nicht ausreichend berücksichtigt wurden.
Damit die Ziele des Dachgesetzes erreicht werden können, sollte die Expertise von Sicherheitsexperten aus dem Umfeld kritischer Infrastrukturen in den Gesetzentwurf einfließen, damit die Regelungen ihre Ziele in der Praxis nicht verfehlen.
Die Ausgestaltung des Gesetzes entscheidet am Ende darüber, ob ein ausreichend hohes und zwischen den Sektoren einheitliches Sicherheitsniveau tatsächlich erreicht wird.

**Noch ein Gesetz ?**
Eine der ersten Fragen, die sich angesichts des KRITIS-Dachgesetzes stellt**,** ist, ob bisherige gesetzliche Regelungen mit dem Ziel resilienter kritischer Infrastrukturen tatsächlich unzureichend waren oder ob deren Umsetzung lediglich nicht konsequent verfolgt und kontrolliert wurden?

Gesetze wie das KonTraG oder das seit 2021 geltende StaRUG**,** erfassen im Geltungsbereich sowohl Personen- wie auch Kapitalgesellschaften und verpflichten bereits zu Risiko-, Krisen**-** und Notfallmanagement (BCM). Ergänzend kommen die zahlreichen Sondervorschriften, z.B. für Krankenhäuser und Chemparks hinzu, die ergänzende Sicherheitsmaßnahmen vorschreiben. Auch für die Absicherung der IT sind aktuell,

u.a. in den Branchenspezifischen Standards (B3S), der All-Gefahrenansatz für die Analyse von Risiken und der physische Schutz an Standorten verpflichtend.
Da die CER EU-Richtlinie umgesetzt werden muss**,** gilt es die bestehenden Regelungen auf nationaler Ebene auf Wirksamkeit, etwaige Schwächen bezüglich Formulierungen, Umsetzung und Kontrollen zu prüfen sowie einheitlich mit dem Dachgesetz oder ergänzend zu verbessern.

Relevant ist zudem die Klärung**,** welche bisher geltenden (Länder-)Verordnungen durch das neue Gesetz abgelöst werden können und welche harmonisiert werden müssen**,** um für Betreiber sowohl konsistente als auch übersichtliche Regelungen zu schaffen.

Die bisherigen Pläne sehen jedoch vor, dass (interessanterweise bereits jetzt angenommene) Regelungslücken durch die Länder und Behörden in Form von Verordnungen oderEmpfehlungen geschlossen werden, was eine Vielzahl neuer Regelungen, zu den bereits bestehenden und dem neuen Dachgesetz, in Ausblick stellt. Dieses Vorgehen würde die angestrebte Vereinheitlichung ad absurdum führen.

**Zuständige Behörden**
Der Begriff einer zuständigen „zentralen Behörde“ aus der EU-Richtlinie klingt vielversprechend. Man erwartet einen zentralen Ansprechpartner für Betreiber und Behörden sowie gebündelte Informationen.
Die Ernüchterung folgt im deutschen Eckpunktepapier**,** wo von dem BBK lediglich als „übergreifend zuständige Behörde“ gesprochen wird. Es soll daneben mehrere Aufsichtsbehörden, wie u.a. die Bundesnetzagentur, Bundesanstalt für Finanzdienstleistungen oder vergleichbare Stellen geben, die für die Aufsicht der Betreiber und Regulierung zur Einhaltung der Mindeststandards in ihren Zuständigkeitsbereichen tätig werden. Sie werden mit umfangreichen Rechten zur Inspektion und Sanktionierung der als kritisch eingestuften Betriebe ausgestattet.

Das BBK soll, neben anderen fachlichen Aufsichtsbehörden, alle Informationen über Sicherheitsvorfälle zusammenführen und die Namen der Ansprechpartner von den Betreibern erhalten. Nachdem das BBK nur im Rahmen „verfügbarer Haushaltsmittel“ zur übergreifend zuständigen Behörde ausgebaut werden soll, bleibt abzuwarten wie umfassend es der Koordinierungsfunktion zwischen allen zuständigen Behörden nachkommen kann.
Das BMI wird aus den Informationen des BBK auf EU-Ebene über Sicherheitsvorfälle und den Stand der Anpassungen zum Schutz der KRITIS berichten.

Durch die Splittung zwischen fachlicher und „disziplinarischer“ Verantwortung auf nationaler Ebene sind erfahrungsgemäß Verantwortungsdiffusion und Zuständigkeitsgerangel auf Bundes- und Länderebene die Folge.

An dieser Stelle lohnt es sich, sich die für notwendig erachtete Verschärfung des IT-Sicherheitsgesetzes 2021, in Erinnerung zu rufen, die am Ende dem BSI umfangreiche Rechte und Pflichten, im Zusammenhang mit dem Schutz der IT von kritischen Infrastrukturen, übertrug.

**Betreiber**
Besondere Herausforderungen ergeben sich für Betreiber kritischer Infrastrukturen**,** die in mehr als 6 europäischen Ländern tätig sind. Ihnen wird eine besondere Bedeutung zugeschrieben. Damit verbunden sind höhere Anforderungen an diese Unternehmen und ihre Betrachtung auf EU-Ebene.
Für Betreiber ist die Beschäftigung mit den Inhalten der CER-Richtline und des Eckpapiers bereits jetzt empfehlenswert**,** um die Auswirkungen auf den eigenen Betrieb zu erkennen und zu ergreifende Maßnahmen frühzeitig anzustoßen. Werden keine Übergangsfristen gewährt, bleiben**,** nach aktuellem Stand, lediglich 6 Monate bis zum Inkrafttreten des Gesetzes Mitte 2023.

**Verantwortungsübernahme durch den Staat**
Da aktuell von einem nicht ausreichend hohen Sicherheitsniveau bei kritischen Infrastrukturen ausgegangen wird, ist von einem entsprechend hohen Aufwand für einige Betreiber bei der Umsetzung der Maßnahmen und Administration im Rahmen der Einhaltung des Gesetzes zu rechnen. Es ist fraglich**,** ob überall ausreichend Know-How und Kapazitäten bereitgestellt werden (können), um die Anforderungen zu erfüllen.
Die angekündigte Verantwortungsübernahme des Staates scheint auf die Benennung für Meldungen und Berichte, die Aufsicht zuständiger Behörden sowie die Bereitstellung von Basisinformationen zu Risiko- und

Reaktionsmanagement begrenzt und damit, angesichts der zu bewältigenden Aufgaben, nicht ausreichend. Laut Eckpapier wird aktuell eine weitergehende Unterstützung der Betreiber geprüft.

Staatliche Förderprogramme, wie sie für die Verfolgung anderer staatlicher Ziele z.B. der Energiewende ebenfalls aufgelegt werden, könnten die Kosten für Betreiber senken und eine schnelle Ergreifung von Sicherheitsmaßnahmen fördern.

**Unterstützung der Betreiber im Sicherheitsmanagement**
Die bisher beschriebene und geplante Unterstützung, in Form von Methodenbeschreibungen und Checklisten des BBK, die es in dieser Form bereits heute gibt, ist keine neue und zudem nicht ausreichende Hilfestellung**,** um das geforderte professionelle, ganzheitliche Sicherheitsmanagement in allen kritischen Infrastrukturen zu verankern.
Bei näherer Analyse der öffentlich verfügbaren Dokumente handelt es sich im Wesentlichen um eine Zusammenfassung von Basisinformationen zu Risiko- Notfall- und Krisenmanagement. In Teilen wird BCM beschrieben, so aber weder benannt noch dessen Kern-Inhalte, wie z.B. Notfallpläne, beschrieben. Die PDF-Dateien sind mit den Hinweisen versehen:
„Die Anwendung ersetzt NICHT den umfassenden Auf- beziehungsweise Ausbau eines Risiko- und Krisenmanagements“ und „Die Checklisten sollten an die individuellen Eigenschaften der Einrichtung angepasst werden.“

Bei der Formulierung der Hilfsdokumente stellt sich zudem die Frage**,** wen sie adressieren.
Das vermittelte Basiswissen ist für Sicherheitsexperten bekannt, lediglich Laien wird damit ein Überblick über die Standardmethoden verschafft. Die Aufgabe der Steigerung des Sicherheitsniveau in den kritischen Infrastrukturen sollte jedoch nicht von Laien übernommen werden, denen dann mit theoretischen Grundkenntnissen noch immer die notwendige praktische Erfahrung zur Umsetzung der beschriebenen Inhalte fehlt. Aufgrund der Vielfalt und Komplexität der einzelnen Sektoren braucht es aus unserer Sicht zum einen sektorspezifische Dokumente, Informationsmaterialien und Schulungsmöglichkeiten, die die Arbeit von Experten unterstützen und Qualitätsstandards setzen. Dies ist auch im Hinblick auf die zu erwartende Einbeziehung privater Sicherheitsdienstleister- und -berater sinnvoll.

Der entsprechende regelmäßige Input könnte beispielsweise aus Forschung und Konzepten des Bundesverbands für den Schutz Kritischer Infrastrukturen (BSKI) kommen.

**Einheitliche Prüfkriterien**
Es ist unklar, weshalb im ersten Schritt nicht auf bereits verfügbare und in der Umsetzung bewährte Methoden, Dokumente und Maßnahmen zurückgegriffen wird.
Das Gesetz könnte, wie in regulierten Branchen (Banken, Versicherungen… ), die Einführung von BCM (ggf. mit Zertifizierungsvorgabe nach ISO 22301 ff.) für kritische Infrastrukturen vorschreiben. Hierfür bestehen umfangreiche Standards, auch für Lieferketten (ISO 22318) oder Notfallmanagement, nach denen einheitlich und objektiv sektorübergreifend geprüft werden kann. Umsetzungshilfen, wie der BSI-Standard 100-4 (geplant 200-4), bieten schon heute praxisnahe und ausführliche stufenweise Implementierungshilfen für BCM.

**Mindestvorgaben für physischen Schutz**
Es bleibt abzuwarten**,** wie detailliert und umfangreich die Mindestvorgaben für physischen Schutz ausfallen. Die Möglichkeit der Abwägung zwischen Risikoeintrittswahrscheinlichkeit und Wirtschaftlichkeit der Sicherheitsmaßnahmen führt häufig zu unterschiedlichen Ergebnissen, abhängig von der Risikobereitschaft des Betreibers, was die angestrebte Herstellung eines einheitlichen Niveaus in der Praxis konterkariert.

Einer der Hauptgründe für bisher unzureichend gesicherte Infrastruktur liegt in der Tatsache, dass häufig unter Kostendruck an Sicherheitsmaßnahmen gespart und dafür im Zweifel hohe Risiken akzeptiert werden. Um hier eine echte Veränderung herbei zu führen**,** reicht ein Beibehalten der Regelung der individuellen Abwägung zwischen Wirtschaftlichkeit von Maßnahmen und Risikoeintrittswahrscheinlichkeit nicht mehr aus.

Ein weiterer Grund dafür liegt, neben der Tendenz von Betreibern dem Kostendruck zu Lasten der Sicherheit nachzugeben, auch in der mangelnden Fähigkeit, Risiken der Zukunft angemessen einzuschätzen, weshalb wir eine Anpassung in der Methodik der Risikobeurteilungen zum Ausgleich für sinnvoll und notwendig erachten. Beispiele zur konkreten Ausgestaltung stellen wir im Februar im Sicherheitsbriefing vor.

**Offene Punkte**
Das Papier gibt weder Auskunft über Details zu Melde- und Berichtswegen, noch relevante Informationen zu Reaktionsmaßnahmen und Warnungen für andere kritische Infrastrukturen oder Behörden. Die Ausgestaltung ist insbesondere mit Blick auf Bundesländer- und Staatenübergreifend tätige Betreiber interessant.

Offen bleibt auch, in welcher Häufigkeit und welchem Umfang Inspektionen bei den Betreibern stattfinden, nach welchen Kriterien geprüft wird und welche Sanktionen bei Nichteinhaltung von Mindeststandards und Sicherheitsverletzungen drohen.

Abzuwarten ist, ob der Gesetzgeber entsprechende Regelungen in Bezug auf Komponenten, die keine informationstechnischen Systeme, Komponenten oder Prozesse im Sinne des BSI-Gesetzes sind, aufnehmen wird, um KRITIS insgesamt vor Einflüssen und Abhängigkeiten von bedenklichen Herstellern aus dem Ausland zu schützen.

*Quellen: IBCRM, BSKI, BBK, BSI,BMI,  Eckpunktepapier Kritis-Dachgesetz, Heise, ntv, Openkritis*

Weitere Fachartikel unserer Experten erhalten
Sie mit unserem Sicherheitsbriefing.