AG KRITIS

Arbeitsgruppe Kritische Infrastrukturen

# Stellungnahme zum Referentenentwurf vom 21.12.2023 des KRITIS-Dachgesetz

Version 1.0 – zuletzt editiert am 24.01.2024

# Inhaltsverzeichnis

# 1 Arbeitsgruppe Kritische Infrastrukturen

Dieses Dokument wurde erstellt von Mitgliedern der unabhängigen Arbeitsgruppe Kritische Infrastrukturen (AG KRITIS).

Wir haben uns im Frühjahr 2018 erstmals zusammengefunden, um Ideen und Anregungen zur Erhöhung der Resilienz und Sicherheit kritischer Dienstleistungen von Betreibern kritischer Infrastrukturen im Sinne des Gemeinwohls zu entwickeln. Unser Ziel ist es, die Versorgungssicherheit der deutschen Bevölkerung zu erhöhen, indem wir die Bewältigungskapazitäten des Staates zur Bewältigung von Großschadenslagen, die durch Cyberangriffe hervorgerufen wurden, ergänzen und erweitern wollen. Unsere Arbeitsgruppe ist unabhängig von Staat, Verwaltung oder wirtschaftlichen Interessen.

Die AG KRITIS besteht aus ca. 42 Fachleuten und Experten, die sich mit Kritischen Infrastrukturen (KRITIS) gemäß § 2 (Abs 10) BSI-Gesetz [1] und gemäß § 10 BSIG zugehöriger *Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz* [2] (BSI-Kritisverordnung - BSI-KritisV) beruflich beschäftigen, zum Beispiel durch Planung, Aufbau, Betrieb sowie Beratung, Forschung oder Prüfung der beteiligten Systeme und Anlagen. Unser Engagement ist getrieben von der Motivation, unabhängig von wirtschaftlichen Interessen eine nachhaltige Verbesserung der Sicherheit jener Anlagen kooperativ mit allen Beteiligten herbeizuführen und damit im Katastrophenfall die öffentliche Sicherheit zu verbessern. Wir sind kein Wirtschaftsverband oder Unternehmen und haben daher auch und insbesondere keine Sponsoren.

Uns eint, dass wir durch unsere Arbeit unabhängig voneinander zu dem Schluss gekommen sind, dass die Ressourcen der Bundesrepublik Deutschland zur Bewältigung von Großschadenslagen auf Grund von informations- und operationstechnischen Vorfällen im Bereich der Kritischen Infrastrukturen nicht ausreichen. In der Folge sind resultierende Krisen oder Katastrophen nicht oder kaum zu bewältigen. Es sollen daher Wege gefunden werden, das Eintreten gravierender Folgen dieser Vorfälle durch schnelles und kompetentes Handeln zu verhindern oder zumindest abzuschwächen und eine Regelversorgung in kürzestmöglicher Zeit wieder sicherzustellen.

1 https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html
2 https://www.gesetze-im-internet.de/bsi-kritisv/index.html

# 2 Stellungnahme

Ziel der Richtlinie soll sein, „einheitliche Mindestverpflichtungen für kritische Einrichtungen festzulegen und deren Umsetzung durch kohärente, gezielte Unterstützungs- und Aufsichtsmaßnahmen zu garantieren.“

Dazu stellen wir fest: Der vorgelegte Gesetzesentwurf enthält keine Mindestverpflichtungen. Stattdessen regelt der Gesetzesentwurf, welche Behörde die Verordnungen erlassen müssen durch die wiederum Mindestverpflichtungen vorgeben würden.

Ob also die vorgesehenen Mindestverpflichtungen zum Ziel der Erhöhung der Resilienz der kritischen Anlagen und Systeme führen würden, lässt sich anhand des vorgelegten Referentenentwurfes nicht bewerten. Konkrete Handlungsanweisungen für KRITIS-Betreiber sind nicht enthalten.

Das Ziel, kritische Anlagen nicht mehr nur aus der Brille der Informatik zu betrachten ist richtig, da hierbei bisher nur die in diesem technischen Rahmen existenten Risiken adressiert wurden.  Der hier vorgelegte “All-Gefahren-Ansatz” eignet sich besser als ein IT-zentrischer Anstatz, um die Steigerung der Versorgungssicherheit zu erreichen.

# §2 Definitionen; Fokus auf Anlagen

In §2 werden die betroffenen kritischen Anlagen und kritischen Dienstleistungen definiert. Hier bleibt jedoch unberücksichtigt, dass all jene Dienstleistungen und vor- oder ausgelagerten Produkte und Dienstleistungen, die zur Erfüllung der kritischen Dienste erforderlich sind, ebenfalls gesichert werden müssten. Diese vor- und ausgelagerten Dienste sind jedoch in der Regel sektorenunabhängig und damit vom Regelungsgehalt des Kritis-DG nicht erfasst.

Ein Paradigmenwechsel - weg von der Betrachtung einzelner Anlagen und hin zu der Betrachtung der gesamten notwendigen Kette an Aufgaben oder Dienstleistungen rund um den Betrieb einer Anlage wäre sinnvoll und notwendig, um die Resilienz zu steigern.

Selbstverständlich kann man sich nicht gegen jedes Risiko wappnen, ein Restrisiko wird am Ende trotzdem überbleiben, dies sollte jedoch möglichst gering bleiben. Entsprechend sieht der Gesetzesentwurf vor, dass eine Abwägung stattfinden soll, ob eine Maßnahme gegenüber der Eintrittswahrscheinlichkeit eines Risikos verhältnismäßig ist.

Diese Abwägung wird im §10 der BetreiberIn der Anlage auferlegt.

# §10 Resilienzmaßnahmen der Betreiber kritischer Anlagen

Bei dieser Abwägung der Interessen, werden die Interessen der Bevölkerung (Versorgungssicherheit) sowie die Interessen des Staates (öffentliche Sicherheit) von niemandem explizit vertreten. Private Betreiber sollen folglich unter Berücksichtigung der eigenen Wirtschaftlichkeit den Risikoappetit der öffentlichen Hand festlegen.

Es wird zwar dem BBK das Recht gegeben, sowohl die getroffenen Maßnahmen zu prüfen, als auch Bußgelder zu verhängen, aber eine regelmäßige Auditierung, wie im BSIG, ist nicht vorgesehen. Damit fehlen wichtige Werkzeuge, die für ein kohärentes Vorgehen unter den Betreibern sorgen würden.

Die von den Betreibern beurteilten Risiken und vorgesehenen Maßnahmen sollten daher ähnlich wie die Prüfung nach BSIG §8a vorgezeichnet, regelmäßig geprüft werden.

# §4 Anwendungsbereich; kritische Anlagen; Geltungsumfang

Der Sektor Staat und Verwaltung ist auch in diesem Entwurf nicht ausreichend adressiert. Aus §4 ist “Staat und Verwaltung” komplett gestrichen worden, aber darüber hinaus sind auch Kommunalverwaltungen und Behörden der Länder unzureichend geregelt.
Da auch durch diese Behörden Dienstleistungen erbracht werden, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten können, halten wir eine Regelung der physischen Sicherheit dieser Anlagen auch in diesem Bereich für unumgänglich.

# §5 Einrichtungen der Bundesverwaltung

Hier finden sich einige minimale Regelungsansätze, die allerdings ausschließlich Bundesministerien  und das Bundeskanzleramt betreffen, dann allerdings weitere Ausnahmen für eine ganze Reihe von  Tätigkeitsbereichen.

Den Ministerien unterstellte, nachgeordnete Behörden, wie zum Beispiel die BDBOS, sollten miterfasst werden.
Wichtige Versorgungsdienstleistungen, die möglicherweise durch Länder und Kommunen ausgeführt werden, aber durch Bundesrecht geregelt werden, wie z.B. Versorgungsleistungen nach SGB sind nicht miterfasst, müssten aber unserer Ansicht nach ebenso Resilienz-Auflagen erfüllen

Landes- und Kommunalverwaltungen sind von den Regelungen nicht betroffen. Es wäre dringend notwendig, den Sektor Staat und Verwaltung – sowohl durch Erlass einer entsprechenden KRITIS-Verordnung, als auch im KRITIS-Dachgesetz gleichwertig zu betrachten und zu regeln.

Landes- und Kommunalverwaltungen sind oftmals nicht ausreichend ausgestattet, um die notwendige 24/7 Überwachung und Administration der IT-Systeme zu gewährleisten. Hieraus entsteht ein politischer Handlungsbedarf des Bundes, Ressourcen übergreifend zu organisieren und Synergien zu schaffen. Die zahlreichen Cyberangriffe auf die öffentliche Hand dokumentieren ein flächendeckendes, mangelhaftes Sicherheitsniveau, welches aus unserer Sicht ausreicht um den Handlungsbedarf zu rechtfertigen.

# §20 Evaluierung

Obwohl die grundsätzliche Idee hier richtig ist, fehlt hier, dass dieser Evaluierungsbericht regelmäßig und durch Dritte einsehbar veröffentlicht wird. Auch weitere Berichtspflichten würden wir begrüßen - z.B. ein regelmäßiger Bericht an das Parlament.
Gemeinsame Meldestelle

# §12 gemeinsame Meldestelle

Der Entwurf des KritisDG verpflichtet BBK und BSI, eine gemeinsame Meldestelle für Vorfälle einzurichten (§12). Dies halten wir für den richtigen Weg, um im Falle eines Vorfalles den Aufwand für Unternehmen zu reduzieren.

# 3 Vorgehensweise

Das BMI hat seine gesetzliche Pflicht erfüllt, die Wirtschaft anzuhören. Neben den Anhörungen gab es darüber hinaus auch ein Werkstattgespräch – zu welchem das BMI nicht verpflichtet war. Wir sind dem BMI dankbar, explizit zu beidem eingeladen worden zu sein und darüber hinaus auch zu bestimmten Entwurfsstadien um schriftliche Stellungnahmen gebeten worden zu sein.

Bedauerlicherweise wurde so gut wie die gesamte Entwurfsversion, sicherlich jedoch so gut wie alle Punkte die VertreterInnen der Wirtschaft oder von uns in den Anhörungen vorgebracht haben, mit dieser Version ignoriert und über Bord geworfen. Der vorliegende Text ist in großen Teilen eine komplette Neufassung der relevanten Kernbestandteile. Diese Neufassung entspricht nun dem, was die EU uns durch die CER-RL vorgibt.

Dies hätte man im BMI ahnen können – das die CER-RL erst so spät im Prozess durch das BMI mit dem DachG-Entwurf geeint wurde, hat die davor auch im Ehrenamt stattgefundene Arbeit überflüssig gemacht.

Trotzdem möchten wir besonders hervorheben, dass wir – zum allerersten Mal in der Geschichte der AG KRITIS – einen Referentenentwurf im Änderungsmodus bekommen haben. Der Änderungsmodus erlaubt, direkt klar sehen zu können, welche Wörter im Vergleich zur Vorversion geändert, gelöscht oder ergänzt wurden.

Noch beim IT-SiG2 haben wir uns sehr deutlich und laut darüber beschwert, dass die in schneller Folge veröffentlichten Entwurfsversionen nur den Text enthielten, aber keine Informationen über Änderungen. Für dieses Gesetz hat sich der Prozess aus unserer Sicht deutlich verbessert