AG KRITIS

Arbeitsgruppe Kritische Infrastrukturen

Stellungnahme zum Referentenentwurf des NIS2UmsuCG vom 23.06.2025

Version 1.0 – zuletzt editiert am 03.07.2025

1 Arbeitsgruppe Kritische Infrastrukturen....3
2 Stellungnahme....4
Definition Kritischer Infrastrukturen....4
KRITIS Sektor Staat und Verwaltung....6
CISO Bund....8
Ausnahmen als Regelfall....8
Risikomanagement, Haftung der Geschäftsleitung und Durchsetzungsmaßnahmen....9
Technische Expertise und Befugnisse des BSI....10
Meldepflicht....11
Empfehlungen des Bundesrechnungshofes....11
Regulierung von DNS-Betreibern....11
Verpflichtung zur Zugangsgewährung zu DN-Registrierungsdaten....12
Veröffentlichung von branchenspezifischen Sicherheitsstandards (B3S)....13
Evaluierung der Umsetzung....13
Würdigung des Prozesses....13
Fazit....14

1 Arbeitsgruppe Kritische Infrastrukturen

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

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 kürzest möglicher Zeit wieder sicherzustellen.

1 www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html
2 www.gesetze-im-internet.de/bsi-kritisv/BJNR095800016.html

2 Stellungnahme

Mit dem vorliegenden Referentenentwurf des *Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz)*, kurz NIS2UmsuCG, wird die Umsetzung der europäischen NIS2-Richtlinie (EU) 2022/2555 angestrebt. Damit einher geht eine Ausweitung des Geltungsbereiches von Betreibern kritischer Anlagen (ehem. sogenannte KRITIS-Betreiber) und der als wichtige und besonders wichtige Einrichtungen definierten sonstigen Unternehmen.

Das NIS2UmsuCG ist ein Artikelgesetz, welches insgesamt 28 Gesetze und Verordnungen ändern soll. Unsere Kommentierung bezieht sich hierbei hauptsächlich auf die unter Artikel 1 eingebrachte Änderung des BSI-Gesetzes.

Mit dem neuen Referentenentwurf vom 23.06.2025 werden aus unserer Sicht keine wesentlichen Verbesserungen zu den bisherigen Referentenentwürfen und dem Entwurf der Bundesregierung aus der letzten Legislaturperiode (BT-Drs. 20/13184) erreicht und wesentliche **Defizite** beibehalten:

- § 15 (1): Einschränkung auf **bekannte** Schwachstellen für die Schwachstellenscanner des BSI
- § 43 (5): **Wegfall** von jährlichen statistischen Meldungen der Geheimdienste für unterdrückte Informationsweitergabe an das BSI
- § 44 (2): **Verpflichtung** des BSI bei Aktualisierungen des IT-Grundschutz und Mindeststandards vor allem die Umsetzungskosten zu minimieren
- § 56 (1-5): Berücksichtigung der Verbände, der Wissenschaft und der **Zivilgesellschaft** vor dem Erlassen von Rechtsverordnungen **fällt komplett weg**

Details zu diesen Punkten sind in den weiteren Erläuterungen ausgeführt.

Die **bisherigen Defizite** bleiben weiterhin bestehen, so dass die Forderungen der AG KRITIS, sie abzustellen, ebenfalls aufrechterhalten werden.

Definition Kritischer Infrastrukturen

Bisher definiert § 2 (10) BSI-Gesetz die "Kritische Infrastrukturen". Mit der Umsetzung der NIS2-Richtlinie leitet sich daraus eine Zugehörigkeit in die "Besonders wichtigen Einrichtungen" (BWE) ab. KRITIS Betreiber werden in "Betreiber kritischer Anlagen" umbenannt.

Weiterhin sind die **KRITIS-Sektoren Chemie und Großforschungseinrichtungen** nicht als kritischen Infrastrukturen ergänzt worden, die bereits vor Jahren vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) deklariert wurden und die weiterhin als KRITIS Berücksichtigung finden müssen.

Definitionen wie "kritische Anlagen" können § 56 entsprechend durch Rechtsverordnungen konkretisiert werden. Diese werden durch das BMI im Zusammenwirken mit anderen Ministerien erarbeitet. Bereits im Entwurf vom 07.05.2024 wurde in Absatz 4 die **Einbindung der Zivilgesellschaft** für die Definition von „kritischen Anlagen“ **entfernt**. Im aktuellen Referentenentwurf wurde diese **fehlgeleitete Anpassung** auf alle 5 Absätze des Artikels **ausgeweitet** und betrifft somit die Definition von kritischen Anlagen, erheblichen Sicherheitsvorfällen, die Verfahren zur Erteilung von Sicherheitszertifikaten, wann die Sicherheitszertifikate verpflichtend sind, sowie das Sicherheitskennzeichen. Entgegen der bisherigen Praxis als auch dem Koalitionsvertrag sollen Akteure aus der Wirtschaft und der Wissenschaft nicht (mehr) eingebunden werden.

Vorhandene Regelungen aus der Gemeinsamen Geschäftsordnung der Bundesministerien adressieren hier lediglich das Recht der Verbände, angehört zu werden. Die Wissenschaft und die Zivilgesellschaft sind weiterhin nicht explizit adressiert, auch wenn das BMI hier einen Ermessensspielraum hat, unter der Kategorie von „Fachkreisen“ weitere Organisationen einzuladen.

Für alle Regelungen des § 56 (Ermächtigung zum Erlass von Rechtsverordnungen) fordern wir weiterhin die verbindliche Einbindung der betroffenen Wirtschafts-Verbände, der Wissenschaft und der Zivilgesellschaft.

Auch die Festlegung in § 56 (4), **keinen Zugang zu Akten zu gewähren**, stößt übel auf. Wir fordern die Definition der kritischen Anlagen und die Festlegung der Schwellenwerte in einem transparenten Verfahren auf Basis von wissenschaftlicher Evidenz.

Das BMI soll die Schwellenwerte neu berechnen und dabei insbesondere die Möglichkeiten der Ersatzerbringung einer kritischen Dienstleistung analysieren. Der Schwellenwert soll jeweils die Zahl sein, bis zu der eine **Ersatzerbringung der kritischen Dienstleistung im Krisenfall** sicher möglich ist. Dies variiert von Sektor zu Sektor und innerhalb der Branchen eines Sektors stark. Die derzeitigen Schwellenwerte von 500.000 versorgten BürgerInnen sind nicht wissenschaftlich entstanden, sondern entstammen einer politischen Festlegung aus dem Jahr 2016.

Aufgrund der Komplexität der Regelungen fallen weitere Sonderfälle auf, wie hier am Beispiel des Sektors Forschung aufgezeigt wird: so wird der Sektor Forschung gemäß der Begriffsdefinition "Forschungseinrichtung" auf angewandte Forschung mit kommerziellem Zweck begrenzt. Nach Ansicht der AG KRITIS ist hier auch die **Grundlagenforschung als Kritische Infrastruktur** zu betrachten. Insbesondere, wenn diese sicherheitsrelevante Auswirkungen haben kann.

Auf der Webseite „EduSec: Sicherheitsvorfälle an deutschsprachigen Hochschulen“ unter www.aheil.de/edusec/ können alle öffentlich bekannt gewordenen Vorfälle eingesehen werden, die ehrenamtlich dort gesammelt und veröffentlicht werden.

Durch den Bund finanzierte Forschungseinrichtungen, welche in der Rechtsform einer Stiftung des öffentlichen Rechts nach Landesrecht aufgebaut wurden, sind darüber hinaus ebenfalls nicht von den Regelungen des Gesetzes erfasst, außer es wird im Einvernehmen mit dem zuständigen Ressort angeordnet.

Die Regelung zur Sektorenzuordnung vernachlässigbarer Geschäftstätigkeiten im neuen § 28 (3) sind problematisch. Die folgende Feststellung stammt von RA Stefan Hessel und wurde auf LinkedIn veröffentlicht[3]: „Nach § 28 Abs. 3 BSIG-E können bei einer Zuordnung zu einer der Einrichtungsarten nach den Anlagen 1 und 2 solche Geschäftstätigkeiten unberücksichtigt bleiben, die im Hinblick auf die gesamte Geschäftstätigkeit der Einrichtung „vernachlässigbar“ sind. Wann eine Geschäftstätigkeit „vernachlässigbar“ ist, wird im Gesetzentwurf nicht definiert. Es handelt sich um einen unbestimmten Rechtsbegriff. Aus der Formulierung „im Hinblick auf die gesamte Geschäftstätigkeit“ lässt sich jedoch ableiten, dass eine relative Bestimmung erforderlich ist.“

Wir teilen die Analyse von Stefan Hessel und fordern das Bundesministerium des Innern auf, diesen Abschnitt zu streichen. Erbringer von Dienstleistungen gemäß Anlage 1 und 2, die über die EU Size Cap Regelung adressiert werden, sollten als wichtige Einrichtung oder besonders wichtige Einrichtungen gelten. Auch dann, wenn dieses Tätigkeit im Hinblick auf die sonstige Geschäftstätigkeit vernachlässigbar erscheint. Die Vorgaben der EU für den Geltungsbereich sollten eins zu eins übernommen werden, auch wenn dies den Geltungsbereich des Gesetzes deutlich ausdehnt. Versuche den Geltungsbereich mit juristischen Tricks wie

3 https://media.licdn.com/dms/document/media/v2/D4E1FAQFo5E1aYmoCqA/feedshare-document-pdf-analyzed/B4EZelojgOHgAY-/0/1750830563460?e=1752105600&v=beta&t=NhN5xPyzMN8dpgr4Jsx26vBXUPc-HAdmW58Ofcug86w

„vernachlässigbaren“ Geschäftstätigkeiten einzuschränken konterkarieren das Gesamtziel der Richtlinie, eine defensive Cybersicherheitsstrategie in allen Mitgliedsstaaten umzusetzen.

KRITIS Sektor Staat und Verwaltung

Für den KRITIS Sektor Staat und Verwaltung gelten im Zuge des NIS2UmsuCG **unzählige Sonderregelungen und Ausnahmen**. Damit unterliegt die Verwaltung insbesondere des Bundes wieder zahlreichen Sonderregelungen und die Verwaltungen auf Kommunaler und Bundeslandebene werden vollständig außen vor gelassen und überhaupt nicht adressiert. Dies ist im Hinblick auf die vielen und teilweise sehr weitreichenden Cybersicherheitsvorfälle wie Landkreis Anhalt Bitterfeld oder S-IT in NRW (über 100 Kommunen waren monatelang betroffen und faktisch handlungsunfähig!) lediglich verfassungsrechtlich nachvollziehbar. Aus EU-rechtlicher Sicht, aber auch aus Sicht der BürgerInnen besteht hier eine systemisches Problem, welches verhindert, dass die Regelungswirkung der EU-Direktive sich auf Landes- und kommunaler Ebene entfalten kann.

Die Kette an Cybersicherheitsversagen und Verantwortungsdiffusion kann beispielsweise unter der ehrenamtlich gepflegten Webseite www.kommunaler-notbetrieb.de eingesehen werden und erweitert sich derweil kontinuierlich. Die Vielzahl der Vorfälle zeugt weder von ernstgemeintem Verständnis der Problemlage noch der Umsetzung einer defensiven Cybersicherheitstrategie im Sinne der EU NIS-2 Richtlinie.

Kommunale Selbstverwaltung und Föderalismus sind ein hohes Gut, was nur dadurch aufrecht gehalten werden kann, wenn die Kommunen und Landkreise eine entsprechende Cybersicherheitsstärkung erhalten, da sie eigenständig dazu nicht in der Lage sind. Dies nicht zu berücksichtigen, ist für die AG KRITIS äußerst fahrlässig, da die betroffene Bevölkerung keine Handlungsalternative hat und die Kommunen und Landkreise eigenständig schlicht keine angemessenen Ressourcen einbringen können.

So sehr zu begrüßen ist, dass der Sektor Staat und Verwaltung mit der NIS2 Richtlinie erstmals umfassend nach KRITIS-Gesichtspunkten reguliert wird, so sehr sehen wir auch, dass hier die Chance auf eine einheitliche Regelung für alle Ebenen des Sektors Staat und Verwaltung vertan wird. Eine effektive Umsetzung im Sinne der EU setzt voraus, dass entweder die 16 Bundesländer vergleichbare Gesetze erlassen, oder eine Föderalismus-Reform durchgeführt wird, die dem Bund die notwendige Kompetenz gibt, die IT-Sicherheit und Resilienz der staatlichen Verwaltung auf Länder- und kommunaler Ebene zu regeln.

Für Einrichtungen der Bundesverwaltung finden nach § 29 (2) NIS2UmsuCG grundsätzlich die Regelungen für "besonders wichtige Einrichtungen" Anwendung, wobei hiervon unverständlicher Weise die folgenden Regelungen ausgenommen werden sollen:

- § 30 - Keine Risikomanagementmaßnahmen außer für das Bundeskanzleramt und die Bundesministerien
- § 43 (5) - Keine Zusammenarbeit der Nachrichtendienste mit dem BSI für z.B. Lagebilder
- § 65 - Keine Bußgeldvorschriften

Der Ausschluss des § 30 adressiert den Kern der Cybersicherheitsmaßnahmen. Maßnahmen nach Stand der Technik wie z.B. Risikoanalysen, Bewältigung von Sicherheitsvorfällen, Sicherheit der Lieferkette, Management und Offenlegung von Schwachstellen, Kryptografie und Verschlüsselung, Sicherheit des Personals und Verwendung von Multi-Faktor-Authentifizierung sind daher allesamt für Einrichtungen der Bundesverwaltung nicht ausschlaggebend und nicht zu berücksichtigen. Offenbar können Einrichtungen der Bundesverwaltung Cybersicherheit Kraft Magie realisieren.

Dieser Ausschluss erzeugt starkes Kopfschütteln und lässt uns mit Verwunderung und Fassungslosigkeit zurück.

Es ist mindestens notwendig, die Pflichten die aus § 30 (1) und (2) folgen, auf den Geltungsbereich des § 43 auszudehnen, denn bisher sind an keiner anderen Stelle vergleichbare Pflichten für die Bundesverwaltung festgelegt.

Mit § 29 (1) Nr. 2 werden im weitesten Sinne alle öffentlichen IT-Dienstleister (Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Vertrauensdiensteanbieter, Managed Service Provider und Managed Security Services Provider) ausgeschlossen, welche Dienste für Landes- oder Kommunalverwaltungen anbieten und bereits durch die Länder (wie auch immer geartet) reguliert wurden.

Es bleibt unverständlich, warum relevante Dienstleister lediglich aufgrund der Rechtsform ausgeschlossen werden. An den erheblichen Auswirkungen erfolgreicher Angriffe auf kommunale und regionale Dienstleister besteht kein Zweifel, völlig unabhängig davon, ob diese sich in öffentlicher Trägerschaft befinden oder als kommerzielle Unternehmen tätig sind.

Die in Deutschland vorgenommene starke Trennung von öffentlicher Verwaltung und kommerziellen Unternehmen ist aber nicht alternativlos. Wer sich die NIS2 Umsetzung in anderen Ländern anschaut, wird schnell feststellen, dass zum Beispiel in Dänemark die regionalen und kommunalen öffentlichen Verwaltungen und deren Organisationen genau wie kommerzielle Unternehmen den jeweiligen Sektoren zugeordnet werden[4]. Darüber hinaus ist zu überlegen, ob öffentliche IT-Dienstleister deutscher Landes- und Kommunalverwaltungen nicht ohnehin in den Anwendungsbereich der „Durchführungsverordnung (EU) 2024/2690 der EU-Kommission“[5] fallen, sofern Dienstleistungen in einem der regulierten Bereiche (zum Beispiel cloud computing service provider, data centre service provider, managed service provider) erbracht werden.

Dementsprechend stellt sich nicht die Frage, „ob“ sondern „wie“ öffentliche IT-Dienstleister auch auf Landes- und Kommunal-Ebene auf ein ausreichendes Sicherheitsniveau gebracht werden können.

Die AG KRITIS fordert auch hier wieder eine klare, bundeseinheitliche Regelung für öffentliche IT-Dienstleister auf allen Ebenen – der Bundesebene, der Bundeslandebene und der Kommunalen Ebene, denn Cyberangriffe und Datenpakete machen keine Ebenenunterscheidung im Cyberraum. Die AG KRITIS sieht - so wie auch das Grundgesetz - den Bund in der Pflicht, gleichwertige Lebensverhältnisse für öffentliche Dienstleistungen der Daseinsvorsorge zu gewährleisten (Art. 72 (2) GG). Dies kann nur ohne Benachteiligung erfolgen, wenn diese länderübergreifend einheitlich definiert sind.

Beispielsweise zeichnet Art. 73 (1) Nr. 7 GG schon deutlich vor, dass Telekommunikation eben nicht an den Landesgrenzen halt macht und daher eine landesübergreifende Regulierung erforderlich macht. Der Themenkomplex der IT-Sicherheitsregulierung konnte insgesamt nur entstehen, weil die Telekommunikationsinfrastruktur eine solch umfassende Bedeutung für ein modernes Staatswesen bekommen hat. Eine bundeseinheitliche Regelung, z.B. durch Konkretisierung des Art 73 (1) Nr. 7 GG erscheint daher als logische Folge auf die Gedanken der Gründerväter der Republik. Auch das BVerfG schreibt in seiner Entscheidung 1 BvR 396/98: „Die durch Art. 73 Nr. 7 GG erfolgte Zuweisung der ausschließlichen Gesetzgebungskompetenz an den Bund für das Fernmeldewesen - jetzt mit dem Begriff Telekommunikation umschrieben - betrifft die technische Seite der Telekommunikationsinfrastruktur und die auf Informationsübermittlung mit Hilfe von Telekommunikationsanlagen bezogenen Dienste, erfasst aber nicht Regelungen zu den übermittelten Inhalten oder zu ihrer Entstehung und Nutzung“. Eine Grundgesetzreform,

4 vgl. Kapitel 6 in https://samsik.dk/wp-content/uploads/2025/06/SAMSIK-vejledning-om-anvendelsesomradet-2025.pdf
5 https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/eng

die dem Bund die Gesetzgebungskompetenz über IT-Sicherheit in Staat und Verwaltung der Länder ermöglicht, scheint daher nicht pauschal dem Föderalismusgedanken zu widersprechen.

Gerade die IT-Sicherheitsvorfälle der vergangenen Monate und Jahre und die hohe Zahl an öffentlichen IT-Dienstleistern, die mehrere Kommunen und Länder bedienen, zeigt die Kritikalität dieser Dienste für die Öffentlichkeit und für alle Bürgerinnen. Eine Unterscheidung nach Zuständigkeiten, Ebenen oder Schwellenwerten würde Bürgerinnen aus Sicht der AG KRITIS in unterschiedliche Versorgungsklassen einordnen, was in deutlichem Widerspruch zu Gleichheitsgebot und Daseinsvorsorge steht.

§ 44 (Vorgaben des Bundesamtes) Absatz 1 wurde geändert. Bislang erhielt der IT-Grundschutz lediglich für die Bundesministerien und das Bundeskanzleramt mittelbaren Gesetzesrang. Nun gilt das für alle Einrichtungen der Bundesverwaltung. Wir begrüßen diese Ausdehnung, kritisieren aber weiterhin die umfassenden Möglichkeiten, Einrichtungen der Bundesverwaltung vom Geltungsbereich dieses Gesetzes auszunehmen. Eine Ausnahme von der Gültigkeit dieses Gesetzes kann aus unserer Sicht nur dann gestattet werden, wenn die Erreichung eines gleichwertigen IT-Sicherheitsniveaus auf andere Weise sichergestellt wird. Dies ist insbesondere notwendig für das BMVg und die Einrichtungen des AA.

Sofern darüber hinaus die Einrichtungen der Bundesverwaltung in § 43 (4) Satz 2 erst nach drei Jahren erstmalig und danach nur „regelmäßig“ statt beispielsweise „anschließend alle drei Jahre“ dem BSI die Erfüllung der Anforderungen nachweisen sollen, wird die überaus lückenhafte Umsetzungsanforderung noch unnötig verzögert. Wir erkennen an, dass zwischen unserer letzten Stellungnahme und dieser die Frist von fünf auf drei Jahre geändert wurde, fordern aber weiterhin die Konkretisierung von „regelmäßig“ zu einem benannten Zeitraum. Noch besser wäre allerdings die Formulierung einer „unverzüglichen“ Meldung der Erfüllung der Anforderungen.

CISO Bund

Zuvorderst begrüßt die AG KRITIS die Einführung des "CISO Bund" (Koordinatorin oder Koordinator für Informationssicherheit). Jedoch sind wir verwundert, dass in § 48 keine Aussagen darüber getroffen werden, wo genau diese Rolle eingerichtet werden soll: hier fordern wir insbesondere eine Unabhängigkeit des „CISO Bund“ vom "CIO Bund" und auch dem Bundesamt für Sicherheit in der Informationstechnik (BSI), um so eine wirkungsvolle Kontrollinstanz darstellen zu können. Idealer Weise ist er auch vom Bundesministerium des Innern (BMI) unabhängig und beispielsweise im Bundeskanzleramt als Stabsstelle zu verankern.

Darüber hinaus wurde dieses Amt weder mit angemessenen Aufgaben, noch mit darauf ausgerichteten angemessenen Befugnissen ausgestattet.

Ausnahmen als Regelfall

In § 37 Ausnahmebescheid ist die Möglichkeit vorgesehen, einen Großteil der Funktionsfähigkeit eines souveränen Staates auszuklammern. **Das BMI, das Bundeskanzleramt, das BMJV, das BMVg, das BMF und die Innenministerien der Bundesländer können BWE oder WE ganz oder teilweise von diesem Gesetz ausnehmen.**

Auch **alle Einrichtungen, die in den Bereichen nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung, einschließlich der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten, (relevante Bereiche) tätig sind oder Dienste erbringen** können dadurch von den Risikomanagementmaßnahmen nach § 30 und den Meldepflichten nach § 32 befreit werden.

Auch **alle Einrichtungen, die ausschließlich für Behörden, die Aufgaben in relevanten Bereichen erfüllen, tätig sind oder Dienste erbringen**, können von den Risikomanagementmaßnahmen nach § 30 und den Meldepflichten nach § 32 befreit werden.

Ein funktionaler und souveräner Staat macht sich bei Bürgerinnen in erster Linie im Rathaus und funktionierenden Fachverfahren in den Landkreisen und Kommunen aus. In zweiter Linie in der (demokratischen) Funktionsfähigkeit der o.g. Strafverfolgungsbehörden und weiteren BOS etc. Falls diese weiterhin von den Cybersicherheitsanforderungen ausgenommen werden und dadurch **weggecybert** werden, wird die **Destabilisierung der Bevölkerung von innen** weiter voranschreiten und nicht aufzuhalten sein.

Risikomanagement, Haftung der Geschäftsleitung und Durchsetzungsmaßnahmen

Mit § 30 des NIS2UmsuCG werden umfassende Maßnahmen zum Risikomanagement für BWE und WE eingeführt, welche nach § 31 für Betreiber kritischer Anlagen zusätzlich verschärft werden. Diesen umfassenden Maßnahmenkatalog begrüßen wir ausdrücklich und bedanken uns vorab beim Gesetzgeber für den Willen zur Umsetzung von Cybersicherheit schon im Jahre **2025**.

Vor allem stellen wir fest, dass die hiermit definierten Maßnahmen die reine Cybersicherheitsbetrachtung zur Umsetzung eines Informationssicherheits-Managementsystems (ISMS) überschreiten. Insbesondere die Rollen des Business Continuity Management (BCM) und des IT Service Continuity Management (ITSCM) werden hiermit in den betroffenen Einrichtungen gefordert und gestärkt, sowie zusätzlich zentrale Kapazitäten im organisationsweiten Krisenmanagement gefordert. Wir sehen dies als notwendige Voraussetzungen dafür, um Kritische Infrastrukturen als auch BWE und WE umfassend vor Gefahren zu schützen, welche die Geschäftstätigkeit gefährden, sowie die Fortführung der kritischen Dienstleistungen auch bei Sicherheitsvorfällen zu gewährleisten. Die Vergangenheit hat gezeigt, dass Einrichtungen in der Selbstregulierung schlicht versagt haben und die bestehenden Anforderungen an KRITIS-Betreiber nicht ausreichen, um die Versorgungssicherheit der Bevölkerung zu gewährleisten.

Der Bitkom Verband mit über 2.200 Mitgliedsunternehmen stellt dazu in einer aktuellen Veröffentlichung[6] fest:

> „8 von 10 Unternehmen von Datendiebstahl, Spionage oder Sabotage betroffen. Rekordschaden von rund 267 Milliarden Euro.“

Offensichtlich belegen diese Zahlen (ermittelt durch die Wirtschaft selbst!), dass die **deutsche Wirtschaft nicht in ihrer Selbstverantwortung Willens** ist, die Versorgungssicherheit der Bevölkerung zu gewährleisten.

Sowohl für BWE als auch für WE sind in §§ 61-62 umfassende Befugnisse des BSI für Maßnahmen zur **Aufsicht und Durchsetzung** zu etablieren. Insbesondere die Möglichkeit, sich die Umsetzung von Maßnahmen durch Betreiber kritischer Anlagen, aller anderen BWE sowie der WE nachweisen zu lassen, sowie diese auch extern auditieren zu dürfen, begrüßt die AG KRITIS ausdrücklich.

Insgesamt ergibt sich hieraus erstmals ein begrüßenswertes und umfassendes Set aus Regelungen, Kontroll- sowie Sanktionsmechanismen, auch wenn die Ausnahmeregelungen leider äußerst umfassend ausgereizt werden. Die mit dem § 61 (3) eingeführte Frist von drei Jahren nach Einführung des Gesetzes, insbesondere für BWE, betrachten wir als nicht erforderlich: die EU NIS2-Richtlinie ist seit 2022 verabschiedet und bereits bekannt.

6 https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2024

Das BSI wird weiterhin fachlich, rechtlich und dienstlich vom BMI beaufsichtigt. Trotz der Änderung des § 1 im Jahr 2021 ist die **fachliche Unabhängigkeit des BSI** weiterhin unzureichend. Wenn das BSI als solches weiterhin leider nicht unabhängig vom BMI sein soll, bedarf es einer vom BMI unabhängigen Kontrolle der umfassenden Tätigkeiten und Rechtsbefugnisse des BSI, die über die Berichtspflichten des BSI gemäß § 58 an das BMI hinaus geht. Obwohl das Versprechen der Ampelregierung, das BSI unabhängiger aufzustellen, durch Änderung des §1 gehalten wurde, so erscheint die **operative Umsetzung der Reduktion der Fachaufsicht seitens BMI unzureichend**.

Technische Expertise und Befugnisse des BSI

Das BSI hat über Jahre hinweg die beachteten **IT-Grundschutz- und Mindeststandards nach dem Stand der Technik** entwickelt und dafür Anerkennung bekommen. Es ist unverständlich, warum dieser Sachverstand in § 44 (2) mit dem Zusatz „dabei wird der Umsetzungsaufwand soweit möglich minimiert“ mit einem Dämpfer versehen wird, um billige Maßnahmen durchzusetzen. Die Bewertung nach Stand der Technik hat bereits die Angemessenheit der empfohlenen Maßnahmen berücksichtigt.

Die Empfehlungen zur Änderung des § 44 (1) und (2) aus unserer letzten Stellungnahme von 2024[7] wurden fast wortwörtlich und sinnerhaltend umgesetzt. Für die Berücksichtigung dieses Impulses bedanken wir uns herzlich.

Weiterhin hat das BSI die letzten Jahre durch regelmäßige Schwachstellenscans und dem direkten Kontaktieren von Betreibern verwundbarer Systeme konkret zur Cybersicherheit im Land beigetragen. Die Einschränkungen auf lediglich „bekannte“ Schwachstellen in § 15 (1) ist nicht nachvollziehbar, da hiermit dem BSI weitere defensive aber hilfreiche technische Möglichkeiten versagt werden.

Zur Abwehr von laufenden Angriffskampagnen (konkrete erhebliche Gefahr) gegen Kommunikationstechnik des Bundes, BWE, WE, Telekommunikationsdienste oder eine erhebliche Anzahl von Systemen, kann das BSI technische Maßnahmen gegenüber Anbietern von Telekommunikationsdiensten (§ 16) und von digitalen Diensten (§ 17) anordnen. Wir begrüßen, dass der zwischenzeitlich gestrichene Begriff „konkret“ wieder ergänzt wurde, denn sonst würden dadurch massive Eingriffe in Systeme wie „technische Befehle zur Bereinigung“ bei einer wesentlich niedrigeren Schwelle möglich, was bei Fehlen eines Angriffs und somit von Gefahr im Verzug nicht nachvollziehbar ist.

Der ergänzte Satz in § 11 (4) i.V.m. § 3 (7) KritisDG erlaubt dem BSI, dem BBK erforderliche Informationen zu Sicherheitsvorfällen mitzuteilen. Wir begrüßen diese Festlegung und erwarten daher, dass die eckigen Klammern um diesen Abschnitt noch nach einer Einigung entfernt werden.

Die Gesetzesbegründung zu § 5c EnWG (IT-Sicherheit im Anlagen- und Netzbetrieb, Festlegungskompetenz) Absatz 2 wurde um sehr begrüßenswerte Abschnitte zur Zusammenarbeit von BSI und Bundesnetzagentur (BnetzA) erweitert. Das begrüßen wir ausdrücklich, da beide Behörden dadurch gemeinsam und abgestimmt am Ziel arbeiten werden, die IT-Sicherheit zu erhöhen und somit gemeinsam die defensive Cybersicherheit im Sinne der EU NIS2 zu realisieren.

Bislang oblag die Aufsicht über KRITIS-Betreiber im Sektor Strom hinsichtlich der Einhaltung von Cybersicherheitsmaßnahmen hauptsächlich der BNetzA. Über die jetzt vorgesehene Einvernehmensregelung bekommt das BSI größeren Einfluss auf die IT-Sicherheitsanforderungen im Sektor Energie. Das BSI kann so ein einheitliches Sicherheitsniveau über alle KRITIS-Sektoren sicherstellen, was es in seiner Rolle als zentrale Cybersicherheitsbehörde stärkt.

7 https://ag.kritis.info/2024/10/27/schriftliche-stellungnahme-zum-gesetzentwurf-der-bundesregierung-des-nis2umsucg-vom-02-10-2024/

Meldepflicht

Die AG KRITIS begrüßt die in § 32 definierte gemeinsame Meldestelle für das BSI sowie das BBK. Insbesondere im Hinblick auf das parallel in der Umsetzung befindliche KRITIS-Dachgesetz, da physische Sicherheit und Cybersicherheit als auch das dafür zu betreibende Krisenmanagement Hand in Hand agieren muss. Sicherheitsvorfälle jedweder Art sollten daher zentral und einheitlich an eine Meldestelle kommuniziert werden. Die AG KRITIS empfiehlt daher auch, dies beispielsweise bei derzeit darüber hinaus gehenden Meldungen an die Bundesnetzagentur (BNetzA) und die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) so zu vereinheitlichen. Bürokratie und Komplexität sind der Feind der Sicherheit, auch bei der Meldung von Sicherheitsvorfällen.

In § 43 (5) werden Einrichtungen der Bundesverwaltung darüber hinaus aufgefordert „alle für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik erforderlichen Informationen, insbesondere zu Schwachstellen“ unverzüglich zu melden. Dies konnte aber zum Beispiel aufgrund von Regelungen zum Geheimschutz oder Vereinbarungen mit Dritten unterbleiben. Dies ist nicht nachvollziehbar, da auch das BSI nicht nur ein berechtigtes Interesse an diesen Informationen hat, sondern auch als Bundesbehörde grundsätzlich vertrauenswürdig ist und mit Unterlagen die dem Geheimschutz unterfallen, umgehen kann. Eine gesetzliche Regelung an dieser Stelle würde auch die Verarbeitung von Informationen erlauben, die unter einen privatrechtlichen NDA mit einem Dritten fallen.

Bis zum Jahresende muss eine Statistik über die unterdrückten Meldungen an das BSI übermittelt werden, dies ist nicht ausreichend. Die AG KRITIS bedauert, dass selbst diese statistische Auswertung für den Bundesnachrichtendienst und das Bundesamt für Verfassungsschutz ausbleiben soll. **Dadurch wird auch den Kontrollgremien wichtige Transparenz über die Verheimlichung von dem Staat bekannten Schwachstellen genommen.**

Empfehlungen des Bundesrechnungshofes

Die AG KRITIS schließt sich den Empfehlungen des Bundesrechnungshofes in seinem „Bericht nach § 88 Absatz 2 BHO an den Haushaltsausschuss des Deutschen Bundestages und den Ausschuss für Inneres und Heimat des Deutschen Bundestages zum Regierungsentwurf des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes (NIS2UmsuCG)“[8] vom 17.09.2024 vollständig an. Die darin aufgeführten Empfehlungen sollten dringend realisiert werden!

Regulierung von DNS-Betreibern

Die im aktuellen Entwurf des NIS2-Umsetzungsgesetzes vorgesehene Definition von DNS-Diensteanbietern (§ 2 Nr. 8) sowie deren pauschale Einstufung als „besonders wichtige Einrichtungen“ (§ 28 Abs. 1) führt zu **erheblichen systematischen und praktischen Problemen**. Nach der derzeitigen Fassung fallen selbst natürliche Personen unter diese Regelung, sofern sie öffentliche rekursive oder autoritative DNS-Dienste betreiben. Damit geraten z.B. auch zivilgesellschaftliche und gemeinnützige Akteure ins Visier der Regulierung – etwa Vereine wie Digitalcourage[9], die mit dem Ziel der digitalen Selbstbestimmung eigene, zensurfreie DNS-Dienste bereitstellen, oder Initiativen wie Freifunk[10], die im Rahmen dezentraler, ehrenamtlich betriebener Netzinfrastruktur ebenfalls öffentliche DNS-Resolver anbieten. Diese Akteure

8 https://www.bundesrechnungshof.de/SharedDocs/Downloads/DE/Berichte/2025/nis-2-richtlinie-volltext.pdf?__blob=publicationFile&v=4
9 https://digitalcourage.de/support/zensurfreier-dns-server
10 https://freifunk.net

handeln ohne wirtschaftliches Interesse und betreiben ihre Dienste im öffentlichen Interesse. Eine Einstufung als besonders wichtige Einrichtung erscheint vor diesem Hintergrund weder sachgerecht noch verhältnismäßig.

Zudem ist die in § 2 Nr. 8 sowie in der Kritisverordnung (Nr. 6.1.2) vorgenommene Ausnahme für Betreiber von Root Nameservern unverständlich. Gerade Root Nameserver bilden das Rückgrat des globalen DNS-Systems und sind daher in besonderem Maße schützenswert. Die Ausklammerung aus der Regelung wirkt daher widersprüchlich.

Auch die versuchte Differenzierung anhand der Frage, ob ein DNS-Dienst integraler Bestandteil eines Internetzugangsdienstes ist oder nicht, überzeugt nicht. Die öffentliche Verfügbarkeit eines rekursiven DNS-Servers besteht unabhängig davon, ob er durch den eigenen oder einen fremden Zugangsanbieter bereitgestellt wird. Die Unterscheidung trägt daher weder zur rechtssicheren Abgrenzung bei, noch löst sie das Problem der übermäßigen Erfassung kleiner, nicht-kommerzieller Betreiber.

Statt einer pauschalen Einbeziehung aller DNS-Diensteanbieter bedarf es einer präziseren und risikobasierten Abgrenzung. Ziel muss es sein, tatsächlich systemrelevante und ausfallgefährdete Infrastrukturen zu identifizieren – nicht jedoch **bürgerschaftliches Engagement und gemeinwohlorientierte digitale Angebote** durch überbordende Regulierung zu gefährden und entsprechende Kollateralschäden zu verursachen.

Wir empfehlen dem BMI daher die Neufassung dieser Festlegungen. Anhand kommerzieller Kriterien wie z.B. einer Gewinnerzielungsabsicht für den Betrieb von autoritativen Nameservern lassen sich ehrenamtliche Initiativen sauber von kommerziellen trennen. Darüber hinaus braucht es die Festlegung, dass Root-Nameserver nicht nur als BWE, sondern direkt als KRITIS gelten.

Verpflichtung zur Zugangsgewährung zu DN-Registrierungsdaten

§ 50 BSIG sieht vor, dass TLD-Registries und Domain-Name-Registry-Dienstleister berechtigten Zugangsnachfragern auf begründeten Antrag hin unter Darlegung eines berechtigten Interesses Zugang zu den nach § 49 BSIG zu sammelnden Registrierungsdaten zu gewähren haben. Das ist unter zwei Gesichtspunkten problematisch.

Zum Einen gehören auch die **Verfassungsschutzbehörden des Bundes und der Länder** nach § 2 Nr. 2e zu den **„berechtigten Zugangsnachfragern“**. Warum diese Zugang benötigen bleibt aber **unklar**. Nach Art. 28 (1) der NIS2 soll die Datenbank „einen Beitrag zur Sicherheit, Stabilität und Resilienz des Domainnamenssystems“ leisten. Da die Nachrichtendienste primär der Informationsbeschaffung dienen, bleibt aber völlig unklar, welchen Beitrag sie zum Ziel des Art. 28 (1) NIS2 leisten sollten. Die Aufnahme in den Kreis der berechtigten Zugangsnachfrager erweckt daher den Eindruck, dass dies weniger dem Ziel der Cybersicherheit dient, sondern eher der **schleichenden Erweiterung nachrichtendienstlicher Befugnisse**. Im Sinne der Cybersicherheit sind die Nachrichtendienste daher aus der Liste der berechtigten Zugangsnachfrager zu streichen!

Zum anderen bleibt auch unklar, wann ein „berechtigtes Interesse“ vorliegen soll. Ohne weitere gesetzliche Festlegung bleibt die Regelung daher für die Herausgabeverpflichteten risikobehaftet und für die Grundrechtsträger, deren Daten herausgegeben werden, ein **problematischer Eingriff in ihre Rechte**. Da der verweigerte oder zu spät gewährte Zugang bußgeldbewehrt ist, droht ihnen, dass ihre Daten von den Registries und Dienstleistern eher einmal zu viel als einmal zu wenig herausgegeben werden, um Bußgelder

zu vermeiden. Das ist nicht akzeptabel. Wir fordern das BMI daher auf, gesetzlich zu regeln, wann ein berechtigtes Interesse vorliegt.

Veröffentlichung von branchenspezifischen Sicherheitsstandards (B3S)

Wir fordern, dass alle branchenspezifischen Sicherheitsstandards, die eine Eignungsfeststellung erhalten, vom BSI **kostenfrei und öffentlich verfügbar** abgerufen werden können. Nur so kann der Stand der Technik eingehalten und transparent abgebildet werden.

Evaluierung der Umsetzung

Jegliche Paragraphen zur wissenschaftliche Evaluierung des Gesetzes sind im Vergleich zu vorherigen Fassungen gestrichen worden. Dies **widerspricht einem wissenschaftlichen und evidenzbasierten Vorgehen**. Wir fordern daher weiterhin die regelmäßig stattfindende wissenschaftliche Evaluierung der in diesem Gesetz getroffenen Festlegungen.

Die regelmäßig stattfindende wissenschaftliche Analyse der Umsetzung der aus diesem Gesetz folgenden Maßnahmen ist für die Feststellung der nationalen Cybersicherheitslage **unumgänglich und alternativlos**. Wenn es also von staatlicher Seite als nötig empfunden wird, auch in ein paar Jahren einen Überblick über die Resilienz der deutschen Wirtschaft und Verwaltung zu haben, sollten dringend wieder umfassende Evaluierungspflichten im Gesetz festgehalten werden. Wir empfehlen dem BMI, für die Evaluierung nicht nur betroffene Unternehmen und deren Wirtschaftsverbände einzubinden, sondern auch Behördenvertreter, die Wissenschaft und die Zivilgesellschaft und die Ergebnisse im Sinne der Nachvollziehbarkeit und Transparenz öffentlich zu machen.

Würdigung des Prozesses

Abschließend betonen wir als AG KRITIS erneut, dass ein transparenter Prozess in der Gesetzgebung sowie umfassende und zeitlich angemessene Beteiligungsverfahren der Wirtschaft, Wissenschaft und Zivilgesellschaft bei derart tiefgreifenden und weitreichenden Gesetzgebungsverfahren dringend geboten ist und bei diesem Vorhaben **weitestgehend berücksichtigt** wurde.

Insbesondere hinsichtlich einer einheitlichen und kongruenten Regulierung im KRITIS-Umfeld betrachten wir als AG KRITIS eine gleichzeitige Veröffentlichung und Diskussion von Gesetzesentwürfen zur Umsetzung der NIS2-Richtlinie (NIS2UmsuCG) und CER-Richtlinie (KRITIS-Dachgesetz) sowie der im NIS2UmsuCG vorgesehenen Verordnungen für **zwingend erforderlich**.

Fazit

Es bleibt festzuhalten, dass weiterhin keine vollständige Harmonisierung der Regelungen zwischen den beiden Gesetzesvorlagen NIS2-Richtlinie (NIS2UmsuCG) und CER-Richtlinie (KRITIS-Dachgesetz) erfolgt ist. Eine hinreichende Überprüfung ist aktuell aufgrund mangelnder Transparenz nicht leistbar. Übrig bleibt eine unsichere Lage bei allen potenziell betroffenen Einrichtungen und ihren Lieferketten, sowie bei allen verantwortlichen Aufsichtsbehörden und Zuständigen für die Umsetzung und Einhaltung der kommenden Regulierungen als auch bei der Wissenschaft, Forschung und zuletzt auch der fachkundigen Bevölkerung, die willens sind, ihren Beitrag durch Fachexpertise ehrenamtlich und kostenfrei beizutragen, dies aber nicht angemessen in den intransparenten Dialog einbringen können.

Die NIS2-Richtlinie soll in erster Linie eine defensive Cybersicherheitstrategie sein, welche bisherige Strukturen stärkt und EU-weit harmonisiert. Für Deutschland würde sich hier die einmalige Chance bieten, die gewachsenen Verantwortlichkeiten, die mit dem "Wimmelbild der Verantwortungsdiffusion" in der Öffentlichkeit bekannt sind, aufzuräumen. Konkret bedeutet das, alle Ebenen im Staat in die Lage zu versetzen effektiv Cybersicherheit herzustellen. In der Wirtschaft werden längst höhere Maßstäbe angesetzt, die staatliche Einrichtungen und öffentliche Verwaltungen nicht leisten müssen. Wenn aus Deutschland eine Cybernation werden soll, dann muss die Regierung aufhören hier Ausnahmen zu machen, sondern hart arbeiten, anpacken und kompromisslos umsetzen.

Cybersicherheit ist eine gesamtgesellschaftliche Leistung und an der Spitze muss ein moderner Staat als Vorbild stehen. Ein Staat der versteht, das offensive Optionen im Cyber- und Informationsraum vorallem seinen BürgerInnen schadet. Die kürzlich geäußerten Forderungen nach einem "Cyberdome" zeigen, dass auch der neue Bundesminister des Inneren nicht verstanden hat, wie der Cyberraum funktioniert.

Jeder IT-Sicherheitsforscher wird bestätigen, dass wir im Cyberraum hohe Burgmauern und tiefe Burggräben benötigen, aber keine Kanonen und erst Recht keinen Cyberdome.

Statt Milliarden für KI-Gigafactorys auszugeben wäre es dringend notwendig, die Brot-und-Butter Aufgaben der Digitalisierung auskömmlich zu finanzieren und konsequent umzusetzen. Damit kann man zwar keine Schlagzeilen machen, aber – und nur das sollte zählen – die Bevölkerung vor Cyberangriffen und deren Auswirkungen schützen.

Statt viel Geld in bürgerrechtsverachtende Spionagesoftware aus dem Hause Palantir zu investieren wäre es zielführender, ein durchgängig hohes IT-Sicherheitsniveau auf allen Ebenen des Staates umzusetzen und den Ländern bei der Einführung von Software ohne verfassungsrechtliche Problemen zu helfen.