AG KRITIS

Arbeitsgruppe Kritische Infrastrukturen

Stellungnahme zum Referentenentwurf des NIS2UmsuCG vom 29.05.2024

Version 1.0 – zuletzt editiert am 29.05.2024

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

Mit dem vorliegenden Referentenentwurf des NIS2UmsuCG wird die Umsetzung der EU NIS2-Richtlinie (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 über 23 Gesetze und Verordnungen ändert. Unsere Kommentierung bezieht sich hierbei ausschließlich auf die unter Artikel 1 und in Teilen unter Artikel 2 eingebrachte Änderung des BSI-Gesetzes.

Definition Kritischer Infrastrukturen

Bisher definiert § 2 (10) BSI-Gesetz die "Kritische Infrastrukturen". Mit der Umsetzung der NIS2-Richtlinie wird dies nunmehr ersetzt durch eine Unterscheidung in "Besonders wichtige Einrichtungen" (BWE) und "wichtige Einrichtungen" (WE) sowie als Teil der BWE die "Betreiber kritischer Anlagen". Die Definitionen als BWE oder WE sind einerseits an Schwellwerte der Beschäftigten und des Umsatzes gebunden (sogenannte EU-Size Cap Regelung), und andererseits an eine klare Sektorendefinition in den Anlagen 1 und 2 des NIS2UmsuCG. Für "kritische Anlagen", welche den bisherigen KRITIS-Anlagen entsprechen, gilt weiterhin eine noch zu erlassende Rechtsverordnung, welche dann die bisherige Kritisverordnung ersetzen soll.

Klar ist damit, dass die Regelungen über Kritische Infrastrukturen (KRITIS) deutlich komplexer einerseits und umfassender andererseits werden. Während wir als AG KRITIS eine umfassendere Auslegung der KRITIS begrüßen, sehen wir erhöhte Komplexität KRITISch:

Einrichtungen sollten idealerweise an einheitlich definierten Sektoren und weiteren Kennzahlen (Umsatz, versorgte Bevölkerung, regionales Versorgungsmonopol uvm.) klar und rechtlich eindeutig identifizieren können, ob sie als KRITIS gelten. Insbesondere unterschiedliche Definitionen der Sektoren in den unterschiedlichen Kategorien (Besonders wichtige Einrichtungen, wichtige Einrichtungen, kritische Anlagen) und Anlagen erhöhen hier die Komplexität bereits in der Betroffenheitsanalyse.

Die Konkretisierung der Definition von "kritischen Anlagen" wird nach § 58 (4) durch das BMI im Zusammenwirken mit anderen Ministerien erarbeitet. Entgegen der bisherigen Praxis sind in diesen Prozess Akteure aus der Wissenschaft nicht (mehr) eingebunden. Für alle Regelungen des § 58 fordern wir weiterhin die verbindliche Einbindung der Zivilgesellschaft, die bisher und offenbar auch zukünftig weiterhin keine Berücksichtigung finden soll.

Aufgrund der Komplexität der Regelungen fallen weitere Sonderfälle auf, wie hier am Beispiel des Sektors Forschung: 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.

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. Auch hier braucht es verbindliche Anforderungen zur Umsetzung von Cybersicherheitsmaßnahmen, da die Selbstregulierung auch in diesen Fällen nicht greift.

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 SIT.NRW (über 100 Kommunen waren monatelang betroffen und faktisch handlungsunfähig!) nicht mehr nachvollziehbar, offensichtlich soll der Jahrzehnte gepflegte Investitionsstau weiterhin aufrecht gehalten werden. Die Kette an Cybersicherheitsversagen und Verantwortungsdiffusion kann beispielsweise unter der ehrenamtlich gepflegten Webseite https://kommunaler-notbetrieb.de eingesehen werden und erweitert sich derweil kontinuierlich. Dies zeugt nicht von ernstgemeintem Verständnis, was nach § 2 (1) Nr. 23:

> *„kritische Dienstleistung“ eine Dienstleistung zur Versorgung der Allgemeinheit in den Sektoren nach § 28 Absatz 7, deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde;*

ist bzw. es soll dieses Jahrzehnte gepflegte systemische Versagen weiterhin aufrecht erhalten bleiben, was in keinster Weise nachvollziehbar ist.

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 damit 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.

Zuvorderst begrüßt die AG KRITIS die Einführung des "CISO Bund" (Koordinatorin oder Koordinator für Informationssicherheit). Jedoch sind wir verwundert, dass in den §§ 48-50 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 und für Heimat (BMI) unabhängig und beispielsweise im Bundeskanzleramt als Stabsstelle zu verankern.

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

- § 38 - keine Billigungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen
- § 40 (3) - Keine Zusammenarbeit mit dem BSI für beispielsweise Lagebilder
- § 61 - Keine Bußgeldvorschriften
- § 65 - Keine Aufsichts- und Durchsetzungsmaßnahmen

Mit dem Ausschluss des § 38 werden "Geschäftsleitungen" der Bundesverwaltung von den mit der NIS2-Regulierung eingeführten Billigungs-, Überwachungs- und Schulungspflicht von Ihrer Verantwortung befreit, was für die AG KRITIS nicht nachvollziehbar ist.

Auch der Ausschluss der Bundesverwaltung von § 40 (3) ist hierbei nicht nachvollziehbar, die Regelung in sich wirkt nicht konsistent, da insbesondere hier ja zu Lagebildern und Erkenntnisgewinn beigetragen werden kann. Dies speziell im Hinblick auf Desinformationskampagnen, Trollfabriken, Kriminellen Organisationen, Geheimdiensten und anderen staatlichen Akteuren in Regierungsnetzen und dem von Vorfällen betroffenen Auswärtigen Amt oder sogar in Bundeskanzlerin Merkels Rechner (zu dem es sogar einen Podcast investigativer Recherche gab).

Dass innerhalb der Bundesverwaltung keine Bußgelder nach § 61 gezahlt werden sollen, ist nachvollziehbar. Eine persönliche Verantwortung und Haftung soll aber zusätzlich aufgrund § 38 ebenfalls nicht erfolgen, was nicht nachvollziehbar ist.

Dass mit dem vorliegenden Gesetzesentwurf größtenteils die Möglichkeit des Bundes, konkret des BSI, genommen wird, Audits und Prüfungen nach § 65 gegenüber den Stellen des Bundes

durchzuführen und daraus Auswirkungen und Maßnahmen abzuleiten, verwundert jedoch und ist dringend anzupassen.

Weiterhin werden mit § 28 (9) 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.

Die AG KRITIS fordert auch hier wieder eine klare bundeseinheitliche Regelungen 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, einheitliche Lebens- und Sicherheitsstandards für öffentliche Dienstleistungen des Daseinsvorsorge zu gewährleisten. Dies kann nur ohne Benachteiligung erfolgen, wenn diese länderübergreifend einheitlich definiert sind. Gerade die IT-Sicherheitsvorfälle der vergangenen Monate und Jahre als auch 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.

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 bereits im Jahre 2024.

Vor allem stellen wir fest, dass die hiermit definierten Maßnahmen die reine Cybersicherheitsbetrachtung zur Umsetzung eines Informationssicherheits-Managementsystem (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. Denn die Vergangenheit hat gezeigt, dass Einrichtungen in

der Selbstregulierung schlicht versagt haben und die bestehenden Anforderungen an KRITIS-Betreiber nicht ausreichen, die Versorgungssicherheit der Bevölkerung zu gewährleisten.

Sowohl in der Definition eines Sicherheitsvorfalls nach § 2 (1) Nr. 39, als auch bei der Definition von Risikomanagementmaßnahmen nach § 30 (1) soll die Authentizität als Schutzziel entfernt werden. Dies unterscheidet sich von bisherigen Entwürfen des NIS2UmsuCG sowie auch von den aktuellen Anforderungen des § 8a BSI-Gesetz. Auch wenn das Sicherstellen der Authentizität mit den unter § 30 (1) festgelegten Maßnahmen angestrebt werden soll, ist deren Verletzung demnach zukünftig nicht mehr als Sicherheitsvorfall zu bewerten. Dies sehen wir sowohl für die IT-basierte Kommunikation von Menschen untereinander, aber insbesondere auch für die technische Kommunikation von Kritischen Infrastrukturen als KRITISch: hier kann eine Verletzung des Schutzziels Authentizität selbstverständlich auch zu erheblichen Folgen führen. Daher sehen wir es als gegeben an, dieses Schutzziel weiterhin explizit aufzuführen.

Sowohl für BWE als auch für WE sollen in §§ 65-66 umfassende Befugnisse des BSI für Maßnahmen zur Aufsicht und Durchsetzung etabliert werden. 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 § 65 (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.

Das BSI wird weiterhin - im Widerspruch zum Ampel-Koalitionsvertrag, nach dem die Unabhängigkeit erweitert werden sollte - fachlich und dienstlich vom BMI unverändert beaufsichtigt, da der § 1 weiterhin so und unverändert bestehen bleibt. Wenn das BSI als solches weiterhin leider nicht unabhängig zum BMI werden soll, bedarf es einer vom BMI unabhängigen Kontrolle der umfassenden Tätigkeiten und Rechtsbefugnisse des BSI, die über die Berichtspflichten des BSI gemäß § 60 an das BMI hinaus gehen.

Meldepflicht

Die AG KRITIS begrüßt die in § 32 definierte gemeinsame Meldestelle für das BSI sowie das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (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.

Würdigung des Prozesses und Fazit

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.

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) für zwingend erforderlich.

Es scheint, als sei keine vollständige Harmonisierung der Regelungen zwischen den beiden Gesetzesvorlagen erfolgt - was aber aktuell aufgrund der mangelnden Transparenz nicht überprüfbar ist. Übrig bleibt eine unsichere Lage bei allen potentiell betroffenen Einrichtungen und ihren Lieferketten als auch bei allen verantwortlichen Aufsichtsbehörden und Zuständigen für die Umsetzung und Einhaltung der kommenden Regulierungen sowie 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.