AG KRITIS

Arbeitsgruppe Kritische Infrastrukturen

Stellungnahme zum Regierungsentwurf des NIS2UmsuCG vom 02.10.2024

Version 1.1 – zuletzt editiert am 27.10.2024

1 Arbeitsgruppe Kritische Infrastrukturen 3
2 Stellungnahme 4
Definition Kritischer Infrastrukturen 4
KRITIS Sektor Staat und Verwaltung 6
Ausnahmen als Regelfall 9
Risikomanagement, Haftung der Geschäftsleitung und Durchsetzungsmaßnahmen 9
Systeme zur Angriffserkennung 10
Mangelhafte Unabhängigkeit des BSI 11
Technische Expertise und Befugnisse des BSI 11
Meldepflicht 12
Empfehlungen des Bundesrechnungshofes 12
Schwachstellenmanagement 13
Würdigung des Prozesses 13
Fazit 13

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 (Gesetzentwurf der Bundesregierung, Drucksache 20/13184) 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 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 ändern soll. Unsere Kommentierung bezieht sich hierbei ausschließlich auf die unter Artikel 1 eingebrachte Änderung des BSI-Gesetzes.

Mit dem neuen Referentenentwurf vom 02.10.2024 werden aus unserer Sicht keine wesentlichen Verbesserungen zu den bisherigen Referentenentwürfen erreicht und lediglich **Defizite** aufrechtgehalten:

- § 15 (1): Einschränkung auf **bekannte** Schwachstellen für die Schwachstellenscanner des BSI
- §§ 16,17: Aufhebung der Einschränkungen auf **konkrete** erhebliche Gefahren für die Anordnung von Maßnahmen ggü. Anbietern von Telekommunikationsdiensten
- § 43 (5): **Wegfall** von jährlichen statistischen Meldevorschriften 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
  Anmerkung: Die Vorabfassung weist hier fälschlicher Weise den „§ 4“ statt den „§ 44“ aus.
- § 58 (1-3): Berücksichtigung der **Zivilgesellschaft** vor dem Erlassen von Rechtsverordnungen **fällt komplett weg**

Details zu diesen Punkten sind in den weiteren Erläuterungen eingearbeitet.

Die **bisherigen aufgeführten Defizite** bleiben weiterhin bestehen und sind somit weiterhin gültige Forderungen der AG KRITIS.

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 Betroffenheitsprüfung drastisch, Stichwort Bürokratie.

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.

Für alle Regelungen des § 56 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 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 ihnen im Einvernehmen mit dem zuständigen Ressort angeordnet.

Generell werden Bundesbehörden, öffentlich-rechtlich organisierte IT-Dienstleister der Bundesverwaltung sowie weitere Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie ihre Vereinigungen, ungeachtet ihrer Rechtsform lediglich als Einrichtungen der Bundesverwaltung im Sinne des Gesetzes angesehen, sofern dies durch das BSI im Einvernehmen mit dem jeweils zuständigen Ressort angeordnet wurde.

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 einer ehrenamtlich gepflegten Webseite[3] eingesehen werden und erweitert sich derweil kontinuierlich. Dies zeugt nicht von ernstgemeintem Verständnis, was nach § 2 Nr. 24:

> *„kritische Dienstleistung“ eine Dienstleistung zur Versorgung der Allgemeinheit in den Sektoren Energie, Transport und Verkehr, Finanzwesen, Sozialversicherungsträger sowie Grundsicherung für Arbeitssuchende, Gesundheitswesen, Wasser, Ernährung, Informationstechnik und Telekommunikation, Weltraum oder Siedlungsabfallentsorgung, 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.

Es ist zwar nachvollziehbar, dass der Bundesgesetzgeber aus kompetenzrechtlichen Gründen derzeit nicht selbst tätig werden kann. **Es ist aber dann umso wichtiger, dass sowohl die Vertreter der Bundesregierung als auch die Mitglieder des Bundestages die Notwendigkeit entsprechender IT-Sicherheitsregelungen für Länder und Kommunen bei ihren jeweiligen Pendants auf Ebene der Länder adressieren.**

Denn im föderalen Staat sind sie es, die die Pflicht zur Umsetzung europäischer Richtlinien trifft, wo das Grundgesetz ihnen die Gesetzgebungs- und Verwaltungskompetenz zuweist. Leider muss derzeit jedoch konstatiert werden, dass diese Verpflichtung auf Länderebene teilweise nicht wahrgenommen wird.

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.

Dies sieht der Bundesrechnungshof 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)“* vom 17.09.2024 identisch: *„Die Bundesregierung läuft Gefahr, ihr Ziel zu verfehlen, die Informations- und Cybersicherheit zu verbessern. Sie will die NIS-2-Richtlinie der Europäischen Union 1:1 umsetzen, ihr bereits*

[3] https://kommunaler-notbetrieb.de

bekannte Defizite dabei jedoch nicht aufgreifen. Wenige Änderungen am Gesetzentwurf könnten das Sicherheitsniveau in der Bundesverwaltung deutlich erhöhen.“

Das NIS2UmsuCG setzt offenbar nur die durch die EU erzwungenen Cybersicherheitsmaßnahmen für Deutschland minimalistisch (1:1 Umsetzung) um und vermeidet jedwede weitere Möglichkeit der Cyberresilienz oder Cybersicherheitsstärkung.

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 und für Heimat (BMI) unabhängig und beispielsweise im Bundeskanzleramt als Stabsstelle zu verankern.

Darüber hinaus wurde dieses Amt weder mit angemessenen Aufgaben, noch mit angemessenen Befugnisse ausgestattet.

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

- § 30 - Keine Risikomanagementmaßnahmen (lediglich für Bundeskanzleramt und die Bundesministerien)
- § 38 - keine Haftungsregelungen für Geschäftsleitungen
- § 40 (3) - Keine Zusammenarbeit mit dem BSI für beispielsweise Lagebilder
- § 61 - Aufsichts- und Durchsetzungsmaßnahmen
- § 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, sofern diese nicht in Mindeststandards des BSI geregelt sind. Offenbar können Einrichtungen der Bundesverwaltung Cybersicherheit Kraft Magie realisieren. Dieser Ausschluss erzeugt starkes Kopfschütteln und lässt uns mit Verwunderung und Fassungslosigkeit zurück.

§ 29 (2) sollte daher wie folgt angepasst werden:

„Für Einrichtungen der Bundesverwaltung sind die Regelungen für besonders wichtige Einrichtungen anzuwenden, nicht jedoch die Regelungen der §§ 38, 40 Absatz 3 und der §§ 61 und 65. ~~**Für Einrichtungen der Bundesverwaltung, ausgenommen das Bundeskanzleramt und die Bundesministerien, sind zusätzlich die Regelungen des § 30 nicht anzuwenden.**~~“

Mit dem Ausschluss des § 38 werden "Geschäftsleitungen" der Bundesverwaltung von den mit der NIS2-Regulierung eingeführten Billigungs-, Überwachungs- und Schulungspflicht von Ihrer Verantwortung befreit. Zwar weist ihnen § 43 dann entsprechende Pflichten zu, ohne jedoch auch eine dem § 38 (2) entsprechende

Haftungsregelung vorzusehen. Das ist für die AG KRITIS nicht nachvollziehbar. **Denn ohne drohende negative Konsequenzen ist der Handlungsdruck bei den agierenden Personen begrenzt.**

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 bereits betroffenen Auswärtigen Amt oder sogar in Bundeskanzlerin Merkels Rechner** (zu dem es sogar einen Podcast[4] investigativer Recherche gab).

Es fällt auf, dass in dem vorliegenden Gesetzesentwurf die Durchsetzungsbefugnisse aus § 61 nicht gegenüber den Stellen des Bundes gelten sollen. Zwar werden etwa in Bezug auf Kontrollen und Prüfungen ähnliche Regelungen in § 7 eingeführt. Diese ermöglichen dem BSI auch, Audits und Prüfungen durchzuführen und daraus Maßnahmen und Anweisungen abzuleiten. Sowohl in Bezug auf die Stellen des Bundes als auch auf die übrigen wichtigen und besonders wichtigen Einrichtungen wird die Wirksamkeit der Regelungen aber von der tatsächlichen Prüf- bzw. Kontrolldichte abhängen. Bereits jetzt ist absehbar, dass das BSI nicht ausreichend Ressourcen für alle Aufsichtsaufgaben erhalten wird. Daher sollte im Gesetz zumindest klargestellt werden, dass regelmäßige Kontrollen der genannten Einrichtungen nicht nur zu den Befugnissen des BSI gehören, sondern zu den Pflichtaufgaben.

Es sollte daher ein neuer § 3 (4) ergänzt werden:

„Das Bundesamt prüft regelmäßig, ob wichtige und besonders wichtige Einrichtungen sowie Einrichtungen der Bundesverwaltung, die notwendigen Vorkehrungen zur Absicherung ihrer informationstechnischen Systeme, Komponenten und Prozesse ergriffen haben, um den Pflichten aus diesem Gesetz gerecht zu werden."

Um **sowohl gegenüber der Bevölkerung als auch gegenüber dem Parlament Klarheit** darüber zu verschaffen, wie das BSI seine dahingehende Kontrollaufgabe wahrnimmt, sollte es beide **regelmäßig darüber unterrichten**. Eine entsprechende Verpflichtung sollte in § 58 (2) ergänzt werden:

„Die Unterrichtung umfasst insbesondere die Zahl der Fälle, in denen das Bundesamt von seinen Prüf- und Kontrollbefugnissen nach § 7 und § 61 dieses Gesetzes Gebrauch gemacht hat."

Weiterhin werden mit § 29 (1) Nr. 2 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 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, einheitliche Lebens- und Sicherheitsstandards für öffentliche Dienstleistungen der Daseinsvorsorge zu gewährleisten.** Dies kann nur ohne Benachteiligung erfolgen, wenn diese länderübergreifend einheitlich definiert sind. 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

[4] https://www.br.de/mediathek/podcast/der-mann-in-merkels-rechner-jagd-auf-putins-hacker/853

Zuständigkeiten, Ebenen oder Schwellenwerten würde Bürgerinnen aus Sicht der AG KRITIS in unterschiedliche Versorgungsklassen einordnen, was in deutlichem Widerspruch zu Gleichheitsgebot und Daseinsvorsorge steht.

Sofern darüber hinaus die Einrichtungen der Bundesverwaltung in § 43 (4) Satz 2 erst nach fünf(!) 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 sehr stark verzögert.

Ausnahmen als Regelfall

In § 37 Ausnahmebescheid wird ein Großteil der Funktionsfähigkeit eines souveränen Staates ausgeklammert. **Das BMI, das Bundeskanzleramt, das BMJ, das BMV, 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 weitern 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 bereits im Jahre ~~**2024**~~ **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[5] fest:

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

Offensichtlich belegen diese Zahlen, dass die deutsche Wirtschaft nicht in ihrer Selbstverantwortung Willens ist, die Versorgungssicherheit der Bevölkerung zu gewährleisten.

Sowohl in der Definition eines Sicherheitsvorfalls nach § 2 Nr. 40, als auch bei der Definition von Risikomanagementmaßnahmen nach § 30 (1) wurde die Authentizität als Schutzziel entfernt. Ebenso wurde sie in den Schutzzielen des § 2 Nr. 23 für kritische Komponenten / IKT-Produkte gestrichen. Dies unterscheidet sich von vorherigen 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. Die Klarstellung in der Begründung Teil B zu § 2 Nr. 1, die in der NIS-2 erwähnte Authentizität sei im deutschen Recht ein Unterfall der Integrität, adressiert die fachlich richtige und relevante Unterscheidung unzureichend. Eine Verletzung des Schutzziels Authentizität kann selbstverständlich auch zu erheblichen Folgen führen, sowohl bei der IT-basierten Kommunikation von Menschen untereinander, aber insbesondere auch bei der technischen Kommunikation von Kritischen Infrastrukturen. Daher sehen wir es als gegeben an, dieses Schutzziel weiterhin explizit aufzuführen.

Sowohl für BWE als auch für WE sollen in §§ 61-62 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 § 63 (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.

Systeme zur Angriffserkennung

Bedauerlich ist, dass § 58 (2) wie die Vorgängerregelung im derzeit geltenden BSIG § 8a weiterhin eine Pflicht für den Einsatz von Systemen zur Angriffserkennung vorsieht. Dagegen hatte sich die AG KRITIS bereits im Rahmen der Ausschussanhörung zum zweiten IT-Sicherheitsgesetz ausgesprochen[6].

Es ist **aus Sicht des Risikomanagements als auch aus technischer Sicht unsinnig**, bestimmte Einzelmaßnahmen wie Systeme zur Angriffserkennung explizit im Gesetz zu nennen. Denn welche konkreten Maßnahmen zur Absicherung in welcher Risikopriorisierung ergriffen werden müssen, ergibt sich aus einer Risikoanalyse im Rahmen des ISMS mit BCM nach § 30 (Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen).

Wenn den Maßnahmen zur Angriffserkennung durch die explizite Nennung im Gesetzestext entsprechende Priorität einzuräumen ist, fehlen die dafür aufzuwendenden Ressourcen im Zweifel bei den Maßnahmen, die nach

[5] https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2024
[6] https://ag.kritis.info/2021/03/01/stellungnahme-zum-it-sicherheitsgesetz-2-0-im-innenausschuss-des-bundestags/

der Risikoanalyse in der Priorität wichtiger und dringend nötiger sind, z.B. eine angemessen abgesicherte Fernwartung nach dem Stand der Technik.

Bei dem durch die EU an Russland attribuierten Angriff[7] gegen das Viasat Satellitennetzwerk KA-SAT beispielweise „a ground-based network intrusion by an attacker exploiting a misconfiguration in a VPN appliance to gain remote access to the trusted management segment of the KA-SAT network“[8] oder wie sie im Fall eines Wasserwerks in Texas[9] ebenfalls unzureichend vorhanden war.

Auch in Deutschland sind aktuell solche Szenarien im Betrieb via Fernwartung weiterhin Alltag. Dort wo sie nach einer Risikoanalyse als notwendige Maßnahme identifiziert werden, zählen Angriffserkennungssysteme auch schon seit dem IT-Sicherheitsgesetz von 2015 zu den technischen Maßnahmen, die nach § 8a (1) BSIG umzusetzen waren. In der Gesetzesbegründung zum IT-Sicherheitsgesetz 2015 werden solche Detektionsmaßnahmen explizit als Teil der Absicherungspflichten nach § 8a (1) BSIG genannt[10]. Um eine wirklich risikoadäquate Absicherung zu ermöglichen, sollte die Verpflichtung auf die Einzelmaßnahme der Angriffserkennungssysteme in § 31(2) gestrichen werden.

Mangelhafte Unabhängigkeit des BSI

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 § 58 an das BMI hinaus gehen.

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.

Darüber hinaus empfiehlt die AG KRITIS dringend, § 44 (1) Satz 1 wie folgt anzupassen, um Cybersicherheit in der Bundesverwaltung aufrichtig und dauerhaft zu etablieren:

„Die Einrichtungen der Bundesverwaltung müssen die ~~**jeweils geltenden Fassungen der**~~ Mindeststandards für die Sicherheit in der Informationstechnik des Bundes (Mindeststandards)**, die BSI-Standards und das IT-Grundschutz-Kompendium des Bundesamtes (IT-Grundschutz) in den jeweils geltenden Fassungen** als Mindestanforderungen zum Schutz der in der Bundesverwaltung verarbeiteten Informationen erfüllen.“

[7] https://www.consilium.europa.eu/de/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/
[8] https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview
[9] https://www.lebensraumwasser.com/hackerangriff-auf-wasserwerk-in-den-usa/
[10] BT-Drucksache 18/4096, Seite 25.

§ 44 (2) Satz 1 und 2 sind des Weiteren wie folgt anzupassen:

„~~**Das Bundeskanzleramt und die Bundesministerien müssen als zusätzliche Mindestanforderungen dD**~~ie BSI-Standards und das IT-Grundschutz-Kompendium des Bundesamtes (IT-Grundschutz) werden in den jeweils geltenden Fassungen ~~**einhalten. Die jeweils geltenden Fassungen werden**~~ auf der Internetseite des Bundesamtes veröffentlicht.“

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.

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.

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 (ja, ein NDA reicht) unterbleiben. Es muss aber zum Jahresende eine Statistik über die so unterdrückten Meldungen an das BSI übermittelt werden. 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)“ vom 17.09.2024 vollständig an. Die darin aufgeführten **Empfehlungen sollten dringend allesamt realisiert werden**!

Schwachstellenmanagement

Im Rahmen der *AG BSI* hat unser Gründer und Sprecher Manuel ‚HonkHase' Atug bereits dargelegt, dass Schwachstellen nicht verwaltet, sondern geschlossen werden müssen.

Das Gesetz sollte daher klarstellen, dass dem BSI gemeldete Informationen ausschließlich für den Schutz der IT-Sicherheit verwendet werden dürfen und der **Einsatz oder die Verwendung von Schwachstellen für offensive oder invasive Zwecke nicht zulässig** ist. Um ein hohes Maß an IT-Sicherheit erreichen zu können, sind alle Sicherheitsbehörden wie z. B. BND, BKA, Bundespolizei, Verfassungsschutz, ZITiS und die Bundeswehr zu verpflichten, von ihnen gefundene oder erworbene Schwachstellen ausnahmslos an das BSI zu melden.

Es braucht diese ausnahmslose Meldepflicht entdeckter Sicherheitslücken, die für alle staatlichen Stellen gelten muss. Ohne ein solch klares Bekenntnis des Gesetzgebers - auch zur Rolle des BSI hin - droht ansonsten ein schwerwiegender Vertrauensverlust bei den relevanten Akteuren aus der Wissenschaft, Wirtschaft, Zivilgesellschaft und den Sicherheitsforscherende.

Zum Thema „Zurückhalten von Schwachstellen" hatte sich die AG KRITIS bereits im Rahmen der Ausschussanhörung zum zweiten IT-Sicherheitsgesetz hinreichend ausgesprochen[11].

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.

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 scheint, als sei weiterhin keine vollständige Harmonisierung der Regelungen zwischen den beiden Gesetzesvorlagen erfolgt - was aktuell aufgrund der mangelnden Transparenz nicht überprüfbar ist. **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.

[11] https://ag.kritis.info/2021/03/01/stellungnahme-zum-it-sicherheitsgesetz-2-0-im-innenausschuss-des-bundestags/

Abgeordnete haben im Rahmen der 1. Lesung zum NIS2UmsuCG im Bundestag auf Cyberdurchfall hingewiesen.

Der Bundesrechnungshof stellt fest: „Wichtige Regelungen sollen nicht für die gesamte Bundesverwaltung in einheitlicher Weise verbindlich sein. Die Folge wäre ein **„Flickenteppich“**, der die Informations- und Cybersicherheit aller Beteiligten gefährden kann.“

Manuel ‚HonkHase‘ Atug, Gründer und Sprecher der unabhängigen AG KRITIS sagt dazu: „Wir brauchen dringend eine **strikt defensive Cybersicherheitsstrategie**, statt dem immer wieder vorgelegten und großflächig zerfaserten Cyberdiarrhö an Lücken, Ausnahmen und offensiven Optionen. Eine Cybernation Deutschland darüber hinaus kann nur umgesetzt werden, wenn das Cyber-Wimmelbild der Verantwortungsdiffusion bereinigt und konsolidiert wird“.