UP KRITIS

Positionspapier zum „Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“ des Bundesministeriums des Innern vom 23.06.2025

Die Wirtschaftsvertreter des UP KRITIS begrüßen die Möglichkeit an der Verbändeanhörung am 04.07.2025 teilnehmen zu dürfen und eine Stellungnahme zum Gesetzesentwurf einreichen zu können ausdrücklich. Die Wirtschaftsvertreter hätten sich eine längere Bearbeitungsfrist gewünscht, da die sektorübergreifende Koordination zur Erstellung einer angemessenen Stellungnahme in den zur Verfügung stehenden 7 Werktagen kaum umsetzbar ist.

Nach wie vor begrüßen die Wirtschaftsvertreter des UP KRITIS die Erweiterung des Nachweiszyklus für Betreiber kritischer Anlagen auf drei Jahre als einen wichtigen Schritt in Richtung Internationalisierung des nationalen Cybersicherheitsrecht entlang der einschlägigen europäischen und internationalen Normen im Bereich der Informationssicherheit. Der vorliegende Referentenentwurf trägt dieser Entwicklung - etwa in § 30 NIS2UmsuCG - grundsätzlich Rechnung. Deshalb sollte die Internationalisierung auch andere wesentliche Regelungsinhalte des NIS2UmsuCG erfassen und nationale Alleingänge etwa bei der Einführung von abweichenden Schutzzielen oder bei der Neuregelung der Prüfung von Konformitätsbewertungsprogrammen vermieden werden. Nationale Alleingänge bei der Umsetzung europäischer Vorgaben können in Zukunft aufgrund steigender Harmonisierungsanforderungen im Unionsgebiet einen aufwändigen Rückbau nationaler Alleingänge erforderlich machen. Nicht zuletzt hat die Vergangenheit gezeigt, dass nationale Alleingänge wie beim IT-Grundschutz oder bei der Smart-Meter-Gateway-Infrastruktur keinen „Leuchtturm-Charakter“ mit Nachahmungswirkung im Unionsgebiet entfalten konnten.

Ebenfalls begrüßen wir, dass besonders wichtige Unternehmen weiterhin nur auf Anforderung des BSI einen Nachweis der Erfüllung der Anforderungen erbringen müssen, hierbei sollte darauf geachtet werden, dass diese Abfrage für ein Unternehmen nicht häufiger erfolgt als bei den Betreibern kritischer Anlagen (neuer 3 Jahres Rhythmus). Des Weiteren sollten angemessene Fristen zur Erstellung eines solchen Nachweises festgelegt werden.

Darüber hinaus plädieren wir dafür, die Regelungen der NIS2-Richtlinie möglichst ohne wesentliche Verschärfungen bzw. Erweiterungen in deutsches Recht zu übernehmen und nur die rechts-systematisch notwendigen Anpassungen vorzunehmen.

Positionen des TAK Regulierung im Überblick

1. NIS2UmsuCG und die noch ausstehende nationale Umsetzung der CER-Richtlinie sollten stärker miteinander abgestimmt, wesentliche Regelungsinhalte im Sinne des All-Gefahren-Ansatzes harmonisiert und beide Gesetze gleichzeitig in den Bundestag eingebracht werden.

2. Kritische Infrastrukturen im öffentlichen Raum sollten stärker in den Fokus der Sicherheitsbehörden bei der Ausübung von deren hoheitlicher Tätigkeit genommen werden und ggfs. die technischen, organisatorischen und personalwirtschaftlichen Voraussetzungen – bei den Sicherheitsbehörden – hierfür weiter ertüchtigt werden. Damit können die Sicherheitsbehörden die Unternehmen praktisch unterstützen.

3. Das angedachte nationale Prüfverfahren nach § 41 NIS2UmsuCG zur Untersagung zum Einsatz kritischer Komponenten mit einzelnen Prüfungen ist mit den vorgesehenen Prüffristen (bis zu vier Monate) nicht praktikabel. Außerdem erscheint eine EU-weite Abstimmung gegenüber einer nationalen Prüfung sinnvoller.

   Die ebenfalls vorgesehenen rückwirkenden Verbote (§ 41 Abs. 4 und 6), die ggf. den Ausbau von Komponenten zur Folge haben können, bergen aus Sicht des UP KRITIS mehr Risiken als Sicherheitsgewinne.

   Zudem ist im Gesetzestext nicht klar geregelt, wie eine Kostenträgerschaft für entstehende Rückabwicklungsaufwände im Falle der Untersagung geregelt wäre. Gleichzeitig können rückwirkende Verbote im Widerspruch zu anderen europäischen Regelungen wie dem Vergaberecht stehen.

4. Die Verpflichtung zur Nutzung von zertifizierten Komponenten und Prozessen nach § 30 Abs. 2 Nr. 6 und die Möglichkeit zum Erlass nationaler technischer Spezifizierungen § 30 Abs. 2 Nr. 5 dürfen nicht zu Beschaffungsengpässen und zur Bildung von Oligopolen führen.

5. Im Sinne einer adäquaten Begriffsbestimmung im § 2 Nr. 11a sollten „finanzielle Verluste“ durch „erhebliche finanzielle Verluste“ (aus Unternehmenssicht KonTraG) ersetzt werden. Ebenso sollten hier immaterielle Schäden explizit ausgeschlossen werden.

6. § 39 Abs. 3 BSIG-E regelt ausschließlich die Zeitpunkte für die nächstfolgende Prüfung. Eine Regelung für Betreiber kritischer Infrastrukturen, die eine Prüfung bereits geplant und beauftragt haben oder sich zum Zeitpunkt der Inkraftsetzung gerade in einer Prüfung befinden, fehlt im aktuellen Referentenentwurf und schafft somit Rechtsunsicherheit und möglicherweise erhebliche Aufwände für betroffene Unternehmen.

7. Die Aussage der „Vernachlässigbarkeit“ in §28 Abs. 3 und die Aussagen in § 30 Abs. 1 zur „Erbringung ihrer Dienste“ und der „Verhältnismäßigkeit“ sollten konkretisiert werden, da beide Punkte in der aktuellen Formulierung Rechtsunsicherheiten schaffen können.

8. Die in § 39 Abs. 2 beschriebene Ermächtigung des BSI zur Ausgestaltung des Verfahrens von Prüfungen und der Erbringung von Nachweisen für Betreiber kritischer Anlagen, darf nicht dazu führen, dass international anerkannte Normen und Verfahren sowie auch national etablierte Prüfverfahren nach dem Stand der Technik nicht mehr möglich sind oder es zu ungerechtfertigten Herabstufungen von Prüfergebnissen kommt.

9. Klärungen zum Weiterbetrieb und Haftung bei Eingriff in die Geschäftsführung durch das BSI nach § 61 Abs. 9: Gegenwärtig ist nicht geregelt, wer den Betrieb leiten soll und für Schäden haftet, die im Zusammenhang mit diesem Eingriff durch das BSI entstehen. Sofern diesbezüglich keine Klärung im Gesetz erfolgt, sollte der Regelungsinhalt ganz entfallen.

10. Integration des Schutzziels Authentizität im international etablierten Schutzziel Integrität, um nicht von internationalen Standards abzuweichen. Das Schutzziel sollte im gesamten Gesetzestext konsequent gleichbehandelt werden.

11. Registrierungspflichten nach §§ 33 und 34 unklar und nicht übereinstimmend mit Artikel 26 NIS2-Richtlinie. Hier werden eindeutige Vorgaben für die Wirtschaft benötigt.

Detailhinweise

Zu Punk 1: Größtmögliche Harmonisierung NIS2UmsuCG und nationalen Umsetzung der CER-Richtlinie:
Die kohärente Umsetzung der CER-Richtlinie und der NIS2-Richtlinie verlangt eine größtmögliche Harmonisierung und Verzahnung von NIS2UmsuCG und der nationalen CER-Umsetzung. Diese Verzahnung sollte bei einer einheitlichen Begriffsbestimmung (z.B. kritische Anlagen) beginnen und mit der engen Abstimmung der Regelungsinhalte (insbesondere gemeinsame Nachweispflichten) fortfahren. Nur so können Doppelaufwendungen vermieden werden und eine Cyberraum und physischen Raum integrierende Sicherheit im Sinne des All-Gefahren-Ansatzes realisiert werden.

Die zu erlassende Rechtsverordnung sollte im Sinne einer größtmöglichen Harmonisierung zwischen NIS2UmsuCG und der nationalen CER-Richtlinienumsetzung auf den Sektorstudien des BSI und der BSI-KritisV aufbauen und die dort erarbeiteten sowie bewährten Methoden zur Bestimmung von Schwellenwerten kritischer Anlagen übernehmen. Die Konkretisierung des Begriffs kritische Anlage sollte sektorspezifisch in enger Abstimmung mit der zuständigen Regulierungsbehörde erfolgen.

Die Erfahrung mit der Erarbeitung und Umsetzung der BSI-KritisV haben darüber hinaus gezeigt, dass eine frühzeitige und umfassende Einbindung der Branchen und ihrer Verbände sinnvoll ist. Schließlich sollten NIS2UmsuCG und die nationale Umsetzung der CER-Richtlinie im Sinne einer größtmöglichen Harmonisierung auch gleichzeitig im Bundestag eingebracht werden.

Nur bei einer zeitgleichen Einbringung der beiden angesprochenen Gesetzesvorhaben hat nach unserer Auffassung das Parlament überhaupt erst eine Möglichkeit, die gegenseitigen Auswirkungen und Ziele effektiv zu erfassen und zu bewerten. Gleiches gilt für die betroffenen Betreiber bzw. Einrichtungen.

Zu Punkt 2: Drohende „Resilienz-Lücke“ nach All-Gefahren-Ansatz gefährdet Wirtschaftlichkeit und rechtskonforme Umsetzung von Anforderungen für Betreiber kritischer Anlagen:
Der Mitigation terroristischer oder (para-)militärischer Bedrohungen können die Betreiber kritischer Infrastrukturen ohne Unterstützung durch den Bund oder die Länder nicht nachkommen. Weder dürfen sie den hoheitlichen, bei den Ländern liegenden Auftrag der Gefahrenabwehr (im Cyberraum oder im physischen Raum) erfüllen noch können Sie dieses wirtschaftlich abbilden.

Um dieser drohenden „Resilienz-Lücke“ zu begegnen, muss der Bund ausreichende Mittel für Landes- und Bundesbehörden zur Unterstützung der Betreiber kritischer Infrastrukturen bereitstellen sowie eine erweiterte Zuständigkeit (etwa der Bundespolizei) beim Schutz kritischer Infrastrukturen in Erwägung ziehen. Nicht zuletzt deshalb haben die dem NIS2UmsuCG und der erwarteten nationalen Umsetzung der CER-Richtlinien zugrundliegenden EU-Richtlinien auch die ausreichende finanzielle, materielle und personelle Unterstützung der Betreiber kritischer Anlagen durch die Mitgliedsstaaten vorgesehen.

Zu Punk 3: Anpassung des Prüfprozesses bei kritischen Komponenten in § 41 NIS2UmsuCG und ein gemeinsames Verfahren für NIS2UmsuCG und der nationalen Umsetzung der CER-Richtlinie:
Das bisherige Verfahren des § 9b BSIG hat sich weder im Telekommunikationssektor noch im Sektor Energie als geeignetes Mittel bewährt, um die technologische Abhängigkeit bei Schlüsseltechnologien bzw. kritischen IT-Komponenten spürbar und nachhaltig zu verringern. Der UP KRITIS fürchtet daher, dass dieses gegenwärtige, ungeeignete Prüfverfahren zur Untersagung des Einsatzes von kritischen Komponenten nun auch für die kritischen Komponenten im Sinne des neuen § 41 NIS2UmsuCG und der nationalen Umsetzung der CER-Richtlinie zum Einsatz kommen wird.

Der UP KRITIS empfiehlt daher, dass in § 41 angedachte Verfahren durch EU-weit abgestimmte Blacklist(s) von Herstellern/Produkten/Technologien zu ergänzen. Dieses würde die Beschaffungsprozesse innerhalb der Unternehmen beschleunigen und weniger Verwaltungsaufwand seitens der Behörden erfordern.

Bezüglich der rückwirkenden Untersagung des Einsatzes kritischer Komponenten sollte eine Formulierung gefunden werden, die einen Austausch außerhalb des normalen Lebenszyklus einer Komponente nur dann vorsieht, wenn durch zusätzliche Mitigations-Maßnahmen das Risiko nicht auf ein akzeptables Maß gesenkt werden kann.

Mögliche hieraus entstehende Rückabwicklungsaufwände im Falle der Untersagung sind im Gesetzestext nicht klar geregelt. Der UP KRITIS empfiehlt eine Kostenübernahme durch den Bund, mindestens jedoch eine klare gesetzliche Regelung.

Ebenfalls fordert der UP KRITIS die Klärung und ggf. die Auflösung der möglichen Widersprüche zu anderen europäischen Regelungen wie z. B. dem Vergaberecht.

Weiterhin muss erwähnt werden, dass die grundsätzliche Untersagung des Einsatzes von Komponenten (bitte auch im Zusammenhang mit § 30 Nr. 5 und 6 sehen) zu einer Verknappung des Angebots (ggf. zu Oligopolen) führen kann und somit neue Cluster-Risiken entstehen können.

Zu Punkt 4: Zertifizierungspflichten von Komponenten und Prozessen dürfen nicht zu Beschaffungsengpässen und zur Bildung von Oligopolen führen:
Nach dem vorliegenden Entwurf zum NIS2UmsuCG sind die Folgen der Verpflichtungen zum Einsatz von zertifizierten Komponenten und Prozessen zur Abschätzung der Aufwendungen durch die Wirtschaft noch zu unbestimmt.

Die Erfahrungen etwa mit der Smart-Meter-Gateway-Infrastruktur haben darüber hinaus gezeigt, dass insbesondere nationale Zertifizierungsframeworks die zügige Einführung sicherer digitaler Infrastrukturen in den KRITIS-Sektoren im Wege stehen und die Bildung von Oligopolen begünstigen können. Diese Oligopole sind aus einer systemischen Sicherheitsperspektive selbst als Cluster-Risiken zu bewerten. Auch im Sinne der internationalen Wettbewerbsfähigkeit deutscher Hersteller sollte der Stand der Technik nicht durch Dokumente und technische Richtlinien einer Bundesbehörde festgelegt, sondern lediglich als Ergänzung zu öffentlich anerkannten Beschreibungen zum Stand der Technik aufgefasst werden.

Eine rein nationale Zertifizierung ist deshalb auch nicht im Sinne der NIS2-Richtlinie, da die NIS2-Richtlinie primär auf einen gemeinsamen europäischen Binnenmarkt ohne Zutrittsbarrieren für Unionsstaaten abzielt. Es kann nicht davon ausgegangen werden, dass Hersteller zwingend ein Interesse an den Aufwänden einer rein deutschen Zertifizierung haben. Zusätzlich ist der Einsatz von ausschließlich zertifizierten Komponenten für eine Aufrechterhaltung eines Regelbetriebes aufgrund Ersatzbeschaffung sehr problematisch und kann im worst-case zum Stillstand der KRITIS führen.

Zu Punkt 5: Notwendige Begriffsbestimmung im § 2 Nr. 11 BSIG (erheblicher Sicherheitsvorfall):
Die Beschreibungen unter diesem Punkt sind missverständlich und können zu deutlichen Überinterpretationen führen. Eine konkretisierende Begriffsbestimmung sollte im Sinne der Klarheit nicht erst über eine Rechtsverordnung entsprechend § 56 Abs. 5 erfolgen, sondern bereits im Gesetzestext klar ausformuliert werden.

Der Wortlaut unter Punkt 11 a) kann so verstanden werden, dass jeder nur mögliche finanzielle Verlust, ganz gleich wie groß er ist, zu einem erheblichen Sicherheitsvorfall führt. Da jeder Sicherheitsvorfall allein durch die Behebung zu einem finanziellen Verlust führt, wäre somit diese Regelung uferlos und unverhältnismäßig. Verstärkt wird dies dadurch, dass nach dem Wortlaut der finanzielle Verlust gar nicht eingetreten sein muss, sondern allein die Möglichkeit des Eintritts ausreicht.

Der UP KRITIS schlägt deshalb vor, „finanziellen Verluste“ im Minimum durch „erhebliche finanzielle Verluste (angemessen aus Unternehmenssicht nach KonTraG)“ in der Beschreibung zu ersetzen.

Grundsätzlich sollte im Hinblick auf die hiermit verbundenen Pflichten stärker nach Art des Sicherheitsvorfalls ausdifferenziert werden, um eine Fehlallokation von Ressourcen zu vermeiden. Beispiel: Im Falle von (z. B. verhinderten oder unwirksamen) DDoS-Attacken wäre nicht von einem „schwerwiegenden Sicherheitsvorfall“ zu sprechen, auch wenn ein beliebiger finanzieller Verlust (durch Aufwand) entstanden ist und es wäre nach Auffassung des UP KRITIS ausreichend, lediglich über den Angriff, dessen Reichweite und Zeitpunkt zu melden, um ein etwaiges nationales Sicherheitsbild durch das BSI zu erstellen und wiederum eine Information durch das BSI an die (betroffenen) Unternehmen bzw. Betreibern kritischer Anlagen sicherzustellen.

Der Wortlaut unter Punkt 11 b) kann so ausgelegt werden, dass auch jeder Datenschutzvorfall mit erheblichen Schäden (Anwendung der Begriffe siehe allgemein gültige Beschreibungen zum Datenschutz nach DSGVO) zusätzlich als „erheblicher Sicherheitsvorfall“ betrachtet werden und an das BSI gemeldet werden müsste. Damit würde eine Doppelbehandlung eines Vorfalls mit entsprechendem Mehraufwand für das Unternehmen erfolgen. Insbesondere ergeben sich in solchen Fällen Mehraufwendungen, da die zeitliche Meldefrist bei Datenschutzvorfällen mit 72h benannt ist (DSGVO) und die für Sicherheitsvorfälle auf 24h begrenzt ist (NIS2-Richtlinie). Hier sollte deutlicher abgegrenzt werden, wann Punkt 11.b) wirklich greifen soll.

Zusätzlich empfiehlt der UP KRITIS die Überschrift des Punktes 11 wie folgt zu ändern:
„**… „erheblicher Sicherheitsvorfall“ ein Sicherheitsvorfall (siehe Punkt 40) der, …**“

Zu Punkt 6: Übergangsfristen in § 39 BSIG-E für Betreiber kritischer Infrastrukturen, die sich in einer KRITIS-Prüfung nach § 8a Abs. 3 BSIG befinden oder diesen bereits beauftragt haben:
Aufgrund der sehr umfangreichen KRITIS-Prüfungen nach §8a Abs. 3 BSIG (inklusive Planung, Beauftragung, Vorbereitung, Durchführung und Berichtserstellung ist mit bis zu 12 Monaten zu rechnen) müssen die Prüfungen frühzeitig geplant und beauftragt werden. Somit wird es vorkommen, dass einige Betreiber sich bei Inkrafttreten der neuen Regelungen nach § 39 BSIG-E noch in einer laufenden Prüfung nach § 8a BSIG befinden oder diese Prüfung kurz danach beginnen wird.

Aufgrund fehlender Regelungen im aktuellen Entwurf besteht für diese Unternehmen die Gefahr, dass nach Abschluss der Prüfung die Ergebnisse nicht anerkannt werden und hierdurch eine weitere Prüfung direkt im Jahr darauf erforderlich ist.

Generell sollten Nachweise aus bereits laufenden oder beauftragten KRITIS-Prüfungen auch nach Inkrafttreten des BSIG-E anerkannt werden.

Der UP KRITIS schlägt daher vor, die folgende Regelung im Gesetzestext mit aufzunehmen:

„Betreiber kritischer Anlagen, die bis zum Inkrafttreten dieses Gesetzes Betreiber Kritischer Infrastrukturen waren, und deren Nachweisfrist nach § 8a Abs. 3 BSI-Gesetzes vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 12 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982) geändert worden ist, innerhalb von zwölf Monaten nach Inkrafttreten abgelaufen wäre, können in diesem Zeitraum einen Nachweis nach den bisher geltenden Vorgaben erbringen."

Zu Punkt 7: Die Aussage der „Vernachlässigbarkeit" in §28 Abs. 3 und die Aussage in § 30 Abs. 1 zur „Erbringung ihrer Dienste" und der „Verhältnismäßigkeit" sollten konkretisiert werden, da beide Punkte in der aktuellen Formulierung Rechtsunsicherheiten schaffen könnten:
Der Begriff „Vernachlässigbar" in Verbindung mit der gesamten Geschäftstätigkeit ist zu ungenau und kann sich zwischen Unternehmen der gleichen Branche unterscheiden. Der UP KRITIS schlägt daher vor, den Absatz 3 § 28 wie folgt zu ändern.

*„Bei der Zuordnung zu einer der Einrichtungsarten nach den Anlagen 1 und 2 können solche Geschäftstätigkeiten unberücksichtigt bleiben, die im Hinblick auf **die genannten Einrichtungsarten und damit für die Erbringung der kritischen Dienstleistungen** der Einrichtung **nicht notwendig** sind."*

Die NIS2-Richtlinie führt in ihren Erwägungsgründen unter „Punkt 1" den folgenden Inhalt an:
„Ziel der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates(4) war der unionsweite Aufbau von Cybersicherheitskapazitäten, die Eindämmung von Bedrohungen für Netz- und Informationssysteme, die zur Erbringung wesentlicher Dienste in Schlüsselsektoren verwendet werden, und die Sicherstellung der Kontinuität solcher Dienste bei Vorfällen, um so zur Sicherheit der Union und zum reibungslosen Funktionieren ihrer Wirtschaft und Gesellschaft beizutragen."

Nach dem Verständnis des UP KRITIS wird dieses Ziel mit der offenen Formulierung *„… die sie für die Erbringung ihrer Dienste nutzen …"* in dem vorliegenden Entwurf in § 30 Abs. 1 zu weit gefasst.
Zudem führt der Begriff der „Verhältnismäßigkeit" in Bezug auf die Umsetzung von Schutzmaßnahmen vor allem bei den wichtigen Einrichtungen zu Rechtsunsicherheit, da keine weiteren Angaben zum umzusetzenden Schutzniveau gemacht werden.

Aus diesen Gründen schlägt der UP KRITIS vor, den Absatz wie folgt zu ändern:

„Besonders wichtige Einrichtungen und wichtige Einrichtungen sind verpflichtet, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die sie für die Erbringung ihrer Dienste im Rahmen der kritischen Dienstleistung entsprechend der Einrichtungsarten nach den Anlagen 1 und 2 nutzen. Dabei soll der Stand der Technik eingehalten werden. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht."

Zu Punkt 8: Konformitätsbewertung nach § 39 Abs. 2:
Die Ausgestaltung des Prüfverfahrens darf nicht dazu führen, dass die hier formulierten Anforderungen, über denen von anerkannten Normen und Verfahren hinausgehen oder zu Verzerrungen der Prüfergebnisse führen. Schon in der jetzigen Praxis kommt es durch die Ausgestaltung des Prüfverfahrens (RUN, Gain) durch das BSI im Rahmen der derzeitigen gültigen Reifegradbewertung zu pauschalen Herabstufungen der Prüfungsergebnisse, ohne dass dies auf Basis einer durchgängigen Herleitung aus der Mängelliste erfolgt. Zwar ist eine Harmonisierung des Prüfungsvorgehens anzustreben, allerdings nicht mit der Folge von erhöhten nationalen Anforderungen oder der pauschalen Herabstufung von Prüfergebnissen. Die Anwendung von § 39 Abs. 2 ist daher zu überprüfen.

Zu Punkt 9: Haftung bei Geschäftsführung durch das BSI nach § 61 Abs. 9:
Kritische Infrastrukturen sind ein wesentlicher Teil der Daseinsvorsorge. Insoweit hat ein Entzug der Berechtigung oder eine Untersagung der Ausübung der Geschäftsführung weitreichende Konsequenzen. Die Übernahme der daraus entstehenden Risiken ist im aktuellen Gesetzestext nicht geregelt. Daher empfiehlt der UP KRITIS die ersatzlose Streichung des kompletten Absatzes.

Zu Punkt 10: Integration des Schutzziels Authentizität im international etablierten Schutzziel Integrität, um nicht von internationalen Normen abzuweichen:
Aus sachlicher Sicht ließen sich die wesentlichen Aspekte des Schutzziels Authentizität im Schutzziel Integrität identifizieren, das in der ISO/IEC 27001 etabliert ist. Dieser Ansatz ist zu großen Teilen im vorliegenden Entwurf beachtet worden, allerdings noch nicht konsequent durchgezogen worden. Wir empfehlen die konsequente Streichung des Begriffes Authentizität und die Aufnahme der Inhalte unter dem Stichwort „Integrität".

Zu Punkt 12: Registrierungspflichten nach §33 und §34 unklar und nicht übereinstimmend mit Artikel 26 NIS2-Richtlinie:
(§ 33 Abs. 1 Nr. 4) -- Auflistung der Mitgliedsstaaten der EU, in denen die Dienste erbracht werden.

Hier ist zum einen fraglich, ob hier der Sitz der Kunden in den Mitgliedsstaaten gemeint ist oder tatsächlich der Dienst. Oftmals wissen wir als Lieferant nicht, wo der Kunde den Dienst nutzt.

Ferner kann sich die Auflistung täglich ändern, da in einem Konzern täglich neue Kunden aus der EU hinzukommen und die Registrierung müsste somit regelmäßig überprüft werden. Andernfalls käme nur eine Auflistung aller Mitgliedsstaaten in Betracht, um im Zweifel hier keinen Fehler zu machen.

Ferner halten wir in diesem Zusammenhang die Drei-Monatsfrist für zu knapp bemessen. Hier würde der UP KRITIS für eine sechsmonatige Frist plädieren.

IP-Adress-Ranges sind ggfls. nicht immer konstant und machen bei der Registrierung wenig Sinn

(§ 34 Abs. 1 Nr. 3) – Anschrift der Hauptniederlassung
Die Definition der Hauptniederlassung und die Auswirkung auf die Tochtergesellschaften in einem Konzernkonstrukt ist nach wie vor unklar. Die Verweise sind hier noch anzupassen. In Bezug auf die Hauptniederlassungsfrage für den IT-Betrieb sei vorweggenommen, dass hier noch einige Punkte unklar sind:

- Welcher Geschäftsführer haftet innerhalb eines Konzernkonstrukts? Der Geschäftsführer der Hauptniederlassung bei einem Fehler der Tochtergesellschaft oder der Geschäftsführer der Tochtergesellschaft?
- Welcher Stand der Technik ist verpflichtend umzusetzen und in welchen Mitgliedsstaaten?
- Wie sieht es aus, wenn die Anforderungen des Mitgliedsstaats der Hauptniederlassung höher (alternativ niedriger) sind als in dem Mitgliedsstaat der Tochtergesellschaft?
- Gilt die Nachweispflicht nur für den Mitgliedsstaat der Hauptniederlassung?