bitkom

Stellungnahme

März 2025

Anhörung gemäß § 8a Absatz 5 BSIG – Novellierung

Der Bitkom bedankt sich für die Möglichkeit, zur geplanten Aktualisierung der verbindlichen Anforderungen im Nachweisverfahren gemäß § 8a Abs. 5 BSIG Stellung zu nehmen. Wir begrüßen die Bestrebungen des BSI, die Aufwände für Betreiber und das BSI bei der Nachweiseinreichung zu reduzieren und gleichzeitig die Qualität der Nachweiserbringung weiter zu verbessern.

Im Rahmen der Anhörung wurden von unserer Mitgliedschaft einige allgemeine Anmerkungen zum Nachweisverfahren und den angekündigten Anpassungen in GAiN geäußert. Im Folgenden möchten wir daher sowohl diesen allgemeinen Punkten Raum geben als auch diejenigen hervorheben, die aus Sicht unserer Mitgliedschaft weiterhin berücksichtigt werden sollten.

Allgemeine Anmerkungen

Die Anpassungen an den Anforderungen N.BN.05, N.BN.06 und N.BN.08 führen zu gewissen Vereinfachungen, die jedoch insgesamt als eher marginal einzustufen sind. Die wesentliche Neuerung liegt in der Einführung von Kapitel 3.1, das bislang lediglich in der Orientierungshilfe zur Nachweiserbringung formulierte Vorgaben in eine rechtverbindliche Verordnung überführt. Auch wenn diese Inhalte keine grundlegend neuen Anforderungen darstellen, bedeutet ihre formale Verankerung eine wesentliche Veränderung mit potenziellen zusätzlichen rechtlichen Implikationen. Vor diesem Hintergrund wäre eine detailliertere Begründung der Änderungen wünschenswert, um deren tatsächliche Tragweite und Auswirkungen transparent darzustellen.

Ein weiteres strukturelles Problem ergibt sich aus der Integration der GAiN-Anforderungen in die bestehende Orientierungshilfe. Anstatt die Orientierungshilfe konsistent weiterzuentwickeln und an die neuen Anforderungen anzupassen, wurden die GAiN-Anforderungen 2023 zusätzlich aufgenommen. Dies erschwert es Betreibern, Prüfstellen und Auditoren, die jeweiligen Vorgaben systematisch nachzuvollziehen und deren Relevanz für die einzelnen Akteure klar zu erkennen. In der Praxis führt dies häufig zu Rückfragen des BSI an Betreiber, die an die Prüfstellen weitergeleitet werden müssen. Diese wiederum stimmen die Antworten in vielen Fällen mit den Auditoren

ab, was zu ineffizienten Kommunikationsprozessen führt und die praxisgerechte Umsetzung der Nachweispflichten erschwert. Die Einführung von RUN – Konkretisierte Reifegrade für KRITIS-Prüfungen ab dem 01. April 2025 – wird den ohnehin bereits komplexen Anforderungskatalog weiter ausweiten. Eine verbesserte Strukturierung und Konsolidierung der Vorgaben wäre daher erforderlich, um eine praktikable Umsetzung zu gewährleisten.

Darüber hinaus sind die Kostenstrukturen der Prüfverfahren ein zentraler Aspekt. Der finanzielle Aufwand hängt maßgeblich vom Prüfungsumfang und der Anzahl der veranschlagten Prüfungstage ab. Dies setzt Anreize, Prüfungen mit möglichst geringem Zeitaufwand durchzuführen, was im Widerspruch zu den erweiterten und gestiegenen Anforderungen des BSI steht. In einem solchen Rahmen können diese Anforderungen nicht in vollem Umfang erfüllt werden. Eine Definition des BSI zum Mindestumfang des Nachweisverfahrens wäre daher sinnvoll, um eine einheitliche und belastbare Prüfungsgrundlage sicherzustellen. In der Praxis zeigt sich, dass der angestrebte Reifegrad häufig auch nach längerer Zeit nicht erreicht wird. In besonders kritischen Fällen könnte es auch zielführend sein, eine direkte Beauftragung der Prüfstellen durch das BSI in Betracht zu ziehen – ähnlich den Regelungen zu Nachprüfungen gemäß § 8a Abs. 4 BSIG. Eine präzisere Definition des Prüfungsumfangs sowie eine objektive Ausgestaltung der Prüfverfahren würden wesentlich dazu beitragen, die Anforderungen an eine angemessene digitale Resilienz für Betreiber kritischer Infrastrukturen praxisgerecht und nachvollziehbar zu erfüllen.

Punkt 3.1
Allgemeine Anforderungen an die Nachweisprüfung

Gemäß D.PA.01 Fußnote 1 (Seite 6) wird das BSI RUN-Dokument einbezogen. Hierdurch werden neue Anforderungen in Bezug auf den Prüfzyklus generiert. In der Mapping-Tabelle zu RUN „Anhang: Mapping von Anforderungen aus der „Konkretisierung der KRITIS-Anforderungen (§ 8a Absatz 1 und Absatz 1a BSIG)“ auf die jeweiligen Umsetzungsgrade“ findet sich auf Seite 9 bei den organisatorischen Maßnahmen die Anforderung: Nr. 89: für den Umsetzungsgrad 4 werden mindestens jährliche Prüfungen durch z.B. unabhängige Dritte wie z.B. WPs. Vorgegeben. Eine solche jährliche Prüfung steht konträr zu der ursprünglich geplanten 3-jährigen Prüfung im NIS2UmsuCG.

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber

Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner

Felix Kuhlenkamp | Bereichsleiter Sicherheitspolitik
T 030 27576-279 | f.kuhlenkamp@bitkom.org

Verantwortliches Bitkom-Gremium

AK Informationssicherheit