bitkom

Stellungnahme

Juli 2024

Novellierung der Anforderungen gemäß § 8a Abs. 5 BSIG

Der Bitkom bedankt sich für die Möglichkeit zur Stellungnahme zur weiterentwickelten Version der verbindlichen Anforderungen im Nachweisverfahren gemäß § 8a Abs. 5 BSIG. Wir begrüßen die Bestrebungen des BSI, die Qualität der Nachweiserbringung in ausgewählten Themenbereichen weiter zu verbessern. Im Folgenden möchten wir die verschiedenen Punkte hervorheben, die aus Sicht unserer Mitgliedschaft noch berücksichtigt werden sollten.

Punkt 2.1
Unabhängigkeit der prüfenden Stelle und Prüfer

Unter den Punkten P.UP.01 und P.UP.02 wird gefordert, dass „die prüfende Stelle gegenüber dem Betreiber der zu prüfenden KRITIS-Anlage bzw. des zu prüfenden KRITIS-Anlagenteils unternehmensfremd [...] sein“ muss. Hier fehlt jedoch eine klare Definition des Begriffs „unternehmensfremd“. Ein unkundiger Leser könnte fälschlicherweise annehmen, dass die prüfende Stelle keine Expertise im zu prüfenden Bereich haben muss. Gemeint ist hier vermutlich, dass die prüfende Stelle nicht mit dem Unternehmen verbunden sein darf (ausgenommen Revisionen), jedoch fachkundig im Tätigkeitsbereich des Unternehmens sein sollte, wie es in D.4A.02 Absatz 1 beschrieben wird.

Des Weiteren begrüßen wir die Änderung des Prüfzyklus innerhalb der Leitung des Prüfteams von zwei auf drei Jahre, entsprechend P.UP.03.

Punkt 3.1
Prüfung nach dem 4-Augen-Prinzip

Die Anforderung 3.1. nach einer Prüfung nach dem Vier-Augen-Prinzip erscheint aus mehreren Gründen überzogen. Dies gilt, obwohl dies heute bereits bei einer KRITIS-Prüfung Anwendung findet.

Erstens verschärft die Anforderung das bereits bestehende Problem, fachkompetente Prüfer zu finden. Der Zertifizierungs- und Testierungsmarkt ist bereits stark durch neue gesetzliche Anforderungen nach objektiven Nachweisen belastet, wie beispielsweise durch DORA oder DigiG mit der C5-Forderung bei Cloud-Dienstleistern im Gesundheitswesen.

Zweitens ist die fachliche Notwendigkeit eines Vier-Augen-Prinzips nicht ersichtlich. Die festgelegten Anforderungen an die Prüfer in Bezug auf fachliche Kompetenzen und Unabhängigkeit gegenüber dem zu prüfenden Unternehmen sind genau dazu gedacht, ein unabhängiges und qualifiziertes Urteil abzugeben. Zwar kann das Vier-Augen-Prinzip die Qualität weiter erhöhen, jedoch sollten Aufwand (Kosten) und Nutzen (potenziell leicht verbesserte Qualität) gegeneinander abgewogen werden.

Drittens ist durch die Prüfung des Prüfberichts durch das BSI bereits ein zusätzliches Quality-Gate vorhanden. Bei Unstimmigkeiten kann das BSI eine Tiefenprüfung anordnen, die ebenfalls eine Qualitätssicherung des Ergebnisses darstellt.

Insgesamt erscheint die Anforderung als ein erheblicher Kostenfaktor für Unternehmen, der in seiner Wirkung das Ziel verfehlt. Wir setzen uns daher für eine ersatzlose Streichung der Anforderung ein.

Punkt 3.2
Dokumentation des Prüfergebnisses

Die Hinzunahme der Reifegradabstufung nach D.PE.13 für sämtliche kritischen Infrastrukturen innerhalb eines Konzerns, die im Scope sind, halten wir für überreguliert und nicht durch einen sachlich gerechtfertigten Mehraufwand begründet. Dieser Punkt sollte daher entfallen. Der Aufwand für eine Reifegradabstufung besteht bereits für die Systeme zur Angriffserkennung und sollte nicht weiter ausgeweitet werden.

Punkt 3.3
Dokumentation des Geltungsbereiches

Die Darstellung der Netzstrukturpläne nach N11 innerhalb eines großen Unternehmens, insbesondere mit Informationen darüber, an welchen Stellen die Netze getrennt oder separiert wurden, ist kaum umsetzbar und äußerst komplex. Wir empfehlen daher die Streichung dieser Anforderung.

Punkt 3.4
Verwendung von bestehenden Prüfungen und Zertifikaten

In N.BG.04 wird darauf verwiesen, dass Prüfungsergebnisse aus der 27001-Zertifizierung, die für die KRITIS-Prüfung berücksichtigt werden, nicht älter als 12 Monate sein sollen. Dabei ist zu beachten, dass im Rahmen der Zertifizierung sowohl Erst- bzw. Rezertifizierungsaudits als auch Überprüfungsaudits durchgeführt werden. Erstere beinhalten eine vollständige Prüfung, während letztere nur die weitere Wirksamkeit des Managementsystems überprüfen und dabei oft nur Teile des Geltungsbereichs auditieren. Als Alternative schlagen wir vor: „*Sollte ein natives ISO/IEC 27001-Zertifikat, ein ISO 27001-Zertifikat auf Basis von IT-Grundschutz, ein C5-Testat oder ein anderes Prüfzertifikat als Bestandteil eines Nachweises gemäß § 8a Absatz 3 BSIG verwendet werden, dürfen die Prüfer nur Prüfergebnisse aus den letzten 12 Monaten berücksichtigen.*“.
Durch die Veränderung des Prüfturnus im NIS2UmsuCG auf drei Jahre wird der KRITIS-Nachweis dann in der Regel immer nach dem Rezertifizierungsaudit erstellt werden.

Bei N.BG.05 gehen wir davon aus, dass die „relevanten Maßnahmen“ aus der Anwendbarkeitserklärung überprüft werden müssen (im Englischen: controls). Als Alternative schlagen wir zur Klarstellung vor: „*Sollte ein natives ISO/IEC 27001-Zertifikat, ein ISO 27001-Zertifikat auf Basis von IT-Grundschutz oder ein anderes Prüfzertifikat als Bestandteil eines Nachweises gemäß § 8a Absatz 3 BSIG verwendet werden, müssen die Prüfer die relevanten Maßnahmen zur Risikominimierung auf Wirksamkeit überprüfen.*“.

Punkt 3.5 & Punkt 3.6
Berücksichtigung alter Mängelliste(n) in Prüfung und Nachweis & Vorlagen für Bestandteile eines Nachweises nach § 8a Abs. 3 BSIG

In D.AM.04 und N.BN.07 (Anlage PE.A) sollte der Verweis auf die Nebenabweichungen des bestehenden ISO-Zertifikats ausreichend sein. Alles weitere führt aus unserer Sicht zu einer Überregulierung.

Glossar

Um eine Harmonisierung mit dem NIS2UmsuCG zu gewährleisten, sollte bei den KRITIS-Schutzzielen eine Streichung von „Authentizität“ in Bezug auf die Aufrechterhaltung der kritischen Dienstleistung erfolgen. Der Begriff wurde ebenfalls im aktuellen Referentenentwurf für ein NIS2UmsuCG entfernt, wir sprechen uns in diesem Sinne für ein kohärentes Vorgehen aus.

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 | Referent Sicherheitspolitik
T 030 27576-279 | f.kuhlenkamp@bitkom.org

Verantwortliches Bitkom-Gremium

AK Informationssicherheit