Bundesamt
für Sicherheit in der
Informationstechnik

FAQ zu Nachweisen gemäß § 8a Absatz 3 BSIG

1. ***Wer kann ein Sicherheitsaudit, eine Prüfung oder Zertifizierung nach § 8a Absatz 3 BSIG durchführen?***

   Grundsätzlich können Nachweise gemäß § 8a Absatz 3 BSIG von allen prüfenden Stellen erbracht werden, die zur Erbringung geeigneter Nachweise fähig sind. Letztendlich liegt die Verantwortung für die Erbringung eines geeigneten Nachweises und damit auch die Auswahl einer geeigneten prüfenden Stelle beim Betreiber der Kritischen Infrastruktur.

   In der "Orientierungshilfe zu Nachweisen gemäß § 8a Absatz 3 BSIG" beschreibt das BSI Kriterien, um die Eignung einer prüfenden Stelle (Kapitel 3) und des Prüfteams (Kapitel 4) bewerten zu können. Die Einhaltung dieser Kriterien bietet den Betreibern Sicherheit in der korrekten Umsetzung von § 8a Absatz 3 BSIG.

2. ***Gemäß der "Orientierungshilfe zu Nachweisen" sind DAkkS-akkreditierte Zertifizierungsstellen als prüfende Stellen zur Erbringung der Nachweise geeignet. Gilt dies auch bei einer Akkreditierung durch andere europäische Akkreditierungsstellen?***

   Das BSI geht grundsätzlich davon aus, dass Akkreditierungen für prüfende Stellen durch die Nationalen Akkreditierungsstellen der EU-Mitgliedstaaten entsprechend der europäischen Verordnung (EG) Nr. 765/2008 (Artikel 4 Absatz 1) gleichwertig zu Akkreditierungen der DAkkS sind und durch eine für den Bereich ISO/IEC 27001 akkreditierte prüfende Stelle die Umsetzung und Einhaltung der ISO/IEC 17021-1 und ISO/IEC 27006 durch die Akkreditierung ausreichend nachgewiesen wurde.

   Im Zweifel kann durch eine Anfrage an das BSI unter Angabe der Akkreditierungsstelle und des Bereiches, für den eine Akkreditierung vorliegt, Sicherheit gewonnen werden.

3. ***Wie lange ist ein Nachweis über den "Stand der Technik" gemäß § 8a Absatz 3 BSIG gültig?***

   Der Nachweis ist gemäß § 8a Absatz 3 BSIG alle zwei Jahre zu erbringen. Bereits vorhandene Prüfungen können hierbei berücksichtigt werden, sofern sie zum Zeitpunkt der Einreichung nicht älter als ein Jahr sind. Details werden in der "Orientierungshilfe zu Nachweisen gemäß § 8a Absatz 3 BSIG" beschrieben.

4. ***Welche Folgen haben Abweichungen von der „Orientierungshilfe zu Nachweisen gemäß § 8a Absatz 3 BSIG“ in der Erbringung von Nachweisen?***

   Die „Orientierungshilfe zu Nachweisen gemäß § 8a Absatz 3 BSIG“ stellt keine Festlegung im Sinne von § 8a Absatz 5 BSIG dar. Abweichungen von den Empfehlungen sind zulässig, solange qualitativ gleichwertige Alternativen genutzt werden.

   Abweichende Vorgehensweisen oder Konkretisierungen können als Teil eines B3S definiert und dem BSI zur Eignungsprüfung eingereicht werden.

5. ***In der Prüfung wurden Sicherheitsmängel festgestellt. Ist eine Behebung der Sicherheitsmängel vor Einreichung der Nachweise zulässig?***

   Das dem BSI eingereichte Nachweisdokument muss alle in der zugrundeliegenden Prüfung aufgedeckten Sicherheitsmängel auflisten. Eine Nachbesserung ist zulässig und im Sinne der Steigerung der IT-Sicherheit in KRITIS sogar erwünscht und zur Bewertung des Mangels in einem Umsetzungsplan zu dokumentieren.

   Bereits behobene Sicherheitsmängel können dem BSI freiwillig mitgeteilt werden, damit diese in das Lagebild aufgenommen werden können.

6. In welcher Sprache müssen die Nachweise erbracht werden?

Das Nachweisdokument inklusive der Anlagen und die Auflistung der Sicherheitsmängel sollen in deutscher Sprache vorgelegt werden. Die Dokumente des Betreibers sowie die Prüfberichte können in englischer Sprache vorliegen.

7. Wie lange sollte eine Prüfung nach § 8a Absatz 3 BSIG dauern?

Allgemeingültige Aussagen über die Prüfdauer sind nicht möglich, da sich die Anlagen der Betreiber Kritischer Infrastrukturen stark unterscheiden. Durch die Prüfung muss sichergestellt werden, dass die betreffende Infrastruktur gemäß § 8a Absatz 1 BSIG geschützt ist. Zu genauen Prüfumfängen kann das BSI keine Angaben machen.

Die Prüfdauer kann ggf. verkürzt werden, sofern frühere oder andere Prüfnachweise noch gültig sind und herangezogen werden können. Dabei sind sowohl Änderungen innerhalb der geprüften Anlage als auch bei der Gefährdungslage zu beachten.

8. Welche Umsetzungsfristen nach §§ 8a und 8b BSIG ergeben sich für Unternehmen, die erst NACH Inkrafttreten der BSI-KritisV erstmalig Schwellenwerte überschreiten?

Die §§ 8a und 8b BSIG enthalten keine generelle Umsetzungsfrist für den Fall des erstmaligen Überschreitens der Schwellenwerte. Vorgesehen sind nur Umsetzungsfristen, die sich auf das erstmalige Inkrafttreten der BSI-KritisV (Korb 1 und 2) beziehen. Betreiber, die nicht bereits mit Inkrafttreten von Korb 1 oder 2, sondern erst zukünftig den Regelungen unterfallen, müssen die Pflichten nach §§ 8a und 8b BSIG unverzüglich umsetzen. Für den Nachweis der Umsetzung haben die Betreiber aber zwei Jahre Zeit.

9. Sind ausschließlich Prüfer mit einer Fortbildung "zusätzlicher Prüfverfahrens-Kompetenz für § 8a BSIG" berechtigt, Prüfungen und Nachweise gemäß § 8a Absatz 3 BSIG zu erbringen?

Nein, die Prüfer können ihre Prüfverfahrenskompetenz für § 8a BSIG auch durch eine gleichwertige Qualifikation erwerben.

Bei einer Prüfung gemäß § 8a Absatz 3 BSIG ist es erforderlich, dass mindestens ein Mitglied des Prüfteams über ausreichend tiefe Prüfkenntnisse und die Besonderheiten einer Prüfung nach § 8a Absatz 3 BSIG verfügt.

Da es sich um ein komplexes Thema handelt, wurde vom BSI ein Schulungskonzept erarbeitet, mit dem diese zusätzliche Prüfverfahrenskompetenz erworben werden kann. Die Fortbildung bietet den Betreibern Kritischer Infrastrukturen ein zusätzliches Qualitätsmerkmal in der Auswahl der Prüfer und hilft bei einer zielgerichteten, geeigneten Prüfung. Das BSI empfiehlt daher den Besuch einer Schulungsmaßnahme bei einem qualifizierten Schulungsanbieter.

Bei der Fortbildung handelt es sich um keine Zulassung, Anerkennung oder Zertifizierung des Prüfers, sondern um eine empfohlene Zusatzqualifikation.

10. Stellt ein B3S eine geeignete Prüfgrundlage im Rahmen von Prüfungen gemäß § 8a Absatz 3 BSIG dar?

Nein. Ein B3S ist keine Prüfgrundlage. Ein B3S, dessen Eignung festgestellt wurde, kann jedoch dazu dienen, eine entsprechende Prüfgrundlage zu erstellen.

B3S dienen nicht der Festlegung der Prüfmethodik oder von Prüfhandlungen. Es ist nicht der Zweck eines B3S, Prüfern als Prüfgrundlage für Nachweise gemäß § 8a Absatz 3 BSIG zu dienen.

Die Auswahl und Verwendung einer geeigneten Prüfgrundlage für Prüfungen im Rahmen des § 8a Absatz 3 BSIG liegt in der Verantwortung der Prüfer. Bei der Erstellung einer geeigneten Prüfgrundlage können die aktuellen B3S nützlich sein, da sie den Stand der Technik in der Branche widerspiegeln.

11. Gibt es im Rahmen einer Prüfung gem. § 8a Absatz 3 BSIG konkrete Vorgaben des BSI, etwa zum Prüfbericht oder zu einer Stichprobengröße?

Bezogen auf den Prüfbericht macht das BSI keine formalen Vorgaben. Das BSI erhält den Prüfbericht erst auf Nachforderung, zunächst benötigt das BSI nur die in den Formularen der Nachweiserbringung abgefragten Informationen.

Die im Rahmen einer Prüfung vorgenommenen Stichproben sollten die Themenfelder angemessen abdecken. Es obliegt der Verantwortung des Prüfers, eine angemessene Stichprobengröße und die korrekte Prüfmethodik zu ermitteln und in geeigneter Form im Prüfbericht zu dokumentieren.

Grundsätzlich kann demnach ein B3S zur Erstellung einer Prüfgrundlage oder zur Erstellung von Bestandteilen hiervon verwendet werden. Allerdings kann es erforderlich sein, die Prüfgrundlage bei einem abstrakten Detailniveau des B3S für die Erbringung des Nachweises anhand konkreter Maßnahmen zu präzisieren oder an die konkreten Begebenheiten eines Betreibers durch Erweiterung oder begründete Kürzung anzupassen.

Zusätzliche Informationen entnehmen Sie der Orientierungshilfe zu Nachweisen und den entsprechenden FAQ.

12. Wie sollte ein Umsetzungsplan für die Behebung von Mängeln aussehen?

Die bei einer Prüfung gemäß § 8a Absatz 3 BSIG gefundenen Mängel sind dem BSI im Rahmen der Nachweiseinreichung in Form einer Mängelliste zu übermitteln. Die Liste beinhaltet einen Plan für die Mängelbehebung, aus dem hervorgeht, welche Maßnahmen bis zu welchem Zeitpunkt ergriffen werden, um die aufgeführten Mängel abzustellen. Die Mindestanforderungen an eine Mängelliste sind in Kapitel 5.7 der Orientierungshilfe zu Nachweisen beschrieben; eine entsprechende Muster-Mängelliste inklusive Umsetzungsplan finden sie in Anhang D der Orientierungshilfe.

Zur Erfassung des Umsetzungsstandes der Mängelbehebung reichen die Betreiber regelmäßig eine aktualisierte Version der Mängelliste beim Sektorreferat ein. Der Turnus der Einreichung der Aktualisierungen beträgt zwischen einem und sechs Monaten und wird Ihnen vom zuständigen Sektorreferat nach Sichtung der initialen Mängelliste mitgeteilt.

In der Aktualisierung ist die Nummerierung (ID) der Mängel aus der mit dem Nachweis eingereichten Mängelliste beizubehalten, damit beim BSI eine eindeutige Zuordnung erfolgen kann.

Bitte konkretisieren Sie insbesondere den Umsetzungstermin der Maßnahmen unter Angabe des tatsächlichen oder geplanten Fertigstellungsmonats. Verzögerungen bei der Umsetzung müssen nachvollziehbar begründet werden.