AuraSec

KRITIS-NACHWEISVERFAHREN

NACH § 8A (3) BSIG

Was wird im Rahmen des Kritis-Nachweisverfahrens inhaltlich geprüft?

Gemäß § 8a Abs. 3 BSI-Gesetz „haben die Betreiber Kritischer Infrastrukturen mindestens alle zwei Jahre die Erfüllung der Anforderungen nach Absatz 1 auf geeignete Weise nachzuweisen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Die Betreiber übermitteln dem Bundesamt die Ergebnisse der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel.

Gemäß der Orientierungshilfe zu Nachweisen gemäß § 8a (2) BSIG kann der Betreiber der kritischen Infrastruktur die Prüfgrundlage in Abstimmung mit der prüfenden Stelle selbst wählen.

Nachfolgend zeigen wir Ihnen auf, welche Prüfgrundlagen in Betracht kommen und welches die inhaltlichen Themen und Anforderungen sind, die im Rahmen eines Nachweisverfahrens nach § 8a (3) BSIG zu prüfen sind.

Welche Prüfgrundlagen kommen in Betracht?

- Prüfung auf Grundlage eines vom BSI anerkannten branchenspezifischen Sicherheitsstandards (B3S) - Freigegebene B3S siehe hier: https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/Stand-der-Technik-umsetzen/Uebersicht-der-B3S/uebersicht-der-b3s_node.html.

- Prüfung ohne Verwendung eines branchenspezifischen Sicherheitsstandards (B3S) und somit Prüfung auf Basis der Themenblöcke/Anforderungen gemäß Kap. 4.4 und 5.3 der Orientierungshilfe zu Nachweisen gemäß § 8a (3) BSIG vom 01.12.2017.

- Berücksichtigung vorhandener Prüfungen oder anderer Prüfgrundlagen: Vorhandene Prüfungen: z.B. Auditberichte zu ISO/IEC 27001 oder IT-Grundschutz-Audits durch eine unabhängige Prüfstelle, Berichte zu IT-Prüfungen durch Wirtschaftsprüfungsgesellschaften oder die interne Revision

- Andere Prüfgrundlagen: Prüfung auf Basis anerkannter Standards und Regelwerken zum Management der Informationssicherheit, wie z.B. ISO/IEC 27000 Normenreiheund/oderIT-Grundschutzkompendium

Der Betreiber hat die Möglichkeit, der prüfenden Stelle bereits vorhandene Prüfgrundlagen zur Verfügung zu stellen. Die prüfende Stelle entscheidet, ob und zu welchem Grad diese in die Prüfung einfließen können.

Die gemäß § 8a (1) BSIG inhaltlich zu prüfenden organisatorischen und technischen Vorkehrungen finden sich sind in Kap. 4.4 und 5.3 der Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a (2) BSIG V1.0 vom 01.12.2017.

Wird eine andere Prüfgrundlage als ein freigegebener Branchenspezifischer Sicherhietsstandard (B3S) verwendet, so sind die nachstehenden Thembereiche und Anforderungen

Organisatorisch und technische Vorkehrungen:

- Informations-Sicherheits-Management-System (ISMS)
- Asset Management
- Risikoanalysemethode
- Continuity Management für die kDL
- Notfallmanagement und Übungen
- Branchenspezifische Technik
- Technische Informationssicherheit (Maßnahmenkategorien)
- Personelle und organisatorische Sicherheit
- Bauliche/physische Sicherheit
- Vorfalls Erkennung und -bearbeitung
- Überprüfung im laufenden Betrieb
- Externe Informations-versorgung und Unterstützung
- Lieferanten, Dienstleister und Dritte

AuraSec

AuraSec GmbH | Unter den Linden 16 | 10117 Berlin
T 030 408173352 | **F** 05334 948624
info@aurasec.de | www.aurasec.de