Inhaltsverzeichnis

1 UMFANG DES PRÜFVERFAHHRENS

Überprüfung der Erfüllung der Anforderungen an ein Informationssicherheitsmanagementsystem gemäß den Anforderungen des Gesetzes des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) und der Anforderungen der Verordnung zur Bestimmung Kritischer Infrastrukturen nach der BSI-Kritisverordnung (BSI-KritisV) nach § 8a (3)

2 PRÜFGRUNDLAGE

Grundlagen sind die Anforderungen des Gesetzes des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) gemäß §8a und der Anforderungen der Verordnung zur Bestimmung Kritischer Infrastrukturen nach der BSI-Kritisverordnung (BSI-KritisV) nach §10. Hiernach sind die Betreiber kritischer Infrastrukturen verpflichtet ein Informationsmanagementsystem (ISMS) aufzubauen, zu betreiben und deren Wirksamkeit in regelmäßigen Abständen – mindestens alle 2 Jahre – überprüfen zu lassen und auftretende Risiken, Probleme oder Angriffe an das BSI zu melden. Die Rahmenbedingungen zur Prüfung sind in der vom BSI herausgegebenen Orientierungshilfe zu Nachweisen gemäß §8a (3) BSIG zu finden. Hierzu haben die Gesetz- und Regelwerksgeber die nachfolgenden Nachweisverfahren zur Auswahl gestellt.

- Prüfung auf Grundlage eines vom BSI anerkannten branchenspezifischen Sicherheitsstandards (B3S)
- Prüfung ohne Verwendung eines branchenspezifischen Sicherheitsstandards (B3S)
- Berücksichtigung vorhandener Prüfungen oder anderer Prüfgrundlagen

3 PRÜFGEGENSTAND

Prüfgegenstand ist die Prüfung des ISMS für Anlagen von Betreibern kritischer Infrastrukturen. Die Anlagekategorien werden in den beiden Teilen (Korb 1 und Korb 2) der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz definiert.

4 GELTUNGSBEREICH

Der Geltungsbereich und die Regelungen des ISMS müssen angemessene Vorkehrungen zur Vermeidung von Störungen […] ihrer informationstechnischen Systeme" nach dem "Stand der Technik" treffen.
Das ISMS muss vollumfänglich definiert, den gesetzlichen Anforderungen, den spezifischen Anforderungen der Anlagen und deren Risiken Rechnung tragen.

5 AUFGABEN, LEISTUNGEN UND PFLICHTEN DER PRÜFENDEN STELLE

Die grundsätzlichen Aufgaben der prüfenden Stelle sind,

- die Einhaltung der Prozesse und Verfahren festzustellen,
- für einheitliche und gleichwertige Prüfungsdurchführung und Prüfergebnisse zu sorgen,
- die Qualitätsprüfung vorzunehmen,
- Rahmenbedingungen für die Prüfdurchführung festzulegen,
- das Prüfteam zusammenzustellen und die Abdeckung aller Kompetenzbereiche sicherzustellen (hierzu ist die prüfende Stelle berechtigt Fachexperten einzubeziehen)
- die Eignung der Prüfer zu bestätigen sowie
- die Kommunikation mit dem Betreiber und dem Prüfteam durchzuführen.

Inhaltlich orientieren sich die Prüfungen an der Mapping-Tabelle zur Orientierungshilfe B3S (3) und werden im Einzelnen in folgenden Leistungsschritten erbracht:

5.1 Vorbereitung der Prüfung

- Erhebung der relevanten Anlagendaten
- Verifizierung der Prüfgrundlage und Festlegung der Prüfthemen
- Feststellung der Komplexität und des Prüfumfangs
- Ermittlung des Prüfaufwands
- Screening der Dokumentation
    - Folgende Dokumentation wird benötigt:
        - Geltungsbereich des ISMS
        - Erklärung zur Anwendbarkeit
        - Netzstrukturplan mit kritischen Assets
        - Risikobeurteilung auf Basis von §8a BSIG
        - Ausgefüllte Mappingliste mit den Maßnahmen
- Erstellung des Prüfkonzeptes & Prüfplans (ggfs. Festlegung einer Stichprobe)
- Abstimmung der Prüftermine & -teilnehmer

5.2 Vor - Prüfung (optional Vor-Ort)

- Vor-Prüfung des ISMS auf:
    - Anwendbarkeit
    - Umfang & Vollständigkeit
    - Plausibilität & - Integrität
    - Wirksamkeit

5.3 Hauptprüfung (Vor-Ort)

- Umsetzung des Prüfkonzeptes und -plans:
  - Eröffnung der Vor-Ort-Aktivitäten
  - Durchführung der Interviews
  - Einsicht und Prüfung der ISMS-Verfahren und Dokumentation
  - Begehungen der Anlage(n)
  - Erstellung von Aufzeichnungen
  - Einholung Erklärungen
  - Zusammenfassung

5.4 Prüfnachbereitung

- Erstellung eines Prüfberichtes
- Prüffeststellung (Votum)
- Erstellung und Aushändigung der Nachweisdokumente (KI, PS, PD, PE und Mängelliste samt Netzstrukturplan)
- Prüfdokumentation und Archivierung
- ggfs. Abstimmung von Folgeterminen

6 PRÜFABLAUF

Grundsätzlich ist der Auftraggeber zur Unterstützung und Mitwirkung des Prüfverfahrens verpflichtet, sowie zur Angabe vollständiger und wahrheitsgemäßer Informationen.
Der Auftraggeber hat hierzu eine rechtsverbindliche Erklärung abzugeben.
Der Auftraggeber verschafft den Prüfern des Auftragnehmers uneingeschränkten Zugang zu allen erforderlichen Anlagen und Informationen.

Für die Dokumentenprüfung stellt der Auftraggeber dem Auftragnehmer folgendes bereit:

- Konzept und Dokumentation des Risikomanagements inkl. Risikoanalyse
- Beschreibung des Informationssicherheitsmanagementsystems (ISMS)
- Notfallkonzept und Beschreibung des Continuity Managements
- Dokumente des Asset Managements
- Dokumentation der Prozesse zur baulichen und physischen Sicherheit (z. B. Zutrittskontrolle oder Brandschutzmaßnahmen)
- Dokumentation der personellen und organisatorischen Sicherheit (z. B. Aufzeichnungen über Mitarbeiterschulungen, Sensibilisierungskampagnen, Berechtigungsmanagement)
- Konzepte und Dokumentation zur Vorfallserkennung und -bearbeitung (z. B. Beschreibung zu Incident Management, Detektion von Angriffen, Forensik)
- Konzepte und Dokumentation von Überprüfungen (z. B. Prüfberichte der internen Revision sowie anderer durchgeführter Audits, Übungen, systematische Log-Auswertungen usw.)
- Richtlinien zur externen Informationsversorgung
- Richtlinien zum Umgang mit Lieferanten und Dienstleistern (z. B. Service Level Agreements und andere die Sicherheit betreffende Vereinbarungen mit Dienstleistern)
- Sicherheitskonzept (inkl. Darstellung umgesetzter und geplanter Maßnahmen), insbesondere der branchenspezifischen Maßnahmen

7 VERANTWORTLICHKEITEN UND HAFTUNGSAUSSCHLÜSSE

Da der Auftraggeber keine juristische Sozietät ist, können auch keine juristischen Prüfungen oder Gutachten zur Erfüllung der geltenden Gesetze und Verordnungen erbracht werden.
Der Auftraggeber ist vollumfänglich für die Einhaltung und Erfüllung der geltenden Gesetze und Verordnungen verantwortlich. Dieses gilt gleichermaßen für die Bestimmung und Kategorisierung der betreffenden Anlagen sowie für die vollständige Abdeckung des Scopes nach BSI-KritisV. Hierfür übernimmt der Auftragnehmer keinerlei Verantwortung oder Haftung.
Bei unzumutbaren Risiken oder Arbeitsbedingungen ist der Auftragnehmer berechtigt die Prüfungen auf Kosten des Auftraggebers abzubrechen oder zu verschieben.

8 MIT GELTENDE UNTERLAGEN

8.1 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG)

Geltung ab: 20. August 2009; Erschienen im: Bundesgesetzblatt Jahrgang 2009 Teil I Nr. 54, ausgegeben zu Bonn am 19. August 2009

8.2 Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz

(BSI-Kritisverordnung - BSI-KritisV) BSI-KritisV; Ausfertigungsdatum: 22.04.2016; Vollzitat: "BSI-Kritisverordnung vom 22. April 2016 (BGBl. I S. 958), die durch Artikel 1 der Verordnung vom 21. Juni 2017 (BGBl. I S. 1903) geändert worden ist"; Stand: Geändert durch Art. 1 V v. 21.6.2017 I 1903

8.3 Mapping Tabelle des BSI

Der Prüfplan und die Prüfinhalte sowie -umfänge orientieren sich an der Mapping-Tabelle des BSI:

8.4 Dokumente des BSI

Die folgenden Dokumente des BSI:

- Aktuelle Orientierungshilfe zu Nachweisen gemäß § 8a (3) BSIG
- Aktuelle Anlage zum Nachweisdokument zu § 8a (3) BSIG; Blatt KI: Angaben zur geprüften Kritischen Infrastruktur und zum Ansprechpartner
- Aktuelle Anlage zum Nachweisdokument zu § 8a (3) BSIG; Blatt PS: Angaben zur Eignung der prüfenden Stelle und zum Prüfteam
- Aktuelle Anlage zum Nachweisdokument zu § 8a (3) BSIG; Blatt PD: Angaben zur Prüfdurchführung
- Aktuelle Anlage zum Nachweisdokument zu § 8a (3) BSIG; Blatt PE: Angaben zum Prüfergebnis