Beschreibung des Prüfungsverfahrens gemäß §8a BSIG

Inhaltsverzeichnis

Haben Sie Fragen zu der Leistungsbeschreibung? Wir helfen Ihnen gern weiter.

Sie erreichen uns per Mail info.tncert@tuev-nord.de oder persönlich von Montag bis Freitag zwischen 07:30 Uhr und 18:00 Uhr unter 0800 – 2457457.

TÜV NORD CERT GmbH

Langemarckstraße 20

45141 Essen

www.tuev-nord-cert.de

1 GELTUNGSBEREICH

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 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.

Durch die Prüfung muss sichergestellt werden, dass der KRITIS-Betreiber wirksame, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit seiner informationstechnischen Systeme, Komponenten oder Prozesse, die für die Funktionsfähigkeit der von ihm betriebenen Kritischen Infrastrukturen maßgeblich sind, getroffen hat.

Der Geltungsbereich des ISMS muss vollumfänglich definiert sein und den gesetzlichen Anforderungen, den spezifischen Anforderungen der Anlagen und deren Risiken Rechnung tragen.

3 PRÜFGRUNDLAGE

Grundlagen sind die Anforderungen gemäß §8a BSIG. Hiernach sind die Betreiber kritischer Infrastrukturen verpflichtet ein 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

4 AUFGABEN, LEISTUNGEN UND PFLICHTEN

4.1 Prüfende 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 Qualitätssicherungsprüfung 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
- die Kommunikation mit dem Betreiber und dem Prüfteam durchzuführen

4.2 KRITIS Betreiber

Grundsätzlich ist der KRITIS Betreiber (Auftraggeber) zur Unterstützung und Mitwirkung des Prüfverfahrens verpflichtet, sowie zur Angabe vollständiger und wahrheitsgemäßer Informationen.

Der Betreiber hat hierzu eine rechtsverbindliche Erklärung abzugeben.

Der Betreiber verschafft den Prüfern der prüfenden Stelle uneingeschränkten Zugang zu allen erforderlichen Anlagen und Informationen.

- Für die Dokumentenprüfung stellt der Betreiber der prüfenden Stelle 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

4.3 Verantwortlichkeiten und Haftungsausschlüsse

Da der Betreiber keine juristische Sozietät ist, können auch keine juristischen Prüfungen oder Gutachten zur Erfüllung der geltenden Gesetze und Verordnungen erbracht werden.

Der Betreiber 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 die prüfende Stelle keinerlei Verantwortung oder Haftung.

Bei unzumutbaren Risiken oder Arbeitsbedingungen ist die prüfende Stelle berechtigt die Prüfungen auf Kosten des Betreibers abzubrechen oder zu verschieben.

5 PRÜFABLAUF

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:
    - Geltungsbereich des ISMS (Beschreibung und grafische Darstellung)
    - Netzstrukturplan
    - Prozess zum Risikomanagement
    - Risikobewertung auf Basis §8a BSIG
    - Asset-Inventarisierungsliste
    - Ggfs. Erklärung zur Anwendbarkeit
- Erstellung des Prüfkonzeptes & Prüfplans (ggfs. Festlegung einer Stichprobe)
- Abstimmung der Prüftermine & -teilnehmer

5.2 Vorprüfung (optional Vor-Ort)

Es ist empfehlenswert eine Vorprüfung mit einem zeitlichen Abstand zur Hauptprüfung durchzuführen. Diese kann bei einem entsprechenden Reifegrad des ISMS ggfs. gemeinsam mit der Hauptprüfung durchgeführt werden.

Für die Koordinierung der Tätigkeiten ggf. die Abstimmung der beteiligten Auditoren untereinander ist der leitende Auditor verantwortlich.

Die Vorprüfung des ISMS wird durchgeführt, um:

- die Managementsystem-Dokumentation des Kunden zu auditieren

- den Standort und die standortspezifischen Bedingungen des Kunden zu beurteilen sowie Diskussionen mit dem Personal der Organisation des Kunden zu führen, um die Bereitschaft für die Hauptprüfung zu ermitteln
- den Status des Kunden sowie das Verständnis bezüglich der Anforderungen der Prüfgrundlage, insbesondere im Hinblick auf die Identifizierung von Schlüsselleistungen bzw. bedeutsamen Aspekten, Prozessen, Zielen und das Betreiben des ISMS zu bewerten
- Informationen bezüglich des Anwendungsbereichs des ISMS, der Prozesse und der Standorte des Kunden zu sammeln und den Umfang und die Vollständigkeit beurteilen zu können

5.3 Hauptprüfung (Vor-Ort)

Mit Beginn der Hauptprüfung erhält der Betreiber einen mit ihm abgestimmten Prüfplan.

Die Prüfung beginnt mit einem Eröffnungsgespräch, in dem sich die Teilnehmer vorstellen. Das Vorgehen während der Prüfung wird erläutert. Im Rahmen der Prüfung im Unternehmen überprüfen und bewerten die Prüfer die Wirksamkeit des eingeführten ISMS.

Umsetzung des Prüfkonzeptes und Prüfplans:

- 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

Zum Abschluss der Hauptprüfung findet ein Schlussgespräch statt. An diesem Gespräch nehmen mindestens die Mitarbeiter teil, die leitende Funktionen im Unternehmen haben und deren Bereiche in das Audit eingebunden waren. Der leitende Auditor berichtet über die einzelnen Elemente, erläutert positive und negative Ergebnisse.

5.4 Prüfnachbereitung

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

6 MITGELTENDE UNTERLAGEN

6.1 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

6.2 Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz

BSI-Kritisverordnung; 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

6.3 Dokumente des BSI

Die folgenden Dokumente des BSI:

Die folgenden Dokumente des BSI:

- Aktuelle Orientierungshilfe zu Nachweisen gemäß §8a (3) BSIG
- Aktuelles Nachweisdokument zu § 8a (3) BSIG; Blatt KI: Angaben zur geprüften Kritischen Infrastruktur und zum Ansprechpartner
- Aktuelles Nachweisdokument zu § 8a (3) BSIG; Nachweisdokument P samt Anlagen