TeleTrusT "IT-Sicherheitsrechtstag 2021"

Berlin, 24.09.2021

Prüfschwerpunkte für KRITIS

Dr.-Ing. Jan Sanders
BSI, Referat WG 15 „Kritische Infrastrukturen – Prüfungen“

Bundesamt
für Sicherheit in der
Informationstechnik

Überblick

1. Tiefenprüfung - Was ist eine „Prüfung nach § 8a Abs. 4 BSIG“?

2. Was soll eine Tiefenprüfung erreichen?

3. Was sind Schwerpunkte einer Tiefenprüfung?

Tiefenprüfung – Was ist das?

Tiefenprüfung (§ 8a Abs. 4 BSIG)

- Das BSI prüft selbst beim Betreiber

- Das BSI kann sich Dritter bedienen

- Die Einhaltung von § 8a Abs. 1 BSIG wird geprüft
  - angemessene organisatorische und technische Vorkehrungen
  - Stand der Technik

- Gebührenpflicht für Prüfungen
  - Wenn Anhaltspunkten berechtigte Zweifel an der Einhaltung der Anforderungen begründen

Tiefenprüfung (§ 8a Abs. 4 BSIG) vs. Nachweise (§ 8a Abs. 3 BSIG)

- Betreiber geben Nachweisprüfung selbst in Auftrag
- Prüfungsschwerpunkte werden von den prüfenden Stellen gesetzt
- BSI bietet für Nachweise eine Orientierungshilfe
- BSI kann Vorgaben für Nachweise nach § 8a Abs. 5 BSIG machen
  (bisher eine Vorgabe im Sektor IKT mit Bezug zu Geltungsbereichen)
- Tiefenprüfungen sind kein Ersatz und keine Heilung von Nachweisprüfungen

Tiefenprüfung – Wozu ist das?

Tiefenprüfung (§ 8a Abs. 4 BSIG)

- Sicherstellen, dass Betreiber angemessene Vorkehrungen getroffen haben
  - durch zufällig gewählte Stichproben
  - durch anlassbezogene Prüfungen
- Abgleich der Nachweis-Lage mit der tatsächlichen Lage

Tiefenprüfung – Schwerpunkte

Prüfungsschwerpunkte - Auswahlkriterien

- Grundsätzliche Fähigkeit der Betreiber Informationssicherheit zu gewährleisten
- Resilienz im Bezug auf dynamische Bedrohungslage
- Integration in Warn- und Meldewesen

Prüfungsschwerpunkte - Themenfelder

- ISMS – Geltungsbereich / KRITIS – Geltungsbereich
- Informationssicherheitsleitlinie
- Sicherheitsorganisation
- Asset Management
- Dienstleistermanagement
- Risikomanagement
- Incident Management
- Business Continuity Management

Prüfungsschwerpunkte - Themenfelder

- ISMS – Geltungsbereich / KRITIS – Geltungsbereich
- Informationssicherheitsleitlinie
- Sicherheitsorganisation
- Asset Management
- Dienstleistermanagement
- Risikomanagement
- Incident Management
- Business Continuity Management

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Diese Folie ist ein Platzhalter für Ihre Fragen

Kontakt

Dr.-Ing. Jan Sanders

Referat WG 15 – Kritische Infrastrukturen – Prüfungen

Referat-WG15@BSI.Bund.DE

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de
www.bsi-fuer-buerger.de

Bundesamt
für Sicherheit in der
Informationstechnik