

## Informationssicherheit-/ KRITIS-Anforderungen für Vergabe

Die Autobahn GmbH etabliert auf Basis des BSI-IT-Grundschutz nach den Standards 200-1, 200-2, 200-3 und 200-4 in den aktuellen Editionen ein übergreifendes Informationssicherheits- und Business Continuity Management System. Weiterhin unterliegen Teile der Autobahn GmbH des Bundes der § 39 BSIG-Nachweispflicht. Die KRITIS Dienstleistungen unterliegen den Vorgaben und Anforderungen, die u. A. im Branchenspezifischen Sicherheitsstandard (B3S)<sup>1</sup> für die Verkehrssteuerungen und Leitsystemen der Bundesautobahn sowie BSIG definiert sind.

### 1 Schutzbedarf

Die Autobahn hat sich für die Vorgehensweise der Standardabsicherung des BSI-Grundschutzes entschieden. Unter dieser Prämisse und der durchgeführten Schutzbedarfsfeststellung, ist beim Ausschreibungsgegenstand von folgendem Schutzbedarf auszugehen:

- a. **Hoch** Schutzbedarf in dem Schutzziel Verfügbarkeit
- b. **Hoch** Schutzbedarf in dem Schutzziel Vertraulichkeit
- c. **Hoch** Schutzbedarf in dem Schutzziel Integrität

Der Ausschreibungsgegenstand betrifft KRITIS Dienstleistungen. Es gelten zusätzlich die Vorgaben des Branchenspezifischer Sicherheitsstandard für die Verkehrssteuerungs- und Leitsysteme der Bundesautobahn sowie dem dazugehörigen IT-Grundschutz Profils<sup>2</sup>.

Es wird darauf hingewiesen, dass bei der Umsetzung aller Sicherheitsanforderungen/-maßnahmen bis zum Stand der Technik eine Risikoakzeptanz bzw. Risikoverschiebung nicht erlaubt ist.

#### 1.1 KRITIS Schutzbedarfsergänzung

Aufgrund der KRITIS Betroffenheit ist zusätzlich von einem

- a. **Hoch** Schutzbedarf in dem Schutzziel Authentizität
- auszugehen.

### 2 Zertifizierung

Der Auftragnehmer hält während der Vertragslaufzeit, für den in der Ausschreibung definierten Aufgabenbereich, eine Zertifizierung idealerweise nach ISO/IEC 27001 auf Basis von IT-Grundschutz, bzw. mindestens nach ISO/IEC 27001 nativ aufrecht. Sollte die Zertifizierung noch nicht vorliegen ist diese innerhalb von 1 Jahr nach Leistungsbeginn zu erlangen. Der entsprechende Projektplan ist der Autobahn GmbH vorzulegen.

---

<sup>1</sup> [Branchenspezifischen Sicherheitsstandard für die Bundesautobahnen - BSI](#)

<sup>2</sup> [IT-Grundschutz-Profil für die Verkehrssteuerungs- und Leitsysteme der Bundesautobahn](#)

Der Auftragnehmer weist während der Vertragslaufzeit für den in der Ausschreibung definierten Aufgabenbereich nach, dass er ein funktionsfähiges Informationssicherheitsmanagement hat. Dies beinhaltet mindestens gem. BSI-IT-Grundschutz-Kompendium<sup>3</sup> in aktueller Version:

- a. Benennung Informationssicherheitsbeauftragter
- b. Strukturierter Umgang mit Informationssicherheitsvorfällen inkl. Erkennung, Behandlung und Bereinigung
- c. Awareness-Schulungen der Mitarbeiter
- d. Lieferantenmanagement (OPS.2.3 und OPS.3.2)
- e. Datensicherung, -löschung und -vernichtung (CON.3 und CON.6)
- f. Informationsaustausch (CON.9)
- g. Allgemeiner IT-Betrieb (OPS.1.1.1)
- h. Ordnungsgemäße IT-Administration (OPS.1.1.2)
- i. Protokollierung (OPS.1.1.5)
- j. Patch- und Änderungsmanagement (OPS.1.1.3)
- k. Systemmanagement und -monitoring (OPS.1.1.7)
- l. Notfallmanagement (DER.4)

### **3 Zusätzliche Sicherheitsanforderungen**

Grundsätzlich hat der Auftragnehmer die genannten Sicherheitsanforderungen für den in der Ausschreibung genannten Aufgabenbereich einzuhalten. Abweichungen hiervon sind vor Vertragsschluss mit dem Auftraggeber abzustimmen und abzuwägen.

#### **3.1 Netzmanagement und Netzkomponenten**

Der Auftragnehmer muss die folgenden Sicherheitsanforderungen einhalten, die für den in der Ausschreibung genannten Aufgabenbereich relevant sind:

- a. Netzmanagement (NET.1.1)
- b. Router und Switches (NET.3.1)
- c. Firewall (NET.3.2)
- d. VPN (NET.3.3)
- e. Network Access Control (NET.3.4)

Abweichungen hiervon sind vor Vertragsschluss mit dem Auftraggeber abzustimmen und abzuwägen.

#### **3.2 (Fern-)Wartung und Instandhaltung**

Der Auftragnehmer muss die folgenden Sicherheitsanforderungen einhalten, die für den in der Ausschreibung genannten Aufgabenbereich relevant sind:

- a. Schutz vor Schadprogrammen (OPS.1.1.4)
- b. Software-Tests und -Freigaben (OPS.1.1.6)
- c. Fernwartung (OPS.1.2.5)

---

<sup>3</sup> [BSI-IT-Grundschutz-Kompendium \(Edition 2023\)](#)

### **3.3 Softwareentwicklung (inkl. Pflege und Support):**

Der Auftragnehmer besitzt für seinen Softwareentwicklungsbereich ein etabliertes Schwachstellenmanagement, um entsprechende CVE-Meldungen etc. zu behandeln. Weiterhin existiert Vorgaben zur sicheren Softwareentwicklung. Dies ist durch den Anbieter entsprechend schriftlich zu bestätigen.

### **3.4 Personal**

Der Auftragnehmer stellt ausschließlich Personal mit nachweisbarem Wissen im Umgang der BSI-Grundschutz Thematik zur Verfügung. Als mögliche Nachweise für die Vertrautheit im Umgang mit den Methodiken des BSI IT-Grundschutzes kann der Auftragnehmer eine Zertifizierung nach ISO/IEC 27001 auf Basis von IT-Grundschutz im eigenen Informationsverbund angeben oder BSI IT-Grundschutz Praktiker/Berater zertifiziertes Personal benennen.

### **3.5 Best-Practice Anforderung an KRITIS-Lieferanten**

Es wird auf die „Best-Practice-Empfehlungen für Anforderungen an Lieferanten zur Gewährleistung der Informationssicherheit in Kritischen Infrastrukturen<sup>4</sup>“ des UP KRITIS, in der aktuellen Version, verwiesen. Die dort dokumentierten Anforderungen sind grundsätzlich einzuhalten. Abweichungen hiervon sind gegenüber dem Auftraggeber inkl. entsprechender Begründung aufzuzeigen und von dieser im Rahmen des Vertragsabschlusses gemeinsam zu bewerten.

---

<sup>4</sup> [Best-Practice-Empfehlungen für Anforderungen an Lieferanten](#)