Anforderungen in Bezug auf die Informationssicherheit

Der Auftragnehmer/die Auftragnehmerin hat ein ganzheitliches, sich über die gesamte IT-Infrastruktur des Fachverfahrens bzw. der Fachanwendung erstreckendes Informationssicherheitskonzept vorzulegen.

I. Allgemeines

Vor Inbetriebnahme des Fachverfahrens bzw. der Fachanwendung muss sichergestellt sein, dass während des Betriebes insbesondere die IT-Sicherheitsziele der Vertraulichkeit, Integrität, Verfügbarkeit, Schutz der Compliance, Authentizität und Rechtssicherheit erreicht werden.

Vor diesem Hintergrund ist insbesondere ein Informationssicherheitskonzept gemäß IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik nach Maßgabe des folgenden Abschnitts (**II.**) zu erstellen und dem Auftraggeber vor Inbetriebnahme vorzulegen. Diese Anforderungen sind vertragliche Hauptleistungspflichten des Auftragnehmers/der Auftragnehmerin; entsprechende Leistungen müssen vom Auftraggeber abgenommen werden.

II. Pflicht des Auftragnehmers/der Auftragnehmerin zur Vorlage eines Informationssicherheitskonzepts nach BSI IT-Grundschutz vor Inbetriebnahme

Die Landesverwaltung Baden-Württemberg orientiert sich bei der Ausgestaltung der Informationssicherheit an den Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Zur Gewährleistung der Informationssicherheit des Fachverfahrens bzw. der Fachanwendung ist daher nach BSI IT-Grundschutz und seinen Standards ein **Informationssicherheitskonzept** zu erstellen und vor Aufnahme des produktiven Betriebs des Fachverfahrens bzw. der Fachanwendung dem Auftraggeber zum Zwecke der Abnahme bzw. Freigabe vorzulegen. Das Informationssicherheitskonzept muss mit den Vorgaben des E-Government-Gesetzes Baden-Württemberg („EGovG BW“) sowie der Verwaltungsvorschrift des Innenministeriums zur Informationssicherheit („VwV Informationssicherheit“) im Einklang stehen. Rechtsgrundlage hierfür ist § 16 Abs. 2 EGovG BW i.V.m. Nummer 3.1 sowie Nummer 3.11 der VwV Informationssicherheit.

Abweichend von Nummer 3.1 der VwV Informationssicherheit ist das Sicherheitskonzept nicht am Maßstab der früheren BSI IT-Grundschutz-Standards 100-1 bis 100-3, sondern vielmehr **am Maßstab der aktuellen BSI IT-Grundschutz-Standards 200-1 bis 200-3** zu erstellen.

In der Vorgehensweise nach BSI IT-Grundschutz wird implizit eine Risikobewertung für Bereiche mit normalem Schutzbedarf durchgeführt. In Abhängigkeit vom im Einvernehmen mit dem Auftraggeber festgestellten Schutzbedarf der verarbeiteten Informationswerte, namentlich wenn der betrachtete Informationsverbund Komponenten mit hohem oder sehr hohem Schutzbedarf enthält, muss jedoch zusätzlich eine **ergänzende Sicherheitsanalyse** und gegebenenfalls eine **explizite Risikoanalyse** durchgeführt und dokumentiert werden.

Wenn der betrachtete Informationsverbund Komponenten mit **hohem oder sehr hohem Schutzbedarf** enthält, muss das dem Auftraggeber vorzulegende Informationssicherheitskonzept insbesondere bestehen aus

1. einer **Strukturanalyse**, ihrerseits bestehend insbesondere aus

   a) der Abgrenzung des Informationsverbundes,

   b) der Erfassung der Geschäftsprozesse, Informationen, Informationstechnik und IT-Anwendungen,

   c) der Bildung von Gruppen sowie

   d) der Erstellung eines sog. bereinigten Netzplans in Form einer Skizze und Beschreibung aller Verbindungen z. B. als Kommunikationsmatrix,

2. einer **Schutzbedarfsfeststellung**,

3. einer **Grundschutzanalyse**, diese insbesondere in Form einer Modellierung der Bausteine nach IT-Grundschutz sowie einem IT-Grundschutz-Check mit Soll-Ist-Vergleich,

4. einer **Risikoanalyse** inklusive Gefährdungsübersicht, Risikoeinstufung, Risikoeinschätzung, Risikobewertung und Risikobehandlung und

5. einer **Realisierungsplanung**, diese insbesondere in Form einer Konsolidierung der Maßnahmen sowie eines Umsetzungsplanes.

Andernfalls, nämlich im Falle eines **normalen Schutzbedarfs**, muss das Informationssicherheitskonzept insbesondere bestehen aus

1. einer **Strukturanalyse** (notwendige Inhalte vgl. oben),
2. einer **Schutzbedarfsfeststellung**,
3. einer **Grundschutzanalyse** (notwendige Inhalte vgl. oben) und
4. einer **Realisierungsplanung** (notwendige Inhalte vgl. oben).

Daher ist die o. g. „**Risikoanalyse**“ optional anzubieten.

Das durch den Auftragnehmer/die Auftragnehmerin zu erstellende Sicherheitskonzept bezieht sich auf das Fachverfahren in seiner Gesamtheit bzw. auf die Fachanwendung in ihrer Gesamtheit, vgl. hierzu Abschnitt VI.

III. Abstimmung mit dem Auftraggeber / Konzeptpapier

Das Erstellen des Sicherheitskonzeptes für das Fachverfahren bzw. die Fachanwendung erfolgt **in enger Abstimmung mit dem Auftraggeber**. Dabei ist zunächst ein **Konzeptpapier (Entwurf) als separates Dokument**, ggf. mit erforderlichen Anlagen (z.B. IT-Grundschutz-Check mit Soll-Ist-Vergleich), auszuformulieren. Die einzelnen, o. a. Abschnitte bauen aufeinander auf und sind daher sukzessive mit dem Auftraggeber abzustimmen. Das Konzeptpapier ist ferner insbesondere hinsichtlich folgender Eckpunkte mit dem Auftraggeber abzustimmen:

1. Festlegung der Verantwortlichkeiten,
2. Festlegung des Geltungsbereiches des Informationsverbundes (auch hinsichtlich Schnittstellen und abzugrenzenden Bereichen) sowie
3. Feststellung des Schutzbedarfs der verarbeiteten Informationen.

IV. Form des Informationssicherheitskonzeptes

Konzeptpapiere und finales Informationssicherheitskonzept sind jeweils in **elektronischer Form**, **nämlich als DOCX**, vorzulegen.

V. Kosten für das Informationssicherheitskonzept

Kosten für das zu erstellende Informationssicherheitskonzept sind in Angeboten und Rechnungen gesondert auszuweisen.

VI. Geltungsbereich des Informationsverbundes

Im Informationssicherheitskonzept müssen **sämtliche Funktionalitäten des Fachverfahrens bzw. der Fachanwendung** betrachten werden einschließlich Schnittstellen, Reporting- und Trackingfunktionen sowie alle weiteren gegebenenfalls geplanten bzw. verfügbaren Funktionalitäten. Daher sind auch **sämtliche hardware- und softwarebezogenen Komponenten**, auch solcher Komponenten etwaiger Dienstleister (zum Beispiel Hosting-Betreiber), zu betrachten. Dies umfasst u. a. sämtliche IT-Infrastrukturkomponenten (Clients, Server etc.) sowie Applikationen (Datenbanksysteme sowie Content-Management-Systeme einschließlich etwaiger Plug-Ins etc.). Gültige **BSI- bzw. ISO27001-Zertifizierungen** der Hosting-Betreiber sind erforderlich. Auf diese muss im Sicherheitskonzept Bezug genommen werden. Die Zertifikate müssen dem Sicherheitskonzept in Form von Anlagen beigefügt werden.

Es müssen geeignete technische und organisatorische Maßnahmen umgesetzt und dokumentiert werden, sodass eine sichere, datenschutzkonforme und zuverlässige Nutzung aller Funktionalitäten des Fachverfahrens bzw. der Fachanwendung ununterbrochen gewährleistet ist.

VII. Behandlung von Sicherheitsvorfällen

Sicherheitsvorfälle müssen dem Auftraggeber schnellstmöglich entsprechend der vertraglichen Regelungen gemeldet und vom Auftragnehmer/von der Auftragnehmerin behoben werden. Die Behandlung von Sicherheitsvorfällen ist sowohl im Angebot als auch im Informationssicherheitskonzept an geeigneter Stelle zu beschreiben (Melde- und Eskalationswege, Erreichbarkeit außerhalb der normalen Arbeitszeit). Insbesondere ist zur Behandlung von Sicherheitsvorfällen ein Ansprechpartner/eine Ansprechpartnerin des Auftragnehmers/der Auftragnehmerin zu benennen.

VIII. Besondere Anforderungen an die Vertraulichkeit

Netzwerkverbindungen müssen verschlüsselt sein. Die Art der Verschlüsselung muss dem jeweils aktuellen Stand der Technik entsprechen; sie ist bei Abgabe des Angebots dort explizit zu benennen und im Informationssicherheitskonzept an geeigneten Stellen zu dokumentieren.

Das Fachverfahren bzw. die Fachanwendung muss durch Authentifizierungsmechanismen verhindern, dass Unbefugte hierauf zugreifen können. Es muss sichergestellt sein, dass administrative Aufgaben nur im jeweiligen Zuständigkeitsbereich des Auftragnehmers erledigt werden können.

IX. Besondere Anforderungen an die Verfügbarkeit

1. Allgemeines

Das Fachverfahren bzw. die Fachanwendung ist so auszulegen, dass es bzw. sie mit möglichst hoher Verfügbarkeit und engen Wartungsfenstern betrieben werden kann. Insbesondere sind Wartungen und Upgrades des Systems so durchzuführen, dass der werktägliche Betrieb möglichst nicht gestört wird.

Das Fachverfahren bzw. die Fachanwendung muss so entworfen sein, dass ein verlässlicher Betrieb gewährleistet ist. Sicherheitsvorfälle müssen schnellstmöglich behoben werden (vgl. oben, VII.). Für Wartungsfenster im Normalbetrieb sind höchstens vier Stunden pro Monat anzusetzen, die zwischen 0.00 Uhr und 4.00 Uhr in der Nacht an Samstagen und Sonntagen vorzusehen sind.

Ein solches Patchen der Server, das mit Betriebsunterbrechungen einhergeht (z. B. in Fällen, in denen Neustarts erforderlich sind), soll zwischen 22.00 Uhr und 5.00 Uhr erfolgen.

Die Sicherstellung dieser Verfügbarkeit muss im Informationssicherheitskonzept, dort an geeigneter Stelle, enthalten sein.

2. Möglichkeit des Erstellens von Datensicherungen

Eine Sicherung der Daten des Fachverfahrens bzw. der Fachanwendung muss jederzeit bei laufendem System und ohne wesentliche Beeinträchtigung der Nutzer möglich sein.

3. Möglichkeit des Wiederherstellens zuvor gesicherter Daten

Erforderlich ist ein Verfahren zum nachprüfbaren und vollständigen Wiederanlauf von gesicherten Datenbeständen (Restart, Recovery).

Vom Auftragnehmer/von der Auftragnehmerin sind Anforderungen an Backup und Recovery vorzulegen, welche die Mengen- und Verfügbarkeitszahlen berücksichtigen und die Rücksicherung sowohl des gesamten Datenbestandes als auch eines ausgewählten Teils vorsehen.