Anforderungen an Webanwendungen in Bezug auf die Informationssicherheit

Der Auftragnehmer hat ein ganzheitliches, sich über die gesamte IT-Infrastruktur der Webanwendung erstreckendes Informationssicherheitskonzept vorzulegen.

I. Allgemeines

Vor Inbetriebnahme der Webanwendung muss sichergestellt sein, dass während ihres 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 der Webanwendung vorzulegen. Diese Anforderungen sind vertragliche Hauptleistungspflichten des Auftragnehmers, die vom Auftraggeber abgenommen werden müssen.

II. Pflicht des Auftragnehmers 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 der Webanwendung ist daher nach BSI IT-Grundschutz und seinen Standards ein **Informationssicherheitskonzept** zu erstellen und vor Aufnahme des produktiven Betriebs der Webanwendung dem Auftraggeber zum Zwecke der Abnahme 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 zu erstellende Sicherheitskonzept bezieht sich auf die Webanwendung in ihrer Gesamtheit, vgl. hierzu Abschnitt VI.

III. Abstimmung mit dem Auftraggeber / Konzeptpapier

Das Erstellen des Sicherheitskonzeptes für die Webanwendung 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.

Da beim Auftraggeber grundsätzlich das Dokumentationssoftware „**HiScout GRC Suite**“ zur Verfügung steht, sind die Konzeptbestandteile vom Auftragnehmer zusätzlich – nach Wahl des Auftraggebers – (1.) mit Erfassungswerkzeugen dieser Software zu erfassen oder (2.) als Datei in einem mit diesem Tool kompatiblen Format bereitzustellen.

V. Kosten für das Informationssicherheitskonzept

Kosten für das zu erstellende Informationssicherheitskonzept sind im Angebot gesondert auszuweisen.

VI. Geltungsbereich des Informationsverbundes

Im Informationssicherheitskonzept müssen **sämtliche Funktionalitäten der Webanwendung** betrachten werden. Vorliegend besteht die Webanwendung aus einer modularen KI-Voicebot-Lösung, mit der ein KI-Voicebot auf dem Fachwebportal www.wirtschaft-digital-bw.de betrieben werden soll. Daher müssen neben der Webanwendung selbst auch deren Schnittstellen zum o. g. Fachwebportal, Reporting- und Trackingfunktionen sowie alle weiteren gegebenenfalls geplanten bzw. verfügbaren Funktionalitäten sicherheitsbetrachtet werden. Dabei 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 (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.

Da über die vorliegende Webanwendung personenbezogene Daten in Form des gesprochenen Wortes verarbeitet (insbesondere übertragen und automatisiert ausgewertet) werden, bedarf es vor allem hinsichtlich dieser Verarbeitungsvorgänge einer hinreichend dokumentierten Sicherheitsarchitektur.

Es müssen geeignete technische und organisatorische Maßnahmen umgesetzt und dokumentiert werden, sodass eine sichere, datenschutzkonforme und zuverlässige Nutzung all dieser Funktionalitäten ununterbrochen gewährleistet ist.

VII. Behandlung von Sicherheitsvorfällen

Sicherheitsvorfälle müssen so schnell als möglich dem Auftraggeber gemeldet und vom Auftragnehmer 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 des Auftragnehmers 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.

Die Webanwendung muss durch Authentifizierungsmechanismen verhindern, dass Unbefugte auf die Anwendung 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

Die Webanwendung 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.

Die Webanwendung muss so entworfen sein, dass ein verlässlicher Betrieb gewährleistet ist. Sicherheitsvorfälle müssen so schnell als möglich behoben werden (vgl. oben). 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 der Webanwendung 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 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.

X. Urheberrechte, Nutzungsrechte und Verwertungsrechte

1. Der Auftragnehmer räumt dem Auftraggeber an seinen Arbeits- und Leistungsergebnissen, namentlich dem Informationssicherheitskonzept einschließlich seiner Entwurfsfassungen – jeweils zum Zeitpunkt des Entstehens, spätestens des Erwerbs – das räumlich, zeitlich und inhaltlich unbeschränkte, ausschließliche, unwiderrufliche, frei auf Dritte übertragbare Recht zur Nutzung für sämtliche derzeit bekannten und zukünftig bekanntwerdenden Nutzungsarten, insbesondere zu deren Vervielfältigung, Verwertung, Bearbeitung sowie Verwertung der bearbeiten Werke, ein.

2. Zieht der Auftragnehmer zur Vertragserfüllung Unterauftragnehmer oder Dritte heran, wird er deren Urhebernutzungsrechte für den Auftraggeber in dem der Rechteeinräumung nach vorherigem Absatz X. 1. entsprechenden Umfang erwerben und im gleichen Umfang auf den Auftraggeber übertragen.

3. Die Übertragung der Nutzungsrechte ist mit den Kosten im Sinne des Abschnitts V. (siehe oben) abgegolten.

4. Der Auftragnehmer stellt den Auftraggeber von der Haftung gegenüber Dritten wegen Urheberrechtsverletzungen frei, sofern und soweit diese im Zusammenhang mit Arbeits- und Leistungsergebnissen nach obigen Absätzen X. 1. und X. 2. stehen.