

Vorgaben aus IT-Sicht für eine Content Bibliothek

26-08945

Inhalt

Vorgaben aus IT-Sicht für eine Content Library	1
Allgemeine Vorgaben zu Anwendungen.....	2
Integrationsfähigkeit in Portale und Workflows.....	2
Qualitätssicherung	3
Vorgaben zu Clients	3
Allgemeine Vorgaben für Clients.....	3
Vorgaben zum Datenschutz	3
Hosting - Auswertung gesammelter Daten nur mit TK-Auftrag	3
Keine Datenübermittlung an Dritte	3
Vorgaben zur Ergonomie.....	3
Barrierefreiheit für interne Anwendungen.....	3
Vorgaben zur IT-Sicherheit.....	4
Benutzerrechte für den Betrieb von Anwendungen	4
Eindeutige Authentifizierung	4
Freiheit von Schadsoftware.....	4
Hosting - Administrationsrechte und Funktionstrennung	4
Hosting - Sicherheitsmaßnahmen	4
Hosting nur mit Sicherheitskonzepten.....	4
Identity und Access Management	5
Meldung von Sicherheitsvorfällen	5
Nutzung von Cookies in Webanwendungen.....	5
Patch- und Release-Management (allgemeine Vorgaben).....	5
Transport Layer Security (TLS).....	6
Transportverschlüsselung nicht-öffentlicher Daten.....	6
Überprüfung von Eingaben	6
Vorgaben für öffentlich erreichbare Webanwendungen.....	6
Wahl von Verschlüsselungsverfahren und Cipher-Suites	6
Vorgaben zu Webclients	6
Lauffähigkeit auf aktuellen Browsern	6
Vorgaben für Webclients (allgemein)	7

Allgemeine Vorgaben zu Anwendungen

Integrationsfähigkeit in Portale und Workflows

Alle wesentlichen Funktionen der Anwendung müssen über eine API und/oder eine URL aufrufbar sein. Eine API soll als REST-API mit der Unterstützung von standardisierten Sicherheits-Mechanismen zur Autorisierung ausgestaltet sein. Ein Aufruf per URL soll über Standardbrowser mit standardisierten Sicherheitsmechanismen möglich sein. Die API soll klar und eindeutig nach OpenAPI Standard dokumentiert sein.

Folgende Funktionen der Anwendung sind über eine API und/oder eine URL aufrufbar.

- Katalogabfrage des Lernangebots
- Abfrage der Details zu einem Lernangebot
- Abfrage der Lernerfolge eines User oder mehrere User
- Abfrage der Änderungen im Katalogs

Genauere Beschreibung der Schnittstellen befindet sich in der Leistungsbeschreibung.

Qualitätssicherung

Der AN unterzieht den Content, die Funktionalitäten und die Anwendungen einer inhaltlichen und technischen, nachhaltigen Qualitätssicherung (QS). Bei festgestellten Mängeln kann die TK Nachbesserung verlangen.

Vorgaben zu Clients

Allgemeine Vorgaben für Clients

Die Anwendung reagiert auf die Eigenschaften des jeweils benutzten Endgerätes und unterstützt eine geräteoptimierte Darstellung, die gute Lesbarkeit und einfache Navigation mit einem Minimum an Verschieben und Blättern ermöglicht (Responsive Design).

Die Validierung von Eingaben erfolgt immer serverseitig und ggf. **ergänzend** clientseitig (z.B. durch JavaScript).

Vorgaben zum Datenschutz

Hosting - Auswertung gesammelter Daten nur mit TK-Auftrag

Der Auftragnehmer gibt keine im Rahmen des Betriebes gesammelten personenbezogenen Daten an Dritte weiter oder wertet diese ohne Auftrag aus.

Keine Datenübermittlung an Dritte

Personenbezogene Daten gem. Art. 4 Nr. 1 DSGVO sowie Sozialdaten gem. § 67 Abs. 2 SGB X dürfen nicht an Dritte gem. Art. 4 Nr. 10 DSGVO übermittelt werden, sofern sich dies nicht explizit aus dem Vertrag oder einer gesetzlichen Verpflichtung nach deutschem oder europäischem Recht ergibt.

Vorgaben zur Ergonomie

Barrierefreiheit für interne Anwendungen

Das User Interface ist barrierefrei. Es unterstützt mindestens:

- Vollständige Tastaturbedienbarkeit
- Unterstützung von Screenreadern und Braille-Zeilen
- Alternativtexte für Bilder
- Bedienbarkeit auch bei Einsatz eines Skalierungsfaktors von 250% gegenüber der von der Berufsgenossenschaft empfohlenen Schriftgröße (Zeichenhöhe für Großbuchstaben in mm = Sehabstand in mm / 155; entsprechend 20-22 Bogenminuten Sehwinkel).
- Bedienbarkeit bei Einsatz der durch das Betriebssystem bereitgestellten Mittel zur erleichterten Bedienung (insbesondere die Nutzung der vom Betriebssystem vorgegebenen Standards, damit individuell angepasste Farbschemata verwendet werden können).

Vorgaben zur IT-Sicherheit

Benutzerrechte für den Betrieb von Anwendungen

Die Anwendung wird nur mit den betrieblich notwendigen Rechten betrieben. Dies bedeutet u.a.:

- Die Anwendung wird ohne administrative Rechte auf dem jeweiligen Endgerät betrieben. (Keine Verwendung von root, Administrator oder SYSTEM, keine Mitgliedschaft in den entsprechenden lokalen Gruppen)

Eindeutige Authentifizierung

Die Anwendung besitzt Verfahren für die eindeutige Authentifizierung von Anwendenden. Bei Anwendungen, die sich an TK-Mitarbeitende richten, entsprechen die Benutzernamen dem bei der TK verwendeten Schema. Das Schema wird dem Auftragnehmer durch die TK auf Anforderung bereitgestellt.

Freiheit von Schadsoftware

Alle Bestandteile des Angebots sind frei von Schadsoftware (Viren, Würmer, Backdoors usw.). Der AN stellt dies durch geeignete Maßnahmen sicher. Der AN prüft insbesondere sämtliche ausgelieferte Software vor Auslieferung mittels marktgängiger und aktueller Scanner oder mindestens gleichwertiger Technologie.

Hosting - Administrationsrechte und Funktionstrennung

Der Auftragnehmer stellt für alle für die TK bereitgestellten IT-Komponenten (Server, Dienste und Anwendungen) sicher, dass seine Mitarbeiter - insbesondere Systemadministratoren - nur die für die jeweilige Aufgabenerfüllung notwendigen Rechte besitzen. Der Auftragnehmer setzt für kritische administrative Prozesse das Vier-Augen-Prinzip um.

Hosting - Sicherheitsmaßnahmen

Der AN ergreift geeignete technische und organisatorische Maßnahmen, die einen unbefugten und missbräuchlichen Zugriff auf die Anwendungen und/oder Internetseiten, zugehörige Komponenten sowie zugehörige Daten unterbinden. Dies gilt insbesondere für die Abwehr von Bedrohungen, die die Integrität, die Verfügbarkeit und die Vertraulichkeit der Anwendung bzw. des Internetauftritts gefährden oder eine Gefährdung (z.B. durch Exploits, Malicious Software) Dritter (z.B. Besucher eines Internetauftritts) darstellen. Die getroffenen Maßnahmen entsprechen dabei dem jeweils aktuell gültigen Stand der Technik. Ferner vermeidet der AN bei der Erstellung und Pflege sowie beim Hosting generell Techniken, die bekanntermaßen hohe Sicherheitsrisiken bzw. Sicherheitslücken enthalten, welche nicht durch entsprechende flankierende Maßnahmen geschlossen werden können.

Sollten sich aufgrund neuer Erkenntnisse und Bedrohungen Lücken ergeben, so zeigt der AN diese unverzüglich der TK an und beseitigt diese durch geeignete Maßnahmen. Der AN schreibt die zugehörigen Sicherheitskonzepte fort und stellt sie der TK zur Prüfung zur Verfügung. Sofern die Maßnahmen die Verfügbarkeit der für die TK zur Verfügung gestellten Dienste beeinflussen, stimmt der AN diese mit der TK ab

Hosting nur mit Sicherheitskonzepten

Der AN dokumentiert alle von ihm ergriffenen Sicherheitsmaßnahmen in zugehörigen Sicherheitskonzepten. Vor der Produktivsetzung sowie bei wesentlichen Änderungen stellt der AN der TK die Sicherheitskonzepte zur Prüfung zur Verfügung. Die Konzepte adressieren mindestens folgende Punkte:

- Schutz vor Malware
- Systemhärtung
- Patch-Management-Prozess
- Verschlüsselung bei Datenübertragungen

- Löschverfahren
- Umgang mit Zugangsdaten und anderen sensiblen Informationen
- Rechtekonzept für Administratoren
- Umgang mit Sicherheitsvorfällen (insbesondere Erkennung, Meldung, Behebung)

Identity und Access Management

Die Anwendung ist in ein Single Sign On bei der TK integrierbar. Es wird das Entra ID bei der Anmeldung unterstützt.

Zur Authentifizierung wird folgendes Protokoll unterstützt:

- OpenID/OAuth2 über Microsoft Entra ID Enterprise Application
(siehe <https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/what-is-application-management>)

Die Anwendung verfügt über ein für den Anwendungszweck geeignetes Rollen- und Rechte-Management. Dieses stellt insbesondere sicher, dass:

- Die Rechte für administrative Tätigkeiten von den Rechten zur regulären Nutzung getrennt sind.
- Auf von der Anwendung verarbeitete Daten nur von denjenigen Mitarbeitern zugegriffen werden kann, die den Zugriff für die Erfüllung ihrer Aufgaben benötigen.

Die Rollen des Berechtigungssystems müssen vom AG Systemen aus gesteuert werden können z.B. über Entra Gruppen.

Die Anwendung muss eine SCIM 2.0 Schnittstelle zur automatischen User Provisionierung bereitstellen. Zusätzliche Felder die nicht im SCIM-Standard definiert sind aber zur Nutzung der Content Library benötigt werden sind zwischen dem AG und dem AN abzusprechen.

Meldung von Sicherheitsvorfällen

Der AN meldet der TK unverzüglich Sicherheitsvorfälle, die direkt oder indirekt den vom AN für die TK bereitgestellten Dienst betreffen. Die Meldung erfolgt an die jeweils verantwortlichen Ansprechpartner sowie an von der TK nach Zuschlag zur Verfügung gestellte E-Mailadressen. Reaktionen auf diese Vorfälle werden gemeinsam abgestimmt.

Nutzung von Cookies in Webanwendungen

Cookies, welche für serverseitiges Tracking von Loginsessions verwendet werden, erfüllen folgende Anforderungen

- Das Attribut "Expires" ist nicht gesetzt.
- Die Attribute "Secure" und "HttpOnly" sind beide gesetzt.
- Das Cookie wird bei jedem Authentisierungsvorgang neu gesetzt.
- Das Cookie wird bei Logout serverseitig invalidiert.

Patch- und Release-Management (allgemeine Vorgaben)

Die Anwendung wird regelmäßig weiterentwickelt und an neue Anforderungen angepasst. Sicherheitsrelevante Patches auf Plattform- und Datenbankebene werden spätestens 2 Wochen nach deren genereller Verfügbarkeit unterstützt. Service Packs und neue Maintenance Level auf Plattform- und Datenbankebene werden spätestens 3 Monate nach der generellen Verfügbarkeit unterstützt. Neue Releases auf Plattform- und Datenbankebene werden spätestens 12 Monate nach deren genereller Verfügbarkeit unterstützt.

Sofern Anwendungskomponenten auf Windows-Clientsystemen vorgesehen sind, unterstützen diese neue Windows-Funktionsupdates innerhalb von 6 Monaten nach genereller Verfügbarkeit.

Der AN informiert die TK selbstständig und ohne Aufforderung über neue Releasestände und Patches, idealerweise per E-Mail.

Bei Änderungen an der API muss die TK rechtzeitig vorher informiert werden.

Vorgaben zur Datenlöschung

Datenlöschung bei Clouddiensten

Bei der Verwendung von SaaS werden Storage-Komponenten (die zur persistenten Speicherung von Daten verwendet werden) bei Außerbetriebnahme einer Appliance, des Services und bei der Beendigung des Vertrages gelöscht. Die Löschung einer Speicherkomponente entspricht einer physischen Vernichtung. Die Löschung aller virtuellen Ressourcen muss in einem Protokoll dokumentiert werden. Dieses Protokoll muss der TK zur Verfügung gestellt werden. Gelöschte Speicherressourcen dürfen nicht wiederherstellbar sein.

Transport Layer Security (TLS)

Der AN hält sich bei der Wahl von TLS-Version(en) und der eingesetzten Cipher-Suites an die Empfehlungen der jeweils aktuellen Fassung der Technischen Richtlinie BSI *TR-02102-2 "Kryptographische Verfahren: Verwendung von Transport Layer Security (TLS)"* des BSI. Der Auftragnehmer stellt sicher, dass alle Kommunikationsteilnehmer mindestens eine der zulässigen Cipher-Suites unterstützen. Der AN gleicht die von ihm gewählte Konfiguration mindestens jährlich gegen die Vorgaben des BSI ab. Bei Abweichungen passt der AN die Konfiguration an, um Konformität mit der o.a. Richtlinie herzustellen.

Transportverschlüsselung nicht-öffentlicher Daten

Nicht-öffentliche Daten werden immer verschlüsselt übertragen.

Überprüfung von Eingaben

Die Anwendung bzw. die vom AN für die TK bereitgestellten Dienste prüfen alle Eingaben vor der Verarbeitung, um bspw. Buffer-Overflows und Injection-Angriffe auszuschließen.

Vorgaben für öffentlich erreichbare Webanwendungen

Eine Anwendungssitzung wird nach maximal 30 Minuten Inaktivität serverseitig beendet.

Die Anwendung setzt KEINE 3rd Party Cookies im Browser der Anwendenden.

Es werden keine Profile durch den AN erstellt. Das Surfverhalten der User (Tracking/Webanalytics) wird nicht ausgewertet.

Wahl von Verschlüsselungsverfahren und Cipher-Suites

Sofern in der Software-Verschlüsselungsalgorithmen eingesetzt werden, müssen diese zur aktuellen Fassung "BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen" konform sein. Sofern Verschlüsselungsalgorithmen im direkten Umfeld von qualifizierten elektronischen Signaturen nach dem bundesdeutschen Signaturgesetz eingesetzt werden, müssen sie sich nach den Veröffentlichungen der Bundesnetzagentur im Bundesanzeiger richten. Verschlüsselungsverfahren müssen vor Ablauf des genehmigten Verwendungsdatums durch aktuelle Verfahren ersetzt werden.

Vorgaben zu Webclients

Lauffähigkeit auf aktuellen Browsern

Die vom AN bereitgestellte Anwendung bzw. die bereitgestellten Internetseiten müssen von folgenden Browsern vollständig und korrekt dargestellt werden:

- Chrome, Firefox, Edge, Safari: es sind alle Versionen zu unterstützen, deren Nutzung 5% in Deutschland in Bezug auf den jeweiligen Browser überschreitet

Die Anwendung bzw. die Internetseiten sind vom AN fortlaufend mit den zu unterstützenden Browsern zu testen.

Die TK kann die Liste der zu unterstützenden Browser aktualisieren, z.B. um die Entwicklungen des Marktes zu berücksichtigen. Sie zeigt dem AN die Aktualisierung schriftlich per Fax oder Brief an. Der AN muss die Unterstützung der in der aktualisierten Liste genannten Browser binnen vier Wochen sicherstellen, sofern die neu hinzugekommenen Browser vergleichbar kompatibel mit der aktuellen HTML Spezifikation des W3C sind.

Vorgaben für Webclients (allgemein)

Für die Internetseiten und -anwendungen gelten nachstehende Anforderungen und Pflichten zu den verwendeten Sprachen und Gestaltungstechniken:

- Andere clientseitige Scriptsprachen als JavaScript sind in keinem Fall zu verwenden.
- Framesets dürfen nicht eingesetzt werden.
- Flash-Animationen und andere Plugins dürfen nicht eingesetzt werden.

Die Anwendung muss die Kommunikation mit einem WEB-Proxy grundsätzlich unterstützen. Darüber hinaus entsprechen die verwendeten Technologien und Protokolle den üblichen Internetstandards gemäß Request for Comments (RFC).