IT Pflichtenheft API Management Lösung (SaaS Teil)

25-08655

Inhalt

Vorgaben für den Betrieb

Antwortzeit

Die Anwendung muss 95% aller Anfragen in weniger als 2 Sekunden beantworten.

Für Anwendungen, bei denen die Antwort über das Internet ausgeliefert wird, kann seitens TK mit einem für die Anwendung zur verfügend stehenden/zugesicherten Bandbreitendurchsatz von 5 MBit gerechnet werden, bei einer Latenz von max. 100ms.

Auf Basis dieser Kennzahlen muss die Anwendung für die geforderten Transaktionen die entsprechenden Antwortzeiten einhalten.

Herstellersupport

Der AN hat Support mit garantierten Responsetimes zu leisten.

Die Responsetime in dem Fall, dass die Anwendung nicht zur Verfügung steht, beträgt 15 Minuten im Zeitraum Montag bis Sonntag, von 0:00 bis 24:00 Uhr.

Die Integration in die ITSM-Prozesse der TK soll für Second- und Third-Level-Support Ticket-basiert automatisierbar sein. Tickets, die beim AN zur Bearbeitung liegen, sollen durch zuständige TK-Mitarbeiter einsehbar sein.

Vorgaben zu Backup & Recovery

Die Anwendung muss die Fähigkeit zu Backup & Recovery besitzen.

Vorgaben zu Clients

Allgemeine Vorgaben für Clients

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

Eine clientseitige Validierung von Eingaben (z. B. mit JavaScript) darf nur ergänzend zu einer serverseitigen Validierung vorgenommen werden.

Vorgaben zur Datenhaltung

Gebot zentraler Datenhaltung

Die Anwendung soll Daten zentral speichern. Eine dezentrale Speicherung auf Endgeräten soll nicht erfolgen. Sofern es eine Herstellerempfehlung gibt, Daten aus Performancegründen dezentral vorzuhalten, so müssen geeignete Verfahren zur Datensicherung und zum Schutz der Daten angegeben werden.

Vorgaben zum Datenschutz

Hosting - Auswertung gesammelter Daten nur mit TK-Auftrag

Der Anbieter darf keine im Rahmen des Hostings gesammelten Daten an Dritte weitergeben oder diese ohne Auftrag auswerten.

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 muss barrierefrei sein. Es muss mindestens unterstützen:

- 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

Eindeutige Authentifizierung

Die Anwendung muss Verfahren für die eindeutige Authentifizierung von Anwendenden besitzen.

Identity und Access Management

Es muss das Microsoft Active Directory oder AzureAD bei der Anmeldung unterstützt werden.

Die Anwendung muss in ein Single Sign On bei der TK integriert werden können.

Zur Authentifizierung soll mindestens eines der folgenden Protokolle unterstützt werden:

- Kerberos
- SAML über Azure AD Enterprise Application (siehe https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-application-management)
- OAuth2 über Azure AD Enterprise Application (siehe https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-application-management)

Die Anwendung muss über ein für den Anwendungszweck geeignetes Rollen- und Rechte-Management verfügen, welches sicherstellt, dass auf personenbezogene Daten nur von denjenigen Mitarbeitern zugegriffen werden kann, die den Zugriff für die Erfüllung ihrer Aufgaben benötigen.

Meldung von Sicherheitsvorfällen

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

Nutzung von Cookies in Webanwendungen

Attribute und Präfixe müssen entsprechend der Kritikalität der Daten, welche in dem jeweiligen Cookie verarbeitet werden, angemessen gesetzt sein. Die Lifetime von Cookies muss -dem Anwendungszweck entsprechend- möglichst kurz sein. Cookies sollen nicht für die Speicherung von Daten verwendet werden, welche nur auf Clientseite verarbeitet werden. Stattdessen sollen -sofern im Client verfügbar- die dafür vorgesehenen APIs (z.B. Web Storage API) verwendet werden.

Für Cookies, welche für serverseitiges Tracking von Loginsessions verwendet werden, gelten folgende detaillierte Anforderungen:

- Das Attribut "Expires" darf nicht gesetzt sein.
- Die Attribute "Secure" und "HttpOnly" müssen gesetzt sein.
- Das Attribut "SameSite" soll auf den Wert "Strict" gesetzt sein.
- Das Attribut "Domain" soll nicht gesetzt sein.
- Das Präfix des Cookies soll "__Host-" sein.
- Das Cookie muss bei jedem Authentisierungsvorgang neu gesetzt werden.
- Das Cookie muss bei Logout serverseitig invalidiert werden.

Vorgaben für öffentlich erreichbare Webanwendungen

Eine Anwendungssitzung muss nach maximal 30 Minuten Inaktivität serverseitig beendet werden.

Der Auftragnehmer darf keine 3rd Party Cookies im Browser des Kunden setzen.

Die Einbindung von externem JavaScript Code (insb. "Pixel" und "Tags") darf ausschließlich mittels des Tag Management Systems der TK erfolgen.

Die Erstellung von Profilen und die Auswertung des Surfverhaltens der User durch den Auftragnehmer (Tracking/Webanalytics) darf nicht erfolgen. Ggf. wird die TK eine Auswertung des Surfverhaltens vornehmen wollen. In diesem Fall muss das Tag Management System der TK durch den AN eingebunden werden, auch wenn dieser keinen externen JavaScript Code verwendet. In diesem Fall muss auch das Consent Management der TK verwendet werden.

Vorgaben zur Datenlöschung

Bei der Außerbetriebnahme einer Appliance, bei Austausch von Hardware-Komponenten sowie bei der Beendigung eines Vertrages und vor der Wiederverwendung von Speichermedien durch andere Kunden des AN, müssen alle permanent speichernden Datenträger sicher vernichtet oder sicher gelöscht werden. Eine Weitergabe oder Rückgabe an Dritte, ausgenommen zur professionellen Löschung bzw. Vernichtung, darf nicht stattfinden. Der AN muss über die erfolgte Vernichtung/Löschung ein Protokoll anfertigen, aus dem hervorgeht, wann und mittels welchen Verfahrens die Datenträger vernichtet/gelöscht wurden. Der AN muss der TK das Protokoll zur Verfügung stellen.

Für Datenträger mit folgenden Kriterien muss eine Vernichtung erfolgen. Löschen ist unzulässig:

- Nicht-öffentliche Daten oder Daten mit unbekannter Klassifizierung sind unverschlüsselt/schwach verschlüsselt auf Datenträger gespeichert
- Datenträger ist defekt
- Daten der VSK "C4 – Streng geheim" sind auf Datenträger gespeichert
- USB-Sticks, Speicherkarten

Eine Vernichtung muss gemäß folgender Vorgaben oder gleich-/höherwertiger Verfahren erfolgen:

- Festplatten (HDD) VSK "C0 - Offen" und "C1 - NfD": DIN 66399-2, mindestens Stufe H-3
- Festplatten (HDD) "C2 vertraulich", "C3 - geheim": DIN 66399-2, mindestens Stufe H-4
- Festplatten (HDD) "C4 - streng geheim": DIN 66399-2, mindestens Stufe H-5
- Solid State Disks (SSD) VSK "C0 - Offen" und "C1 - NfD": DIN 66399-2, mindestens Stufe E-3
- Solid State Disks (SSD) "C2 vertraulich", "C3 - geheim": DIN 66399-2, mindestens Stufe E-4
- Solid State Disks (SSD) "C4 - streng geheim": DIN 66399-2, mindestens Stufe E-5
- Für die Vernichtung von Hybridfestplatten (SSHD), USB-Sticks und Speicherkarten gelten dieselben Anforderungen wie bei Solid State Disks

Bei allen funktionsfähigen, verschlüsselten magnetischen Datenträgern kann eine elektronische sichere Löschung durchgeführt werden. Dabei muss die Löschung auf dem gesamten Datenträger nach einem der nachfolgenden Löschverfahren erfolgen:

- C0 – Offen
    1. Löschfunktion des Laufwerks (ATA "Secure Erase")
- C1 – NfD
    1. Löschfunktion des Laufwerks (ATA "Secure Erase")
    2. DoD 5220.22-M (E) bzw. gleich-/höherwertig
    3. Löschfunktion des Laufwerks (ATA "Secure Erase")
- C2 – Vertraulich, C3 – Geheim
    1. Löschfunktion des Laufwerks (ATA "Secure Erase")
    2. DoD 5220.22-M (ECE) bzw. gleich-/höherwertig
    3. Löschfunktion des Laufwerks (ATA "Secure Erase")

- C4 - streng geheim: Eine Löschung ist nicht zulässig. Der Datenträger muss vernichtet werden.

Bei allen funktionsfähigen, verschlüsselten halbleiterbasierten Datenträgern kann eine elektronische sichere Löschung durchgeführt werden. Dabei muss die Löschung auf dem gesamten Datenträger nach einem der nachfolgenden Löschverfahren erfolgen:

- C0 - Offen bis C3 - geheim:
  - Verfahren 1:
    - Löschfunktion des Mediums (ATA-"Secure-Erase")
    - Überschreiben des gesamten Speichers
    - Löschfunktion des Mediums (ATA-"Secure-Erase")
  - oder Verfahren 2:
    - Löschen des Schlüssels für die Festplattenverschlüsselung im TPM-Chip
    - Überschreiben des gesamten Speichers
    - Löschen des Schlüssels für die Festplattenverschlüsselung im TPM-Chip
- C4 - streng geheim: Eine Löschung ist nicht zulässig. Der Datenträger muss vernichtet werden.

Zufallszahlen

Sollen Zufallszahlen in einer Anwendung verwendet werden, so müssen diese – dem Anwendungszweck entsprechend – hinreichend zufällig sein. Als Informationsquelle für zulässige Zufallszahlengeneratoren kann das Kapitel 9 "Zufallszahlengeneratoren" der aktuellen Technischen Richtlinie TR-02102-120 des BSI dienen.

Vorgaben zur Verfügbarkeit

Basisanforderungen zur Verfügbarkeit

Der AN legt die von ihm bereitgestellten Dienste und Anwendungen hochverfügbar aus. Sie müssen im Zeitraum Montag bis Sonntag, von 0:00 bis 24:00 Uhr verfügbar sein. Der AN schuldet während der Betriebszeit eine Verfügbarkeit von mindestens der Verfügbarkeitsklasse VK1 im Bezugszeitraum (Siehe EVT-IT Cloud AGBs).

Sofern das Internet verwendet wird, stellt der AN eine leistungsfähige und redundante Anbindung an den Internet-Backbone sicher.

Bei geplanten Änderungen an Systemen und Anwendungen, die zu einer Abweichung von den vereinbarten Betriebszeiten führen oder führen können, muss der AN die TK mit einem Vorlauf von einer Woche informieren. Dies kann schriftlich oder per E-Mail an den vereinbarten Ansprechpartner der TK erfolgen.

Der AN richtet seine Backup- und Recovery-Verfahren so ein, dass nach einer Störung der Dienst innerhalb von 8h wieder zur Verfügung steht. In jedem Fall darf nach einem Wiederanlauf nur ein Datenverlust des Transaktionsvolumens von maximal 10 min auftreten.

Der AN muss das Operating der TK nach Feststellung eines Fehlers und bei Beeinträchtigung des Dienstes unverzüglich per Telefon oder E-Mail informieren. Er gibt dabei die Art der Störung und die voraussichtliche Zeitdauer der Beeinträchtigung bzw. des Ausfalls an. Nach Beseitigung der Störung gibt der AN eine Entwarnung per Telefon oder E-Mail an das Operating der TK.

Die maximale Ausfallzeit - auch bei Hardware-Defekten – beträgt 8h.

Erweiterte Anforderungen an die Verfügbarkeit

Für die Überprüfung der Einhaltung des Service Level Agreements (SLA) hinsichtlich der Transaktionszeiten soll der AN der TK mind. eine entsprechende offene Schnittstelle (API) bieten, über die Antwortzeit- und Verfügbarkeitsmetriken in Intervallen von maximal 15 Minuten maschinenlesbar abgerufen werden können. Folgendes Verfahren steht dabei zur Verfügung:

- Die Anwendung bietet einen HTTPS Metricendpoint (z.B. nach Prometheus-Standard bzw. OpenTelemetry Spezifikationen) und liefert darüber detailliert Performancemetriken zu den ausgeführten Transaktionen.

Zur Überprüfung der Erreichbarkeit des Service soll der AN einen Referenzdienst bereitstellen. Der Referenzdienst simuliert das Verhalten des bereitgestellten Dienstes und muss ein sicherer Indikator für die Verfügbarkeit und Performance aller beteiligten Komponenten sein. Die Details zur Nutzung des Referenzdienstes im Rahmen des Monitoring werden zwischen TK und AN abgestimmt.

Ein Dienst gilt in einem Abfrage-Referenzintervall als nicht verfügbar, wenn entweder der Dienst nicht erreicht werden kann oder in diesem und den beiden vorhergehenden Referenzintervallen die vereinbarten Antwortzeiten nicht eingehalten wurden.

Die Anwendung soll ein automatisches Umschalten beim Schwenken von benutzten Server- und Netzwerk-Ressourcen unterstützen, ohne dass dazu manuelle Eingriffe nötig sind.

Patch- und Upgrade-Einspielungen müssen unterbrechungsfrei erfolgen können.

Der AN soll nachweisen, dass er ein funktionierendes Business Continuity Management bei sich etabliert hat und soll der TK gegenüber diesbezügliche Tests nachweisen.

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.
- Der AN setzt konsequent Cascading Style Sheets ein und gewährleistet damit die Trennung von Inhalt und Darstellung - unter Einhaltung des Corporate Design der TK.
- Die vom AN eingesetzten Stylesheets müssen entsprechend der aktuellen W3C-Konvention syntaktisch richtig sein.
- 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).