Vorgaben aus IT-Sicht (Quantitative Ad-hoc Befragungen mittels Marktforschungsplattform)

12-2025

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 3 Tage im Zeitraum von Montag bis Freitag, von 09:00 bis 17:00 Uhr.

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 zum Datenaustausch

Verfahren für den Austausch von Dateien

Die TK unterstützt für den Austausch mit externen Stellen folgende Verfahren:

- automatisierte Austauschverfahren für den Datenaustausch im Gesundheitswesen (s. "Gemeinsame Grundsätze Technik", https://www.gkv-datenaustausch.de/technische_standards_1/technische_standards.jsp)
- manueller Austausch über Cryptshare (https://webft.tk.de)
- Austausch über fest definierte S-FTP bzw. FTP-S Server bei externen Partnern.

Für Datentransfers von und zur TK müssen die unterstützten Verfahren genutzt werden.

Im Falle von Austauschverfahren für den Datenaustausch soll als Transportverschlüsselung eines der Protokolle S-FTP oder FTP-S zum Einsatz kommen.

Das gewählte Verfahren ist zwischen TK und AN zu vereinbaren und vom AN zu beschreiben.

Der Austausch von Daten zwischen dem AN und der TK muss über sichere Protokolle (z.B. S-FTP oder gleichwertig) erfolgen, sofern es sich um personenbeziehbare und/oder sensible Daten handelt.

Soweit technisch machbar und wirtschaftlich umsetzbar, sind die Verfahren des Datenaustausches im Gesundheits- und Sozialwesen über Datenannahmestellen (siehe http://www.gkv-datenaustausch.de) zu verwenden.

Für den sicheren Ad-hoc-Datenaustausch muss die durch die TK bereitgestellte Plattform cryptshare genutzt werden.

Alternativ kann die Übertragung von sensiblen Daten auch per S/MIME-verschlüsselter Mail oder über einen sicheren und mit der TK abgestimmten Dienst erfolgen.

Bei Verwendung von S-FTP bzw. FTP-S muss der Auftragnehmer den entsprechenden Server bereitstellen und betreiben.

Wenn ein Datenaustausch regelmäßig vorgesehen ist und eine automatisierte Verarbeitung erfolgen soll, sollen zur Integritäts- und Vollständigkeitskontrolle geeignete Verfahren vom AN unterstützt und eingerichtet 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

Authentifizierungsverfahren mit geheimem Wissen als Faktor

Jede Anwendung, welche sich an TK-Mitarbeitende richtet, soll an zentrale Authentifizierungsdienste angebunden werden (siehe Anforderung "Identity und Access Management"). Sofern die Anwendung eine eigene Authentifizierungskomponente implementiert, welche nicht an einen der o.g. Authentifizierungsdienste angebunden ist und bei der Authentifizierung geheimes Wissen als Faktor verwendet, gelten nachfolgende Anforderungen.

- Die Authentifizierungskomponente muss die Anzahl von Fehlversuchen wirksam begrenzen. Dies kann z.B. dadurch erreicht werden, dass ein Konto nach 10 Fehlversuchen gesperrt und nach 15 Minuten automatisch wieder entsperrt wird.
- Die Authentifizierungskomponente muss die Auswahl von trivialen Geheimnissen durch Anwendende verhindern. Dies kann durch Erzeugung des Geheimnisses mittels eines technischen Prozesses erreicht werden.
- Sofern die Authentifizierungskomponente nicht für offline Angriffe anfällig ist (z.B. Smart Cards) muss die Entropie des Geheimnisses mindestens log2(10^6) betragen. Dies kann mittels einer 6-stelligen numerischen PIN erreicht werden. Das Geheimnis soll durch einen technischen Prozess mindestens annähernd zufällig erzeugt werden. Sofern das Geheimnis durch Anwendende selbst wählbar ist, muss es mindestens 8-stellig sein sowie aus Buchstaben und einer weiteren Zeichenklasse (Sonderzeichen oder Ziffern) bestehen. Dies kann durch eine alphanumerische PIN erreicht werden.
- Sofern die Authentifizierungskomponente anfällig für offline Angriffe ist, so muss das Geheimnis mindestens 12-stellig sein. Sofern eine Maximallänge definiert ist, so muss diese mindestens 64 Stellen sein. Führende und abschließende Leerzeichen sollen verhindert werden. Dies dient der Vermeidung von Eingabefehlern. Leerzeichen innerhalb des Geheimnisses sollen erlaubt sein. Alle Zeichen der Klassen Großbuchstabe, Kleinbuchstabe, Ziffer und druckbare Sonderzeichen sollen durch Anwendende verwendbar sein. Die Verwendung von mindestens zwei der angegebenen Klassen soll erzwungen werden. Bei reduziertem Zeichensatz muss die Mindestlänge des Geheimnisses so erhöht werden, dass die Anzahl der Möglichkeiten äquivalent ist. Die Ausführung von offline Angriffen auf Geheimnisse muss mittels geeigneter Verfahren (bspw. Verwendung von Passworthashingverfahren wie PBKDF2 oder Argon2) wirksam erschwert werden.
- Sofern aus dem Geheimnis direkt kryptographisches Material abgeleitet wird, so muss seine Entropie mindestens 2^100 betragen.
- Bei einem Passwortwechsel muss das aktuelle Kennwort abgefragt werden. Es darf nicht als neues Kennwort vergebbar sein.
- Passwörter/PINs sollen mindestens einmal jährlich gewechselt werden.

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 Cookie muss bei jedem Authentisierungsvorgang neu gesetzt werden.
- Das Cookie muss bei Logout serverseitig invalidiert werden.

Prüfrechte der TK

Die TK ist berechtigt, sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim AN getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Darüber hinaus hat die TK das Recht, die Sicherheit der beteiligten Systeme und Prozesse im Rahmen von Assessments zu überprüfen. Insbesondere stimmt der AN zu, dass die TK bzw. ein von Ihr beauftragter Prüfer nach Vorankündigung eigene Penetrationstests durchführen darf.

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 Erstellung von Profilen und die Auswertung des Surfverhaltens der User durch den Auftragnehmer (Tracking/Webanalytics) darf nicht erfolgen.

Vorgaben zur Verfügbarkeit

Basisanforderungen zur Verfügbarkeit

Der AN legt die von ihm bereitgestellten Dienste und Anwendungen hochverfügbar aus. Sie müssen im Zeitraum von Montag bis Freitag, von 9:00 bis 17:00 Uhr verfügbar sein. Ihre durchschnittliche Verfügbarkeit im Jahr muss mindestens 99,7 % innerhalb der vereinbarten Betriebszeiten betragen.

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 7 Tagen wieder zur Verfügung steht. In jedem Fall darf nach einem Wiederanlauf nur ein Datenverlust des Transaktionsvolumens von maximal 7 Tagen 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 7 Tage.

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).