Anlage L1

Vorgaben aus IT-Sicht für TK-TelefonCoach

25-08497

Inhaltsverzeichnis

Vorgaben aus IT-Sicht für TK-TelefonCoach 1
- Vorgaben zu Apps 3
  - Zugekaufte Apps - allgemeine Vorgaben 3
  - Zugekaufte Apps - MASVS 4
- Vorgaben für den Betrieb 4
  - Antwortzeit 4
  - Herstellersupport 4
- Vorgaben zu Clients 5
  - Allgemeine Vorgaben für Clients 5
- Vorgaben zum Datenaustausch 5
  - Verfahren für den Austausch von Dateien 5
  - Gebot zentraler Datenhaltung 5
- Vorgaben zum Datenschutz 6
  - Hosting - Auswertung gesammelter Daten nur mit TK-Auftrag 6
- Keine Datenübermittlung an Dritte 6
- Vorgaben zur Ergonomie 6
  - Barrierefreiheit für externe Anwendungen 6
  - Barrierefreiheit für interne Anwendungen 6
- Vorgaben zur IT-Sicherheit 6
  - Eindeutige Authentifizierung 6
  - Freiheit von Schadsoftware 6
  - Identity und Access Management 6
  - Nutzung von Cookies in Webanwendungen 7
  - Überprüfung von Eingaben 7
  - Vorgaben für öffentlich erreichbare Webanwendungen 7
- Vorgaben zur Verfügbarkeit 8
  - Basisanforderungen zur Verfügbarkeit 8
  - Erweiterte Anforderungen an die Verfügbarkeit 8
- Vorgaben zu Webclients 9
  - Lauffähigkeit auf aktuellen Browsern 9
  - Vorgaben für Webclients (allgemein) 9

Vorgaben zu Apps

Zugekaufte Apps - allgemeine Vorgaben

Stores
Apps sind über die Standard-App-Stores der Plattformen Android und iOS verfügbar. Sie entsprechen den dort geltenden Richtlinien. Sie werden über den Store-Account des APP-Anbieters veröffentlicht.

Berechtigungen
Es wird dem Kunden explizit erläutert, wozu eine App Berechtigungen benötigt, sofern dies nicht offensichtlich ist. Berechtigungen, die für die Kernfunktionalität der App nicht erforderlich sind, sondern nur dem Benutzerkomfort dienen, können vom Nutzer verweigert werden. In diesem Fall steht die Kernfunktionalität der App weiterhin zur Verfügung.

Unterstützte Versionen
Apps unterstützen alle Betriebssystemversionen der jeweiligen Plattform (iOS und Android) für einen Zeitraum von mindestens 36 Monaten ab deren Veröffentlichung. Apps sollen stets auch mit den Beta-Versionen der Betriebssysteme getestet werden.

Verwendete Fremdbibliotheken
Verwendete Fremdbibliotheken sind unter Angabe der genutzten Versionen bei jedem Store-Upload zu dokumentieren.

Sicherheitsupdates für externe Bibliotheken und Frameworks müssen zeitnah integriert und die neuen App-Versionen über die Stores veröffentlicht werden.

Fremdbibliotheken müssen datensparsam konfiguriert werden.

Bedienkonzept
Apps sind intuitiv bedienbar und folgen dabei dem Bedienkonzept der jeweiligen Plattform.

Aktualisierung
Aktualisierungen von Apps erfolgen über den App-Store der jeweiligen Plattform.

Einverständniserklärung
Es wird dem Kunden explizit erläutert, welche Daten erhoben, verarbeitet und gespeichert werden. Dies schließt auch die nicht offensichtliche Datenverarbeitung wie z. B. Tracking ein. Die Verwendung dieser Daten wird dargestellt und die Erlaubnis des Kunden dazu wird eingeholt. Der Nutzer kann den Datenverwendungen, die nicht für die Kernfunktionalität der App notwendig sind, widersprechen. In diesem Fall steht die Kernfunktionalität trotzdem zur Verfügung.

Zusätzlicher Zugangsschutz bei sensiblen Daten
Wenn die App den Zugang zu sensiblen Daten ermöglicht, muss vom Nutzer ein zusätzlicher App-spezifischer Zugangsschutz eingerichtet werden können (z. B. biometrische Merkmale, Hardwaretoken oder Kennwort).

Kommunikation
Daten werden nur über TLS transportiert, die jeweiligen Empfehlungen der Plattform wie „Apple App Transport Security“ oder OkHttp.RESTRICTED_TLS müssen genutzt werden.

Lokale Speicherung von Daten
Sensible Daten dürfen nur sicher verschlüsselt lokal gespeichert werden.

Benachrichtigungen
Benachrichtigungen durch die App sollen abschaltbar sein.

Datenverbrauch
Die App geht mit dem Datenvolumen des Kunden sparsam um. Aus Sicht des Kunden muss der Verbrauch des Datenvolumens dem Zweck angemessen sein.

Stromverbrauch
Die App geht mit dem Akkuvolumen des Kunden sparsam um. Aus Sicht des Kunden muss der Stromverbrauch dem Zweck angemessen sein.

Zugekaufte Apps - MASVS

Checkliste nach Mobile Application Security Verification Standard
Der Mobile Application Security Verification Standard (MASVS, siehe https://github.com/OWASP/owasp-masvs/releases/) ist eine Community-Initiative mit dem Ziel ein Rahmenwerk von Security-Anforderungen für Design, Entwicklung und Test von mobilen Apps unter iOS und Android zu etablieren. Der MASVS legt für unterschiedliche Bedrohungslevel ("L1", "L2") sowie für Resilienz gegen Reverse Engineering und Manipulation ("R") eine Reihe von Anforderungen fest.

Der APP-Entwickler muss bei Einführung und bei jeder größeren Änderung – mindestens aber alle 24 Monate - eine Checkliste pflegen, welche Anforderungen des MASVS in der jeweils gültigen Version (siehe https://github.com/OWASP/owasp-masvs/releases/) erfüllt sind und welche noch nicht. Dazu wählt er zunächst den angemessenen Prüflevel (z. B. "L1"+"R" oder "L2") aus und begründet diese Wahl. Die Checkliste ist der Dokumentation bei jeder Version beizufügen.

Zugekaufte Apps - Vorgaben für das Backend und weitere Datenendpunkte

Einhaltung aller IT-Vorgaben
Alle IT-Vorgaben in diesem Dokument müssen auch durch das Backend und Provider von weiterem Content eingehalten werden.

Schutz gegen Missbrauch
Alle Schnittstellen des Backends und weiterer Datenendpunkte sind gegen Missbrauch geschützt, beispielsweise durch verpflichtende Authentifizierung und Verschlüsselung.

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 48 Stunden im Zeitraum von Montag bis Freitag, von 6:00 bis 22:00 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 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.

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 externe Anwendungen

Anwendungen, die für die Benutzung durch TK-Kunden oder die Allgemeinheit gedacht sind, müssen die BITV 2.0 einhalten.

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.

Freiheit von Schadsoftware

Alle Bestandteile des Angebots müssen frei von Schadsoftware (Viren, Würmer, Backdoors usw.) sein. Der AN muss dies durch geeignete Maßnahmen sicherstellen. Der AN muss insbesondere sämtliche ausgelieferte Software vor Auslieferung mittels eines marktgängigen und aktuellen Scanners oder mindestens gleichwertiger Technologie prüfen.

Identity und Access Management

Es muss das Microsoft Entra 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:

- SAML über MS Entra (siehe https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-application-management)
- OAuth2 über MS Entra (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.

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 Login-Sessions 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.

Überprüfung von Eingaben

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

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 Verfügbarkeit

Basisanforderungen zur Verfügbarkeit

Der AN legt die von ihm bereitgestellten Dienste und Anwendungen hochverfügbar aus. Sie müssen im Zeitraum von Montag bis Sonntag, von 0:00 bis 24:00 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 48 Stunden wieder zur Verfügung steht. In jedem Fall darf nach einem Wiederanlauf nur ein Datenverlust des Transaktionsvolumens von maximal 4 Stunden 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 48 Stunden.

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. Folgende Verfahren stehen dabei alternativ 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.
- Die Anwendung bzw. eine eigene Monitoringagentenkomponente unterstützt nativ die Weiterleitung von ihren eigenen Performancedaten an einen InfluxDB kompatiblen Endpoint.
- Sofern es sich um netzwerknahe Services (z. B. Printspool) handelt, ist zusätzlich möglich: Die Anwendung bietet eine SNMP-Schnittstelle, welche Abfragen via SNMP (v3) zulässt, um Performancemetriken der Anwendung aktiv auszulesen.

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 Monitorings 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.

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).