IT-Pflichtenheft API Management Lösung (On Premise Teil)

25-08655

Inhalt

Allgemeine Vorgaben zu Anwendungen

Qualitätssicherung

Der AN muss den Content, die Funktionalitäten und die Anwendungen einer inhaltlichen und technischen, nachhaltigen Qualitätssicherung (QS) unterziehen. Folgende Maßnahmen müssen durch den AN im Rahmen der QS mindestens eingesetzt werden:

- Tests inkl. Dokumentation der Testfälle und -ergebnisse
- Überprüfen von Qualitätsstandards
- Change-Management inkl. Freigabeverfahren
- Problem-Management inkl. Lösungen und Maßnahmen zur künftigen Prävention

Der AN muss im Rahmen der Auftragsdurchführung das Verfahren zur QS gegenüber der TK offen legen. Bei festgestellten Mängeln kann die TK Nachbesserung verlangen.

Vorgaben für den Betrieb

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.

Plattform-Konformität

Die Anwendung muss im RZ der TK auf folgender Plattform lauffähig sein:

- Red Hat OpenShift 4.x (aktuelles Minor-Release)

Remote-Management von Serverkomponenten

Die Serverkomponente der Anwendung muss remote administriert und konfiguriert werden können.

Der serverseitige Teil der Anwendung muss komplett ohne interaktive Eingaben über die Kommandozeile zu starten, zu stoppen und der Status abzufragen sein. Entsprechende Skripte oder Konfigurationsdateien für die vorgesehene Plattform sollen mitgeliefert werden (z. B. Deployment-Konfigurationen).

Ein Monitoring aller Serverprozesse von einem zentralen Punkt muss möglich sein.

Das Logging muss über die von der Plattform vorgegebene Logging Facility erfolgen.

Vorgaben für Installationsverfahren

Anwendungen sollen ohne Benutzerinteraktion (silent) installierbar sein.

Vorgaben zur Netzwerkkommunikation

Alle verwendeten Netzwerk-Kommunikationsprotokolle müssen gemäß den jeweils gültigen RFCs implementiert sein.

Das Produkt muss in Netzwerken, in denen IPv4-Netzwerk-Adress-Translation eingesetzt wird, integrierbar sein.

Die Netzwerk-Kommunikation des Produktes muss zwischen per Firewallsystemen getrennten Netzwerkbereichen möglich sein.

Vorgaben zum Datenschutz

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 IT-Sicherheit

Benutzerrechte für den Betrieb von Anwendungen

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

- Die Anwendung soll ohne administrative Rechte betrieben werden. (Keine Verwendung von root, Administrator oder SYSTEM, keine Mitgliedschaft in den entsprechenden lokalen Gruppen)

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.

Logging

Zugriffe auf sensible oder sozialversicherungsrechtliche Daten sowie administrative Zugriffe und das Starten von Batch-Prozessen müssen mittels Logging protokolliert werden.

Das Logging soll mittels der Logging Facility der jeweiligen Plattform (bspw. Windows-Eventlog, Syslog) erfolgen. Sofern die Logging Facility der jeweiligen Plattform nicht verwendet wird, müssen Logeinträge in Dateien oder Datenbanken gespeichert werden.

Logeinträge müssen maschinell auswertbar sein. Über das Format der Logeinträge muss ab Leistungsbeginn eine vollständige und verständliche Dokumentation geliefert werden.

Sämtliche Logeinträge müssen einen Zeitstempel enthalten. Der Zeitstempel muss auf der Betriebssystemzeit beruhen oder es muss anderweitig sichergestellt werden, dass die Abweichung zu einer offiziellen Zeitquelle (z. B. einem NTP-Server) weniger als 3 Sekunden beträgt.

Sofern die Logeinträge nicht in von Menschen lesbarer und verständlicher Form für Revisionszwecke vorliegen, müssen entsprechende Aufbereitungsprogramme zur Verfügung gestellt werden.

Logdaten müssen vor unberechtigten Zugriffen geschützt sein.

Eine Anbindung an ein SIEM muss möglich sein.

Patch- und Release-Management (allgemeine Vorgaben)

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

Die TK muss vom AN selbstständig und ohne Aufforderung über neue Releasestände und Patches informiert werden, idealerweise per E-Mail.

Patch Management Prozess bei Betrieb durch die TK

Sicherheitsrelevante Updates, Patches und/oder Anleitungen müssen der TK unverzüglich zur Verfügung gestellt werden.

Falls in der Leistungsbeschreibung festgelegt wird, dass das Patchmanagement durch den Auftragnehmer durchgeführt wird, müssen sicherheitsrelevante Patches spätestens 2 Wochen nach allgemeiner Verfügbarkeit eingespielt werden. Ebenso ist dann der Betrieb aller für das Patchmanagement notwendigen Komponenten (Hardware, Lizenzen) durch den Auftragnehmer zu leisten.

Falls die Anwendung für einen 7*24-Stunden-Betrieb vorgesehen ist, soll ein Einspielen von Patches und Updates ohne Unterbrechung der Anwendung erfolgen können. Wenn dies nicht möglich ist, müssen minimal notwendige Ausfallzeiten und die dafür notwendigen Prozeduren explizit angegeben werden.

Der Aufwand beim AG für das Einspielen von Patches und neuen Releases soll möglichst gering sein.

Speicherung von Kennwörtern

Eine Speicherung von Kennwörtern im Klartext darf nicht erfolgen. Kennwörter müssen mittels Kennworthashingalgorithmen wie PBKDF2 oder Argon2 oder vergleichbar sicheren Verfahren geschützt werden.

Transport Layer Security (TLS)

Der AN muss sich bei der Wahl von TLS-Version(en) und der einzusetzenden Cipher-Suites an die Empfehlungen der jeweils aktuellen Fassung der Technischen Richtlinie

"Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 2 – Verwendung von Transport Layer Security (TLS))" des BSI halten. Dabei ist sicher zu stellen, dass alle Kommunikationsteilnehmer mindestens eine der angebotenen Cipher-Suites unterstützen. Der AN muss die von ihm gewählte Konfiguration mindestens jährlich gegen die Vorgaben des BSI abgleichen und bei Bedarf anpassen.

Transportverschlüsselung nicht-öffentlicher Daten

Nicht-öffentliche Daten müssen verschlüsselt übertragen werden. Hierfür soll TLS (Transport Layer Security) verwendet werden.

Transportverschlüsselung von Zugangsdaten

Werden Zugangsdaten zur Authentifizierung verwendet, so müssen diese verschlüsselt übertragen 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.

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.

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.