Vorgaben aus IT-Sicht

25-08538

Inhalt

Vorgaben aus IT-Sicht 1
Allgemeine Vorgaben zu Anwendungen 3
Vorgaben für den Betrieb 3
Herstellersupport 3
Vorgaben zur Netzwerkkommunikation 3
Vorgaben zum Datenaustausch 3
Verfahren für den Austausch von Dateien 3
Vorgaben zum Datenschutz 3
Hosting - Auswertung gesammelter Daten nur mit TK-Auftrag 3
Keine Datenübermittlung an Dritte 3
Vorgaben zur IT-Sicherheit 4
Authentifizierungsverfahren mit geheimem Wissen als Faktor 4
Benutzerrechte für den Betrieb von Anwendungen 4
Eindeutige Authentifizierung 4
Freiheit von Schadsoftware 5
Hosting - Administrationsrechte und Funktionstrennung 5
Hosting - Sicherheitsmaßnahmen 5
Hosting nur mit Sicherheitskonzepten 5
Identity und Access Management 5
Logging 6
Meldung von Sicherheitsvorfällen 6
Patch- und Release-Management (allgemeine Vorgaben) 6
Patch Management Prozess bei gehosteten Anwendungen 7
Prüfrechte der TK 7
Speicherung von Passwörtern 7
Transport Layer Security (TLS) 7
Transportverschlüsselung nicht-öffentlicher Daten 7
Überprüfung von Eingaben 7
Vorgaben zur Datenlöschung 7
Wahl von Verschlüsselungsverfahren und Cipher-Suites 9
Sicherheitsrelevante Zufallswerte 9
Zugriff auf das Active Directory per LDAP 9
Vorgaben zur Verfügbarkeit 9
Basisanforderungen zur Verfügbarkeit 9
Erweiterte Anforderungen an die Verfügbarkeit 10

Allgemeine Vorgaben zu Anwendungen

Vorgaben für den Betrieb

Herstellersupport

Der AN leistet Support mit garantierten Responsetimes. Die Responsetime in dem Fall, dass die Anwendung nicht zur Verfügung steht, beträgt 48h im Zeitraum von Montag bis Freitag, von 5:00 bis 23:00 Uhr. Bearbeitung von Events werktags 6:00 bis 22:00 Uhr.

Vorgaben zur Netzwerkkommunikation

Alle verwendeten Netzwerk-Kommunikationsprotokolle sind gemäß den jeweils gültigen RFCs implementiert. Die Anwendung ist integrierbar in Netzwerken, in denen IPv4-Netzwerk-Adress-Translation eingesetzt wird. Die Netzwerk-Kommunikation des Produktes ist zwischen per Firewallsystemen getrennten Netzwerkbereichen möglich.

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)
- Austausch über fest definierte S-FTP bzw. FTP-S Server bei externen Partnern.
- S/MIME-gesicherte E-Mails
- Manueller Austausch über Cryptshare (https://webft.tk.de)

Für Datentransfers von und zur TK müssen die unterstützten Verfahren genutzt werden. Das gewählte Verfahren ist zwischen TK und AN zu vereinbaren und vom AN zu beschreiben. Soweit technisch machbar und wirtschaftlich umsetzbar, sind die Verfahren des Datenaustausches im Gesundheits- und Sozialwesen über Datenannahmestellen (siehe https://www.gkv-datenaustausch.de) bevorzugt zu verwenden.

Bei Verwendung von S-FTP bzw. FTP-S stellt der Auftragnehmer den entsprechenden Server bereit und betreibt diesen.

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 IT-Sicherheit

Authentifizierungsverfahren mit geheimem Wissen als Faktor

Sofern die Anwendung eine eigene Authentifizierungskomponente implementiert und bei der Authentifizierung geheimes Wissen als Faktor verwendet, gelten nachfolgende Anforderungen.

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

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 im Active Directory betrieben. (Keine Verwendung des Domänenadministrators oder Enterpriseadministrators, keine Mitgliedschaft in den entsprechenden Domain-Gruppen)
- 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 Microsoft Active Directory oder Entra ID bei der Anmeldung unterstützt.

Zur Authentifizierung wird mindestens eines der folgenden Protokolle unterstützt:

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

- SAML über Microsoft Entra ID Enterprise Application (siehe https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/what-is-application-management)
- Kerberos über Microsoft Active Directory. Dies ist jedoch NICHT zulässig für Anwendungen, die über eine HTTP-Schnittstelle angesprochen werden. In diesem Fall unterstützt die Anwendung mindestens eines der beiden anderen genannten Protokolle.

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.

Logging

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

Für das Logging wird die Logging-Facility des Betriebssystems verwendet (Linux Syslog, Windows Eventlog) oder die Logeinträge werden in Dateien oder Datenbanken gespeichert.

Logeinträge sind maschinell auswertbar. Über Format und Inhalt der Logeinträge wird ab Leistungsbeginn eine vollständige und verständliche Dokumentation geliefert.

Sämtliche Logeinträge enthalten einen Zeitstempel. Der Zeitstempel beruht auf der Betriebssystemzeit oder es wird anderweitig sichergestellt, 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, werden entsprechende Aufbereitungsprogramme zur Verfügung gestellt.

Logdaten sind vor unberechtigten Schreib- und Lesezugriffen geschützt.

Eine Anbindung an ein SIEM-System (Security Information and Event Management) ist möglich.

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.

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.

Patch Management Prozess bei gehosteten Anwendungen

Der AN gewährleistet über einen Patch-Management-Prozess, dass alle von ihm eingesetzten Systeme, Systemkomponenten und Entwicklungswerkzeuge jeweils auf einem aktuellen Versionsstand und insbesondere frei von Schwachstellen sind. Der AN stellt sicher, dass je nach Risiko für die Anwendung (bewertet durch den AN) Sicherheitspatches - innerhalb von 1-18 Arbeitstagen nach Veröffentlichung des Patches eingespielt sind. Darüber sorgt der AN für eine angemessene Härtung der Systeme.

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. Die TK ist berechtigt, regelmäßig (mindestens monatlich, höchstens täglich) oder anlassbezogen (z.B. Bekanntwerden einer über das Netzwerk ausnutzbaren Schwachstelle oder Nachverfolgung von Härtungsmaßnahmen) nichtinvasive Prüfungen wie Portscans und Aufrufe der Webschnittstellen durchzuführen. 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.

Speicherung von Passwörtern

Sofern die Anwendung eine Authentifizierungskomponente enthält, die auf Passwörtern basiert, werden die Passwörter niemals im Klartext gespeichert. Gespeicherte Passwörter sind mittels Passworthashingverfahren wie PBKDF2 oder Argon2 oder vergleichbar sicheren Verfahren geschützt.

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. Richtline 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 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.

Datenlöschung bei Datenträgern

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, werden alle permanent speichernden Datenträger sicher vernichtet oder sicher gelöscht. Eine Weitergabe oder Rückgabe an Dritte, ausgenommen zur professionellen Löschung bzw. Vernichtung, findet nicht statt. Der AN fertigt über die erfolgte Vernichtung/Löschung ein Protokoll an. Aus dem Protokoll geht hervor, wann und mittels welchen Verfahrens die Datenträger vernichtet/gelöscht wurden. Der AN stellt der TK das Protokoll zur Verfügung.

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
- Kryptographisches Material, welches in zentralen Prozessen verwendet wird (Rootschlüssel einer PKI und vergleichbar). Im weiteren Verlauf “Kryptographisches Material” genannt.
- USB-Sticks, Speicherkarten

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

- Festplatten (HDD) VSK "C0 - Offen" und "C1 - Intern": DIN 66399-2, mindestens Stufe H-3
- Festplatten (HDD) "C2 vertraulich", "C3 - streng vertraulich": DIN 66399-2, mindestens Stufe H-4
- Festplatten (HDD) "Kryptographisches Material": DIN 66399-2, mindestens Stufe H-5
- Solid State Disks (SSD) VSK "C0 - Offen" und "C1 - Intern": DIN 66399-2, mindestens Stufe E-3
- Solid State Disks (SSD) "C2 vertraulich", "C3 - streng vertraulich": DIN 66399-2, mindestens Stufe E-4
- Solid State Disks (SSD) "Kryptographisches Material": 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
  - Löschfunktion des Laufwerks (ATA "Secure Erase")
- C1 – Intern
  - Löschfunktion des Laufwerks (ATA "Secure Erase")
  - DoD 5220.22-M (E) bzw. gleich-/höherwertig
  - Löschfunktion des Laufwerks (ATA "Secure Erase")
- C2 – Vertraulich, C3 – Streng Vertraulich
  - Löschfunktion des Laufwerks (ATA "Secure Erase")
  - DoD 5220.22-M (ECE) bzw. gleich-/höherwertig
  - Löschfunktion des Laufwerks (ATA "Secure Erase")
- Kryptographisches Material: 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:

- 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

Wahl von Verschlüsselungsverfahren und Cipher-Suites

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

Sicherheitsrelevante Zufallswerte

Sollen sicherheitsrelevante Zufallswerte (z.B. Session-IDs, kryptographisches Material, Initial-PINs) in einer Anwendung verwendet werden, so müssen diese hinreichend zufällig sein. Die dafür verwendeten Zufallsgeneratoren müssen den Vorgaben aus Kapitel "Zufallszahlengeneratoren" der aktuellen Technischen Richtlinie BSI TR-02102-1 des BSI entsprechen.

Zugriff auf das Active Directory per LDAP

Zugriffe auf das Active Directory per LDAP erfolgen weder anonym noch mit Gast-Identität.

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 5:00 bis 23:00 Uhr verfügbar sein. Ihre durchschnittliche Verfügbarkeit im Jahr beträgt mindestens 99,9 % innerhalb der vereinbarten Betriebszeiten.

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, informiert der AN die TK mit einem Vorlauf von einer Woche. Dies kann schriftlich oder per E-Mail an den vereinbarten Ansprechpartner der TK erfolgen.

Der AN richtet seine eingesetzten IT-Kontinuitätslösungen so ein, dass nach einer Störung der Dienst innerhalb von 48h wieder zur Verfügung steht. In jedem Fall darf nach einem Wiederanlauf nur ein Datenverlust des Transaktionsvolumens von maximal 4h auftreten.

Der AN informiert das Network Operations Center der TK nach Feststellung eines Fehlers und bei Beeinträchtigung des Dienstes unverzüglich per Telefon oder E-Mail. 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 Network Operations Center der TK.

Die maximale Ausfallzeit - auch bei Hardware-Defekten - beträgt <Zeit aus Wiederanlaufklasse einfügen>.

Erweiterte Anforderungen an die Verfügbarkeit

Für die Überprüfung der Einhaltung des Service Level Agreements (SLA) hinsichtlich der Transaktionszeiten stellt der AN der TK mind. eine entsprechende offene Schnittstelle (API) bereit, 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 stellt der AN einen Referenzdienst bereit. 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 Auftragnehmer hat ein funktionierendes Business Continuity Management nach BSI-Standard 200-4 oder ISO 22301 BCMS bei sich etabliert.