

Leistungsbeschreibung Awareness-Plattform für die Saarländische Landesverwaltung

Ausgangslage

Bisher wurden zweistündige Online-Schulungsveranstaltungen im Vortragsformat zur Sensibilisierung im Bereich der Informationssicherheit der Beschäftigten der Saarländischen Landesverwaltung (SL) angeboten und durchgeführt.

Diese Maßnahme soll durch eine anzuschaffende Awareness-Plattform ersetzt werden.

Die Awarenessformate müssen durch Inhalt und Aufmachung überzeugen und das Interesse und die Neugier der Beschäftigten wecken. Diese sollten durch niedrigschwellige Angebote (insbesondere was die Dauer betrifft, Stichwort microlearnings und gamification) aber auch zeitlich unabhängige Formate (E-Learnings anstelle von Veranstaltungs- und Schulungsformaten) erreicht werden.

Größtes Einfallstor für Cyberangriffe sind weiterhin E-Mails, so dass auch im Themengebiet Phishingmails auf zeitgemäße und weitestgehend automatisierte Angebote gesetzt werden soll. Diese sollten in Verbindung mit den Lerninhalten in Kampagnenform zur Verfügung gestellt und aufwandsarm durchgeführt werden können.

Gegenstand und Zweck des Auftrags

Gegenstand des Auftrags ist die Bereitstellung und der zeitlich befristete Betrieb einer Awareness-Plattform mit den Modulen E-Learnings und Phishingsimulation, nebst ergänzender Dienstleistungen.

Die Awareness-Plattform soll die Beschäftigten der Auftraggeber (AG) für das Thema Informationssicherheit und die Gefahren externer Cyber-Angriffe verstärkt sensibilisieren. Die Plattform selbst, sämtliche E-Learning-Module und Phishing-Templates sind in deutscher Sprache bereitzustellen und es existiert keine zwingende Anforderung zur Mehrsprachigkeit (Multi-Language-Support).

Mit der Awareness-Plattform verbunden ist die Funktion des Reportings/Analytics, um datengesteuert zielgruppengerechte Maßnahmen durchführen und den Erfolg messen zu können. Ziel ist es dabei, den Auftraggeber in die Lage zu versetzen, über einzelne und kombinierte Auswertungsmöglichkeiten von Phishing-Kampagnen und absolvierte E-Learnings festzustellen, wie der Wissensstand zum Thema Informationssicherheit bei den Beschäftigten ist, auf Basis der Ergebnisse gezielte Vorschläge für Lerninhalte zu unterbreiten, zu messen wie die Lerninhalte absolviert wurden und schließlich welchen Effekt das Absolvieren der Lerninhalte auf die wiederholte Durchführung der Phishing-Kampagne hat. Mit inhaltlich fundierten und motivierend aufbereiteten Lerninhalten soll das Interesse bei den Beschäftigten geweckt werden, sich mit diesem Thema gerne beschäftigen zu wollen und präventiv der häufig etwas naiv vorherrschenden „Ich falle da nicht drauf rein“-Haltung entgegenwirken zu können.

1. Anforderungen an den technischen Betrieb

1.1. Clienttechnologie

1.1.1. Webbrowser

1.1.1.1. Der clientseitige Zugriff auf die IT-Awareness-Plattform muss über einen Browser Client (hier mindestens die aktuellen Versionen Edge und Chrome) möglich sein.

1.1.2. Client-Betriebssystemvoraussetzungen

1.1.2.1. Es muss mindestens folgendes Client-Betriebssystem unterstützt werden: Windows Version 11 Enterprise und höher.

1.2. Plattformtechnologie

1.2.1. Die Module Phishing und E-Learning müssen eigenständig betreib- und nutzbar sein. Phishing-Kampagnen sind ohne vorheriges oder nachfolgendes E-Learning durchführbar. Die Nutzung des E-Learnings muss ohne vorherige oder nachgelagerte Durchführung einer Phishing-Kampagne möglich sein.

1.2.2. Das Phishingmodul muss dabei komplett eigenständig vom Anbieter (AN) auf einer von ihm gestellten technischen Plattform betrieben werden. Die inhaltlich fachliche Steuerung der Phishing-Kampagnen muss in Abstimmung mit den AG durchgeführt werden.

Die Lösung muss skalierbar und gegebenenfalls auf weitere optionale Mandanten (Ebenen) erweiterbar sein.

1.2.3. Die Lösung muss eine Anbindung an den Active Directory Service (AD) des jeweiligen AG oder eine Importfunktion für die Übermittlung der Userdaten enthalten. Dabei müssen die Informationen zur Zuweisung der User an die Jeweilige Organisationseinheit (z. B. Zugehörigkeit zu Behörde, Abteilung) ebenfalls mit übergeben werden können. Außerdem muss auch die Möglichkeit des manuellen Importes von Usern, bspw. via CSV-Datei, bestehen.

1.2.4. Abbildbarkeit Umressortierung z. B. nach Wahlen

Der AN muss sicherstellen, dass eingerichtete Nutzerkonten auch bei organisatorischen Änderungen auf Seiten der AG, insbesondere bei Ressortumstrukturierungen Aufgabenverlagerungen, Umbenennungen, Behördenzusammenlegungen oder sonstigen internen Zuständigkeitsänderungen uneingeschränkt erhalten bleiben.

Die Funktionsfähigkeit, Zugriffsrechte und gespeicherten Daten der Nutzerkonten müssen hierbei vollständig gewährleisten sein. Eine technische Migration oder Anpassung der Kontenzuordnung muss ohne Unterbrechung des laufenden Betriebs und ohne Verlust von Daten erfolgen können. Hierdurch entstehende Anpassungen innerhalb der bestehenden Systemumgebung gelten nicht als Leistungsänderung, sofern sie sich im Rahmen der vereinbarten Nutzer- und Systemstruktur bewegen.

2. Modul Phishing

Die Awareness-Plattform muss eine Funktion für die Durchführung von Phishing-Kampagnen zur Verfügung stellen. Es müssen Phishing-Kampagnen mit künstlichen Phishingmails durchgeführt werden können, wobei diese inhaltlich unter anderem auf den Kontext der AG anpassbar sein müssen. Eine Integration der Meldefunktion (Phishing-Meldebutton) muss für die E-Mailclients Microsoft Outlook für Windows bereitgestellt werden, damit die Nutzenden des Systems in ihren Mailclients über eine entsprechende Schaltfläche einfach und intuitiv erkannte Phishing-Mails an eine zentrale oder jeweils organisationsspezifische Meldestelle der AG melden können und Feedback darüber erhalten. Vor Beginn einer Phishing-Kampagne müssen die Inhalte mit den AG abgestimmt werden.

2.1. Es muss möglich sein, Adressatengruppen zu erstellen (z.B. Zugehörigkeit zu Behörde, Abteilung). Innerhalb der Hierarchieebenen müssen Nutzergruppen (über Merkmale aus dem AD-Import) automatisch anzulegen- und steuerbar sein (z. B. Führungskräfte, IT-Fachpersonal).

- 2.2. Für die Landing Page der Phishing-Mails aus der künstlichen Phishing-Kampagne muss gelten:
 - Keine Speicherung eingegebener Daten, insbesondere von Passwörtern (Dateneingabe wird im Idealfall bereits vor Eingabe des Passworts verhindert)
 - Landing Page verweist auf Erläuterungen und Hinweise zu Phishing bzw. verweist auf die E-Learning-Inhalte
 - Möglichkeit zur individuellen Anpassung an das look&feel (Schriftart und -größe, Farbgebung der Seite und Einbinden eines Wappens/Logos) der AG
- 2.3. Die Lösung muss einen Phishing-Meldebutton beinhalten, welcher mindestens für die Microsoft Outlook-Versionen 2021 und 2024 als Add-In installierbar ist.
- 2.4. Die Lösung muss sicherstellen, dass nur E-Mails aus den Phishing-Kampagnen in das Phishingmodul des AN übertragen und geprüft, bzw. aufgelöst werden.
- 2.5. Echte Phishingmails müssen jedoch an eine zentrale Stelle des AG gemeldet werden können. Der AN sollte möglichst Erfahrungswerte zum erwarteten Bearbeitungsaufwand und zum erwartenden Mengengerüst (in Relation zur Anzahl der Gesamtuser) gemeldeter E-Mails nach Einführung des Phishingbuttons liefern.
- 2.6. Bei erkannten und über den Phishingbutton gemeldeten E-Mails aus der Phishing-Kampagne müssen allgemeine Hinweise zum Erkennen von Phishingmails an den Anwender gegeben werden, zum Beispiel über eine Landing Page.
- 2.7. Die Lösung muss eine systemseitige Unterstützung bei der Erkennung und Auswertung der via Phishingbutton gemeldeten Phishingmails bieten. Hierbei dürfen keine E-Mail-Inhalte unseren Hoheitsbereich verlassen. Die Auswertung muss lokal auf den jeweiligen Endgeräten geschehen.
- 2.8. Auswertungen der Phishing-Kampagnen
 - 2.8.1. Die Auswertungen müssen mindestens folgende Parameter erfüllen:
 - Wie viele Phishingmails wurden versandt? Ggf. an welche Gruppen oder Organisationseinheiten?
 - Wie viele Phishingmails wurden erkannt und gemeldet (via Phishingbutton)?
 - Auf wie viele mitgeschickte Links, Anhänge etc. wurde geklickt?
 - Wie viele User haben Daten (z. B. Benutzerkennungen, Passwörter oder andere sensible Informationen) eingegeben?
 - Wie viele User haben auf der Landing Page ggf. vorhandene microlearnings aufgerufen?
 - 2.8.2. Alle Auswertungen müssen anonym erfolgen. Ein Rückschluss auf einzelne User darf nicht möglich sein.
 - 2.8.3. Die Auswertungen müssen gem. den Anforderungen aus 2.10.1 für Ebene 1 über den gesamten Bereich des jeweiligen AG, Ebene 2 jeweilige Behörden inkl. ggf. nachgelagerter Organisationseinheiten und für Ebene 3 nur auf die eigene Organisationseinheit bezogen möglich sein.
 - 2.8.4. Die Auswertungen müssen exportierbar sein.
 - 2.8.5. Eine Auswertung muss in einer aufbereiteten und veränderbaren Berichtsform (z.B. Word-Dokument) erfolgen.
- 2.9. Kampagnen
 - 2.9.1. Es muss die Erstellung zielgruppenorientierter Kampagnen (z.B. nur Führungskräfte, IT-Spezialisten, aber auch bestimmte Bereiche in einer Behörde oder Organisationseinheit

- oder auf Basis von AD-Gruppen oder Import von ausgewählten Benutzergruppen) für Phishing und E-Learnings für den AG möglich und steuerbar sein.
- 2.9.2. Es muss die Möglichkeit für den Auftraggeber bestehen, mehrere und voneinander unabhängige Kampagnen parallel zu steuern.
 - 2.9.3. Zeitliche Wiederkehr: Es müssen anpassbare Frequenzen der Kampagnen für verschiedene Benutzergruppen möglich sein.
 - 2.9.4. Der Auftragnehmer muss vorgefertigte Kampagnen und Templates in allgemeiner Form und für spezielle Nutzergruppen bereithalten. Er muss während der Vertragslaufzeit jährlich eine neue zentrale und vorgefertigte Kampagne (Masterkampagne) zur Nachnutzung durch den AG bereitgestellt werden. Diese muss aus jährlich mindestens 3 neuen unterschiedlichen Phishingmails-Templates zu verschiedenen Themen bestehen und mit dem AG abgestimmt werden.
 - 2.9.5. Inhalte (z. B. eigene Phishingmails) müssen durch den Auftraggeber selbst angepasst oder erstellt werden können.
- 2.10. Rollen- und Rechtekonzept / Hierarchiestufen
- 2.10.1. Die Lösung des AN muss folgende Ebenen abbilden können:
 - Ebene 1: Übergeordneten Organisationseinheit
 - Rechte im Sinne eines Global Administrators
 - Ebene 2: Dezentrale Organisationseinheiten
 - Fachadministration für die eigene Organisationseinheit und ggf. der dazugehörigen Ebene 3
 - Ebene 3: Nachgeordnete Organisationseinheiten
 - Fachadministration nur für die eigene Organisationseinheit
 - 2.10.2. Die Zugriffe auf z.B. Auswertungen müssen differenziert und granular steuerbar sein.
 - 2.10.3. Zugriffssteuerung

Die Rollen müssen eindeutig und mit klaren Zuständigkeiten und Verantwortlichkeiten definiert sein. Die Abgrenzung zwischen den Rollen muss nachvollziehbar und anpassbar sein.

Das Rollenkonzept muss transparent, effizient und überschneidungsfrei sein.

Verschiedene Rollen mit spezifischen Berechtigungen wären zum Beispiel:

 - Administratoren
 - Auswertende
 - Kampagnengestaltende
 - Nutzende

3. Modul E-Learning

Die Awareness-Plattform muss neben dem Phishingmodul auch E-Learnings mit verschiedenen Inhalten zu Themen der Informationssicherheit und zu Themen des Datenschutzes bereitstellen.

- 3.1. Das komplette E-Learning (inkl. Planung, Durchführung und Erfolgskontrolle) muss in der Plattform des AN stattfinden. Die Auswertung der E-Learnings muss in der Plattform des AN erfolgen.
- 3.2. Lerninhalte

Die Inhalte müssen korrekt, aktuell und relevant für die Zielgruppe sein.

 - 3.2.1. Folgende Inhalte müssen mindestens in den E-Learnings der Lernplattform enthalten sein:
 - 3.2.1.1. Schulungsinhalte Informationssicherheit:
 - Grundlagen der IT-Sicherheit

- Internet und Web
 - Passwortsicherheit
 - Social Engineering
 - Schadsoftware
 - Sicherer Umgang mit Emails
 - Ransomware
 - Phishing
 - KI
- 3.2.1.2. Schulungsinhalte Datenschutz:
- Grundlagen des Datenschutzes
 - Grundprinzipien DSGVO
 - Umgang mit personenbezogenen Daten
 - Umgang mit Sensiblen Daten
- 3.2.2. Es muss eine Lernerfolgskontrolle über die vermittelten Lerninhalte bereitgestellt werden (z. B. Multiple Choice, Quizfragen o. ä.). Außerdem muss die Definition von Zielmarken (z.B. bestimmte Schulungen müssen von allen Usern absolviert werden oder es müssen mind. 80% der Wissensabfragen erreicht werden) und deren Erreichung eigenständig durch den AG möglich sein.
- 3.2.3. Die Inhalte müssen durch den AN inhaltlich kontinuierlich aktualisiert und an die Marktgegebenheiten und an aktualisierte rechtliche Gegebenheiten angepasst werden.
- 3.2.4. Es muss die Möglichkeit zur individuellen Anpassung der Plattform vorhanden sein (z.B. Logos und Anpassungen entsprechend dem Corporate Design).
- 3.2.5. Inhalte müssen durch den Auftraggeber individuell angepasst oder erstellt werden können.
- 3.2.6. Regulatorischen *bzw. organisationsspezifische Vorgaben* (z. B. *Passwortvorgaben des jeweiligen Auftraggebers*) müssen in der Plattform konfiguriert werden können. Die entsprechenden Schulungsinhalte (z. B. zum Thema Passwortsicherheit) müssen sich auf Grundlage dieser Vorgaben dynamisch anpassen lassen.
- 3.2.7. Die Plattform muss vielfältige Lernformate beinhalten. Dabei gehen wir von mindestens folgenden Kategorien aus:
- Multimedia-Inhalte (Videos, Animationen)
 - Interaktive Formate (Trainings, Games, Quiz)
 - Individualisierte Feedback-Mechanismen
- 3.2.8. Die Lerninhalte sollten logisch strukturiert sein und verschiedene Lernstile berücksichtigen:
- Visueller Lernstil (Sehen): Nutzung von Grafiken, Diagrammen, Videos und Mindmaps.
 - Auditiver Lernstil (Hören): Einbindung von Audioaufnahmen, Podcasts und Diskussionen.
 - Kinästhetischer Lernstil (Tun): Interaktive Übungen, Simulationen und praxisorientierte Aufgaben.
 - Adaptives Lernen: Inhalte sollten dynamisch an das Vorwissen und den Lernfortschritt der Teilnehmenden angepasst werden können.
 - Gamification: Gamifizierte Elemente wie Punkte, Abzeichen oder Lernwettbewerbe können die Motivation erhöhen.
 - Storytelling: Der Einsatz narrativer Elemente kann die Inhalte emotional ansprechender und einprägsamer machen.
 - Lerntransfer: Aktivitäten zur Anwendung des Gelernten in der Praxis, wie Reflexionsaufgaben oder Transferaufgaben, sollten integriert werden.

- Microlearning: Die Inhalte sollten in kurzen, leicht verdaulichen Modulen bereitgestellt werden, um den Lernprozess zu erleichtern.

3.2.9. Der AN muss Inhalte einer Musterkampagne für das Absolvieren der E-Learnings definieren.

4. Hilfsfunktionen, Schulungen und Dokumentation

- 4.1. Eine Benutzeranleitung muss im System hinterlegt und abrufbar sein.
- 4.2. Der Auftragnehmer hat in seinem Angebot beschreiben, wie in einem Bedarfsfall die Benutzerhilfe einen Nutzenden (bspw. Fachadministrator) unterstützt
- 4.3. In Abstimmung mit dem AG müssen strukturierte Schulungen für die Fachadministratoren/Informationssicherheitsbeauftragte bei Einführung der Plattform stattfinden. Die Schulungen werden während der Vertragslaufzeit im Abstand von jeweils 6 Monaten wiederholt. Die Schulungen werden als online-Schulungen durchgeführt und durch den Auftragnehmer organisiert.
- 4.4. Es muss während der kompletten Vertragslaufzeit eine nachvollziehbare elektronische Schulungsdokumentation zur Verfügung gestellt werden, welche fortlaufend (z.B. bei Änderungen nach einem Systemupdate) aktualisiert wird.

5. Einfache Bedienbarkeit und Barrierefreiheit

5.1. Einfache Bedienbarkeit

Unabhängig von dem wichtigen Kriterium der Barrierefreiheit (s. Ziffer 5.3) wird Wert gelegt auf eine einfache und intuitive Bedienbarkeit, die sich nach aktuellen Erkenntnissen der Kognitionspsychologie und der visuellen Wahrnehmung und Verarbeitung von Informationen im Rahmen von Bildschirmarbeit ausrichtet. Darüber hinaus soll die Nutzung der Plattform durch bestimmte Anwendendengruppen, die eher selten mit Plattformen arbeiten werden, durch geeignete Unterstützungsfunktionen/-features (z. B. Mouseover, Assistenzsysteme, Chatbots, o. ä.) erleichtert werden. Die Funktionen sollen dabei mit unterschiedlichen Eingabegeräten (Tastatur, Maus, Stift, Finger) genutzt werden können, um mit verschiedenen Clientgeräten effektiv und im Sinne einer „einfachen Bedienbarkeit“ arbeiten zu können.

5.2. Es ist wünschenswert, dass Module auch in leichter Sprache verfügbar sind.

5.3. Barrierefreiheit

Die Awareness-Plattform muss gemäß §§ 4, 12a SGB für Menschen mit Behinderungen in der allgemein üblichen Weise, ohne besondere Erschwernis und grundsätzlich ohne fremde Hilfe auffindbar, zugänglich und im Sinne der DIN EN ISO 9241 nutzbar sein. Dies erfordert gemäß § 3 Absatz 1 BITV 2.0, dass sie wahrnehmbar, bedienbar, verständlich und robust ist. Hierbei ist die Nutzung behinderungsbedingt notwendiger Hilfsmittel zulässig. Barrieren sind lediglich zulässig, wenn der aktuelle Stand der Technik vollumfängliche Barrierefreiheit nicht ermöglicht.

Die Barrierefreiheit der Awareness-Plattform ermöglicht eine Nutzung durch folgende Gruppen:

- Menschen ohne Sehvermögen sowie Menschen mit eingeschränktem Sehvermögen
- Menschen ohne Farbwahrnehmung sowie Menschen mit eingeschränkter Farbwahrnehmung
- Menschen ohne Hörvermögen sowie Menschen mit eingeschränktem Hörvermögen
- Menschen ohne Sprachvermögen
- Menschen mit eingeschränkter Handhabung oder Kraft
- Menschen mit eingeschränkter Reichweite
- Menschen mit Anfälligkeit durch Lichtreize (Photosensibilität)
- Menschen mit kognitiven Einschränkungen

Nähere Ausführungen sind Abschnitt 4 der DIN EN 301 549 V3.2.1 zu entnehmen.

Ihr Angebot hat alle zur Erfüllung der in der Leistungsbeschreibung enthaltenen Anforderungen an die Barrierefreiheit zu enthalten.

Die Anforderungen an die Barrierefreiheit an die IT-Lösung müssen über die gesamte Vertragslaufzeit – das heißt sowohl über die Laufzeit einer Rahmenvereinbarung als auch über die Laufzeit eines jeden Einzelabrufs – erfüllt werden

6. Datenschutz und Informationssicherheit

6.1. Datenschutz und Informationssicherheit

DSGVO-Konformität muss gegeben sein. Die Datenverarbeitung muss zu 100 % DSGVO konform stattfinden.

Die jeweiligen AN müssen sicherstellen, dass die Plattform die Anforderungen hinsichtlich Informationssicherheit und Datenschutz vollständig erfüllt. Dazu muss der AN eine Übersicht der konkreten Maßnahmen, die getroffen wurden, um die DSGVO-Konformität zu gewährleisten, zuliefern. Damit ist auch eine Verfahrensdokumentation gemeint, aus der Datenschutz und IT-Sicherheits-Konzepte hervorgehen oder die dazu verwendet werden kann, eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen. Es ist darzulegen, wie die Plattform den Grundsatz nach BSI (Bundesamt für Sicherheit in der Informationstechnik) oder gleichwertig (z. B. ISO/IEC 27001, Anforderungskatalog Cloud Computing (C5), Cloud Controls Matrix der Cloud Security Alliance) umsetzt.

Für den Schutz der persönlichen Daten muss ein Privacy by Design Ansatz gewährleistet sein. Hierbei geht es um die spezifischen Maßnahmen, die innerhalb der Plattform ergriffen werden, um den Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen sicherzustellen. Dazu gehören Anonymisierungs- und Pseudonymisierungstechniken, die Minimierung der Datenerhebung und strenge Zugriffskontrollen.

Der AN muss eine Übersicht über jegliche Standorte zu liefern, an denen die Daten der jeweiligen AG verarbeitet werden. Dies umfasst auch eventuell eingesetzte Subunternehmer und insbesondere eine Zusicherung, dass die Datenverarbeitung ausschließlich innerhalb der

EU stattfindet, um die DSGVO-Konformität sicherzustellen. Die Rechenzentren sollten BSI- oder gleichwertig (z.B. ISO 27001-Norm) zertifiziert sein.

Die Verarbeitung von Daten des Auftraggebers durch den Auftragsnehmer muss innerhalb der EU und dem EWR erfolgen. Die Verarbeitung von Metadaten im Sinne des Anforderungskataloges C 5 (in Version 2020: OPS 11) ist unabhängig von Satz 1 nach dessen Maßgabe möglich, soweit die dort geforderten Maßnahmen zur sicheren Handhabung der Metadaten tatsächlich umgesetzt sind; für personenbezogene Metadaten gelten die Regelungen zur Verarbeitung personenbezogener Daten vorrangig. Rein technische Serviceleistungen von außerhalb der EU/des EWR, für die sichergestellt ist, dass kein Zugriff auf personenbezogene Metadaten oder personenbezogene Daten i.S.d. DSGVO erfolgen kann, dürfen erfolgen. Der Auftragnehmer führt eine laufende Liste der Standorte der Leistungserbringung, die als Anlage 6 zum Vertrag genommen wird. Er wird den Auftraggeber über eine Änderung der Leistungsstandorte unverzüglich schriftlich oder per E-Mail zu benachrichtigen.

6.2. Informationssicherheit zum Cloudbetrieb

Eine sichere Verschlüsselung von Daten, insbesondere bei der Übertragung, muss gewährleistet werden. Es müssen auf Seiten des AN regelmäßige Backups erstellt werden, um Datenverluste zu vermeiden. Um auf Ausfälle vorbereitet zu sein, sollten Notfallpläne vorliegen, die im Ernstfall greifen können.

Durch die kontinuierliche Überwachung der Cloud-Dienste und die Einhaltung der vereinbarten Standards bleibt die Nutzung nicht nur sicher, sondern auch effizient. So kann gewährleistet werden, dass die Cloud-Lösung den Anforderungen des Betreibers und den geltenden Regelungen entspricht.

7. Systemservice

7.3 Der Auftragnehmer erbringt einen Systemservice, der die Wiederherstellung der Betriebsbereitschaft im Falle von Störungen (Störungsbeseitigung) umfasst, die Aufrechterhaltung der Betriebsbereitschaft durch vorbeugende Maßnahmen (Wartung) und die Überlassung von neuen, verfügbaren Programmständen der eingesetzten Software.

7.4 Der Auftragnehmer ist jedenfalls von Montag bis Freitag von 09.00 Uhr bis 17.00 Uhr (ausgenommen gesetzliche Feiertage am Erfüllungsort) für Störungsmeldungen und Serviceanfragen telefonisch und per E-Mail erreichbar und erbringt während dieser Zeit Serviceleistungen (Servicezeit).

7.5 Es werden folgende Reaktionszeiten vereinbart:

- Für allgemeine Anfragen: zwei Werktage
- Im Falle von Störungen (z.B. wenn die Plattform nur eingeschränkt zugänglich ist): ein Werktag

7.7 Zur Wartung gehören alle zur Vermeidung zukünftiger Störungen erforderliche Maßnahmen des Auftragnehmers am System oder an Systemkomponenten. Dies umfasst insbesondere die Überlassung von fehlerbeseitigenden Programmständen der Software.

- 7.10 Sofern das System über einen Fernzugriff verfügt, darf dieser vom Auftragnehmer ausschließlich zum Zwecke des Systemservice genutzt werden. Der Auftragnehmer verpflichtet sich, die ihm ggf. mitgeteilten Zugangsdaten und Informationen zur Nutzung des Fernzugriffs gemäß den Anforderungen des Vertrags vertraulich zu behandeln.
- 7.11 Die Störungsbeseitigung erfasst erforderlichenfalls auch Vor-Ort-Maßnahmen. Sollte zur Beseitigung von Störungen oder sonstige Systemserviceleistungen eine Vor-Ort-Unterstützung notwendig werden, so ist der AG unverzüglich darüber zu informieren.