

Infinigate Security Awareness Services

Leistungsbeschreibung

Version	Date	Amends	Author
V2.0	01-08-2026		Christian Ederer

Content

1.	Kurzbeschreibung	4
2.	Leistungsumfang.....	4
2.1	Security Awareness Plattform – Servicemodelle.....	4
2.2	Security Awareness Plattform – Optionen.....	5
2.2.1	Managed Customization	5
2.2.2	Premium Content	5
2.3	Weitere Projektbausteine	6
2.3.1	Onboarding Workshop	6
2.3.2	Live-Workshop Management.....	6
2.3.3	Live-Workshop Technik	6
2.3.4	Awareness Basic und Kompakt.....	7
2.3.5	Vertiefungsmodule	7
2.3.6	Awareness Sprechstunde	7
2.3.7	Targeted Phishing Premium	8
2.3.8	KI-Awareness Training	8
2.4	Einschränkungen & Ausschlüsse.....	8
3.	Voraussetzungen & Rahmenbedingungen.....	9
3.1	Vertragspartner	9
3.2	Unmittelbare Mitwirkungspflichten.....	9
3.3	Empfohlene organisatorische und technische Mitwirkung	9
4.	Inbetriebnahme & Bereitstellung	10
4.1	Beauftragung des Service.....	10
4.2	Onboarding	10
4.3	Vertragslaufzeit und Kündigung	10
5.	Leistungserbringung & SLA	11
5.1	Qualitäts- und Sicherheitsmanagement.....	11
5.2	Annahme & Kategorisierung von Störungen	11
5.3	Service-, Reaktions- und Entstörungszeiten	14
5.4	Verfügbarkeit & Ausfallzeit	15
5.5	Wartungsfenster	15

5.6	Zeitangaben	16
5.7	Sprache	16
5.8	Weitere Leistungen	16
6.	Allgemeinregelungen.....	16

1. Kurzbeschreibung

Diese Leistungsbeschreibung regelt die individuellen Leistungen des im Dokument bezeichneten Service und ergänzt damit das Rahmenwerk der Allgemeinen Servicebedingungen, in denen für alle Services grundlegende Themen einheitlich geregelt werden.

Infinigate Security Awareness ist ein Managed Service zur nachhaltigen Sensibilisierung von Mitarbeitenden gegenüber Cyberbedrohungen, insbesondere Phishing und Social Engineering.

Der Service kombiniert eine Cloud-Plattform (Technologie von Keepnet, Tenant-Betrieb und -Verwaltung durch Infinigate bzw. den Kunden je nach Servicemodell) mit Live-Trainings, Workshops und der persönlichen Begleitung durch zertifizierte Security Awareness Koordinatoren.

Ziel ist die Schaffung, Erhaltung und nachhaltige Steigerung der Security Awareness bei jedem einzelnen Mitarbeitenden im Unternehmen. Der Service unterstützt Kunden dabei, Nachweispflichten zu Mitarbeiter-Sensibilisierung im Rahmen von NIS2, DORA und vergleichbaren Regularien zu erfüllen.

Der Service dient der Sensibilisierung und ersetzt keine technischen Schutzmaßnahmen (z. B. Firewalls, E-Mail-Security, EDR). Eine vollständige Verhaltensänderung oder ein absoluter Schutz vor erfolgreichen Angriffen wird nicht gewährleistet.

2. Leistungsumfang

2.1 Security Awareness Plattform - Servicemodelle

Die „Infinigate Security Awareness Plattform“ steht in zwei Servicemodellen zur Auswahl. Leitfrage für die Auswahl: Verfügen Sie als Reseller über eigene Ressourcen und das Know-How für den Plattformbetrieb oder soll Infinigate den Betrieb vollständig übernehmen?

Merkmal	Self-Serviced	Managed Awareness Service
Bereitstellung des Tenants	durch Infinigate	durch Infinigate
Nutzeranlage und -verwaltung	durch den Kunden	durch Infinigate
Kampagnenverwaltung	durch den Kunden	durch Infinigate
Regelmäßiges Ausrollen der Lerninhalte	durch den Kunden	durch Infinigate

Durchführung von Phishing-Kampagnen	durch den Kunden	durch Infinigate
Kickoff-Meeting	–	inklusive
Reporting	Standard-Reporting (Selbstausswertung)	monatliches Reporting durch Infinigate
Empfehlung für	Kunden mit eigener IT / Awareness-Ressourcen	Kunden ohne eigene Security-Ressourcen

Beide Servicemodelle werden in Preisstaffeln abhängig von der Anzahl der gebuchten User abgerechnet; die jeweils aktuellen Staffeln sind der Preisliste zu entnehmen.

Die Staffelermittlung erfolgt modellabhängig unterschiedlich. Beim Servicemodell Self-Serviced werden die User-Lizenzen aller Endkunden eines Resellers kumuliert und die Staffel auf dieser Grundlage ermittelt. Beim Servicemodell Managed Awareness Service erfolgt keine Kumulierung auf Reseller-Ebene; die Staffel wird je Endkunde einzeln ermittelt, da der Management-Aufwand pro Endkunde und nicht pro Reseller anfällt.

2.2 Security Awareness Plattform - Optionen

Zusätzlich zu den oben beschriebenen Servicemodellen können folgende Erweiterungen dauerhaft hinzugebucht werden.

2.2.1 Managed Customization

Bei Buchung dieser Erweiterung erfolgt ein noch individuelleres, direkt auf den Kunden zugeschnittenes Kampagnen-Management mit monatlich situationsbedingt angepassten Lerninhalten und monatlich individualisierter Phishing-Kampagne.

Optional wird ein monatliches Review-Meeting mit dem Kunden durchgeführt, in dem ein Austausch über den aktuellen Stand sowie die Planung der nächsten Monate erfolgen kann.

Auf Wunsch ergänzt um eine jährliche Smishing- und/oder Vishing-Kampagne.

2.2.2 Premium Content

Die User erhalten Zugriff auf exklusive Video-Inhalte mit hohem Wiedererkennungswert der Infinigate Awareness Koordinatoren, die in den regelmäßigen Lernplan eingebaut werden.

Durch diese abwechslungsreichen und erfrischend präsentieren Lerninhalte kann ein noch besserer

Lernfortschritt erzielt werden.

2.3 Weitere Projektbausteine

Die folgenden Bausteine sind Einzelleistungen ohne Dauerschuldverhältnis. Sie werden je Beauftragung separat abgerechnet und unterliegen keiner Mindestlaufzeit.

2.3.1 Onboarding Workshop

Empfohlen für einen optimalen Start im Self-Serviced-Modell. Halbtägige Einführung in die Plattform für bis zu vier Personen durch zertifizierte Security Awareness Koordinatoren.

Die Inhalte gehen dabei weit über die reine Administration der Plattform hinaus und behandeln zusätzlich den Aufbau nachhaltiger Awareness-Kampagnen, die Aktivierung von Nutzern, die Grundlagen der Phishing-Simulation.

2.3.2 Live-Workshop Management

Interaktives, auf den entsprechenden Kunden zugeschnittener Workshop; inklusive digitalem Footprinting light zur individuellen Vorbereitung. Zwei Stunden Vortrag plus zwei Stunden Workshop für die Führungsebene eines Unternehmens.

Inhalte sind unter anderem:

- Sicherheitskultur und Reifegrade – wo steht Ihr Unternehmen?
- Sicherheit ist Führungsaufgabe – Verantwortung übernehmen, unterstützen, planen, delegieren, kontrollieren, steuern
- Der Weg ist das Ziel – Sicherheit ist kein Projekt, sondern ein Prozess – Nachhaltigkeit mit Kampagne
- Wie Mitarbeiter zur Gefahr werden – Fahrlässigkeit und Vorsatz – Konflikte managen

2.3.3 Live-Workshop Technik

Interaktives, auf den entsprechenden Kunden zugeschnittener Workshop; inklusive digitalem Footprinting light zur individuellen Vorbereitung. Zwei Stunden Vortrag plus zwei Stunden Workshop speziell für die IT-Abteilung.

Inhalte sind unter anderem:

- Angriffe rechtzeitig erkennen und richtig reagieren

- Miteinander reden – aber richtig
- Menschliche Fehler in der IT-Abteilung
- Wie Angreifer sich durch ein Unternehmen hacken
- Erkennung, Eindämmung, Abwehr
- Die Meldekette
- Know your assets – know your risks – plan your actions.
- Ein Notfall ohne Plan endet im Desaster

2.3.4 Awareness Basic und Kompakt

Grundagentraining für alle Mitarbeitenden zu gängigen Angriffstechniken (Social Engineering, Identitätsdiebstahl, mobiles Arbeiten, Perimetersicherheit u. a.), wahlweise als 90-minütiges Kompaktformat oder vierstündiges Intensivformat. Empfohlene Gruppengröße: maximal 20 Teilnehmende.

Inhalte unter anderem:

- Was ist Security Awareness
- Gründe für IT-Angriffe
- Identitäten & sichere Passwörter
- Aufbau von Mails und Erkennung bösartiger Mails
- sichere Nutzung des Internets
- Social Engineering erkennen und vermeiden
- mobiles Arbeiten und zugehörige Risiken
- gezielte Angriffe erkennen
- eventuelle Maßnahmen einleiten

2.3.5 Vertiefungsmodule

Bei den Vertiefungsmodulen handelt es sich um Live-Elemente, die wahlweise vor Ort (empfohlen) oder online vermittelt werden können.

Jeweils 90-minütige Vertiefung einzelner Themen mit Live-Demonstrationen und interaktivem Austausch, u. a. Phishing-Erkennung, Passwörter & Identitäten, mobiles Arbeiten, Social Engineering.

2.3.6 Awareness Sprechstunde

Offene Fragerunde von bis zu einer Stunde je Termin, in der Mitarbeitende sich mit einem Awareness

Koordinator zu individuellen Fragen austauschen können.

2.3.7 Targeted Phishing Premium

Einzel-Aktion in Form einer individuell auf die aktuelle Situation des Kunden zugeschnittenen Phishing-Kampagne, von der einfachen Massenmail bis zum auf einzelne Benutzer zugeschnittenen Targeted Attack, inklusive Auswertung und Ableitung von Folgemaßnahmen.

2.3.8 KI-Awareness Training

Halbtägiger Online-Workshop zum sicheren und verantwortungsvollen Umgang mit Künstlicher Intelligenz im Arbeitsalltag.

2.4 Einschränkungen & Ausschlüsse

Der Service ersetzt keine technischen Sicherheitslösungen (z. B. Firewalls, E-Mail-Security, EDR), sondern ergänzt das IT-Security-Gesamtkonzept um die Sensibilisierung der Mitarbeitenden als zusätzlichen Baustein.

Trotz hoher Sorgfalt kann Infinigate weder eine vollständige Verhaltensänderung der Mitarbeitenden noch eine lückenlose Erkennung sämtlicher simulierter oder realer Angriffe zusichern.

Phishing-Simulationen werden ausschließlich auf eigenen, durch den Kunden verifizierten Domains durchgeführt. Für die Durchführung ist die vorherige Freigabe des Kampagnen-Konzepts durch den Kunden erforderlich (siehe Ziffer 3.2).

Die Plattform wird durch den Subunternehmer Keepnet auf Microsoft-Azure-Rechenzentren im Vereinigten Königreich betrieben. Die Verarbeitung personenbezogener Daten erfolgt auf Grundlage des Angemessenheitsbeschlusses der EU-Kommission für das Vereinigte Königreich (Art. 45 DSGVO).

Infinigate Security Awareness erhebt und wertet unter anderem individuelles Klick- und Meldeverhalten bei simulierten Phishing-Kampagnen sowie Trainingsfortschritte aus. Diese Daten dienen ausschließlich der Sensibilisierung und der Kampagnensteuerung; eine Leistungsbeurteilung einzelner Mitarbeitender durch Infinigate erfolgt nicht. Die Einbindung der zuständigen betrieblichen Mitbestimmung und des Datenschutzbeauftragten vor Kampagnenstart obliegt dem Kunden (siehe Ziffer 3.3).

Infinigate haftet nicht für Schäden, die durch unterlassene oder verspätete Maßnahmen auf Kundenseite entstehen.

Eine Überschreitung einzelner Reaktionszeiten oder Verfügbarkeitswerte stellt keinen Mangel dar, sofern die Abweichung unerheblich ist und den Gesamtzweck der Leistung nicht wesentlich beeinträchtigt.

3. Voraussetzungen & Rahmenbedingungen

3.1 Vertragspartner

Vertragspartner und Rechnungsempfänger ist stets der Reseller; ein direkter Erwerb von Infinigate Security Awareness durch Endkunden ist nicht möglich.

Zur Erbringung des Service nutzt Infinigate die von der Keepnet Labs Ltd. betriebene und gehostete Cloud-Plattform als Subunternehmer; die Verwaltung des Kunden-Tenants erfolgt durch Infinigate bzw. je nach Servicemodell durch den Kunden selbst. Ein eigenständiges Vertragsverhältnis zwischen Keepnet und dem Reseller oder dem Endkunden kommt dabei nicht zustande. Vertragspartner ist in der gesamten Kette (Endkunde – Reseller – Infinigate – Keepnet) ausschließlich die jeweils vorgelagerte Vertragspartei; dies gilt in gleicher Weise für etwaige Auftragsverarbeitungsverträge (AVV).

3.2 Unmittelbare Mitwirkungspflichten

Damit Infinigate Security Awareness ordnungsgemäß und effektiv erbracht werden kann, sind seitens des Kunden folgende Mitwirkungspflichten erforderlich:

- Bereitstellung einer aktuellen Liste der zu schulenden Mitarbeitenden bzw. der für die Nutzerverwaltung erforderlichen Daten.
- Benennung eigener, verifizierter Domains für die Durchführung von Phishing-Simulationen; die Nutzung fremder oder nicht verifizierter Domains ist ausgeschlossen.
- Vorherige Freigabe des jeweiligen Kampagnen-Konzepts (Inhalte, Zeitraum, Zielgruppe) vor Durchführung einer Phishing-, Smishing- oder Vishing-Simulation.
- Benennung eines Ansprechpartners für den Service beim Reseller bzw. beim Kunden.

3.3 Empfohlene organisatorische und technische Mitwirkung

Darüber hinaus trägt der Kunde durch folgende Maßnahmen wesentlich zur Effektivität und Akzeptanz des Service bei:

- Einbindung der zuständigen betrieblichen Mitbestimmung (z. B. Betriebsrat), soweit vorhanden, vor Start individualisierter Phishing-, Smishing- oder Vishing-Kampagnen, da hierbei

Verhaltens- und Leistungsdaten einzelner Mitarbeitender erhoben werden können.

- Abstimmung mit dem betrieblichen Datenschutzbeauftragten vor Kampagnenstart.
- Technisches Whitelisting der von Keepnet genutzten Domains und Absenderadressen, damit Simulationen nicht durch bestehende Schutzmaßnahmen (Spamfilter, Sandboxing) blockiert werden.
- Transparente Kommunikation an die Belegschaft zum grundsätzlichen Vorgehen und Zweck der Security-Awareness-Maßnahmen.

4. Inbetriebnahme & Bereitstellung

4.1 Beauftragung des Service

Für die Beauftragung von Infinigate Security Awareness reicht eine schriftliche Bestellung an den zuständigen Vertriebsmitarbeiter oder unsere TechServices Abteilung (techservices@infinigate.de) aus.

4.2 Onboarding

Beim Servicemodell Self-Serviced richtet Infinigate den Tenant ein und übergibt die Zugangsdaten an den vom Kunden benannten Ansprechpartner; die weitere Nutzerverwaltung und Kampagnensteuerung erfolgt eigenständig durch den Kunden. Der Onboarding Workshop kann optional hinzugebucht werden.

Beim Servicemodell Managed Awareness Service richtet Infinigate den Tenant ein und führt zusätzlich ein Kickoff-Meeting durch, in dem Konfiguration, Zielgruppen und der weitere Kampagnenverlauf gemeinsam mit dem Kunden festgelegt werden.

4.3 Vertragslaufzeit und Kündigung

Für die Servicemodelle gemäß Ziffer 2.1 sowie die Erweiterungen Managed Customization und Premium Content gemäß Ziffer 2.2 gilt die in den Allgemeinen Servicebedingungen geregelte Standardlaufzeit. Der Vertrag hat eine Mindestlaufzeit von 12 Monaten und verlängert sich automatisch um jeweils ein weiteres Jahr, sofern er nicht mit einer Frist von mindestens 30 Tagen zum jeweiligen Laufzeitende gekündigt wird.

Die Projektbausteine gemäß Ziffer 2.3 sind Einzelleistungen ohne Dauerschuldverhältnis; für sie gelten weder Mindestlaufzeit noch Kündigungsfrist, sie enden mit Erbringung der jeweils beauftragten Leistung.

5. Leistungserbringung & SLA

5.1 Qualitäts- und Sicherheitsmanagement

Das Qualitäts- und Sicherheitsmanagement des Auftragnehmers ist nach ISO 9001 und ISO 27001 zertifiziert und arbeitet nach definierten Prozessen, um für seine Kunden ein möglichst hohes Niveau an Qualität und Sicherheit zu realisieren. Der Subunternehmer Keepnet ist nach ISO 27001, ISO 27017, ISO 27018 und ISO/IEC 42001:2023 zertifiziert; Daten werden bei Übertragung mit TLS 1.2/1.3 und im Ruhezustand mit AES-256 verschlüsselt, der Zugriff auf die Plattform ist durch Multi-Faktor-Authentifizierung abgesichert.

Dieses Service Level Agreement (SLA) regelt die Bedingungen für die Erbringung von Support- und Betriebsleistungen im Zusammenhang mit den eingesetzten IT-Services. Es beschreibt die Verfahren zur Annahme und Klassifizierung von Störungen, definiert Reaktions- und Entstörrungszeiten, regelt den Umgang mit Ausfallzeiten sowie die Durchführung geplanter Wartungsfenster. Darüber hinaus enthält es weitere Bestimmungen zur Sicherstellung einer transparenten und verlässlichen Serviceerbringung. Dieses SLA bezieht sich auf den Betrieb der Infinigate Awareness Plattform (Servicemodelle gemäß Ziffer 2.1 sowie deren Erweiterungen gemäß Ziffer 2.2); für die Projektbausteine gemäß Ziffer 2.3 gelten die im jeweiligen Einzelauftrag vereinbarten Termine.

5.2 Annahme & Kategorisierung von Störungen

Der Auftragnehmer nimmt Störmeldungen des Kunden täglich an 24 Stunden, 365 Tage im Jahr (7x24) entgegen.

Der Service ist für den Kunden wie folgt erreichbar:

- per Ticketsystem <https://msp.infinigate.de/de/ts/list/open>
- per Mail support@infinigate.de

Störungen sollten bevorzugt über das Ticketsystem des Auftragnehmers gemeldet werden.

Jede Meldung erhält eine eindeutige Ticketnummer. Der Kunde wird über den Eingang der Meldung automatisch informiert.

Eine Bearbeitung der Tickets durch die Techniker des Auftragnehmers erfolgt innerhalb der definierten Servicezeiten; in diesen Zeiten ist auch eine telefonische Störungsannahme möglich. Alle erbrachten Leistungen werden im Ticket dokumentiert (inhaltlich und zeitlich).

Ein Incident ist eine Störung im Betriebslauf durch eine ungeplante Unterbrechung oder Verminderung

der Qualität in der Bereitstellung und Erbringung eines IT-Services. Die Incidents werden vom Kunden nach seinem Ermessen gemäß den folgenden Definitionen von Auswirkung und Dringlichkeit klassifiziert.

Die **Auswirkung** ('Impact') drückt aus, wie umfangreich der Incident ist und welcher (potentielle) Schaden durch den Incident verursacht werden kann.

Auswirkung		Beschreibung und Beispiele
1	firmenweit	• Betroffene Nutzer: Sehr viele Nutzer, nahezu alle Mitarbeiter, oder eine große externe Kundengruppe (> 500 Personen) ist betroffen und/oder kann ihre Aufgaben nicht erfüllen. • Reichweite: Gesamtes Unternehmen oder große Kundensegmente betroffen. • Geschäftsauswirkung: Geschäftskritische Prozesse stehen still, Compliance-Verstöße, Imageschäden möglich. • Finanziell/strategisch: Hohe finanzielle Verluste, direkte Gefährdung von Umsatz, Verträgen oder Reputation. • Beispiel: Der Online-Shop ist weltweit ausgefallen, kein Kunde kann einkaufen
2	Benutzergruppen	• Betroffene Nutzer: Eine mäßige Anzahl von Mitarbeitern ist betroffen und/oder kann ihre Aufgaben nicht wie vorgesehen erfüllen • Reichweite: Unternehmensweit relevante Prozesse oder zentrale Funktionen betroffen. • Geschäftsauswirkung: Spürbare Einschränkung der Effizienz, Qualität oder Kundenzufriedenheit. • Finanziell/strategisch: Messbare Einbußen bei Produktivität, Kosten oder KPIs. • Beispiel: Zentrales ERP-System verlangsamt, mehrere Abteilungen können Bestellungen nur eingeschränkt bearbeiten.
3	Einzelne User	• Betroffene Nutzer: Eine minimale Anzahl von Mitarbeitern ist betroffen und/oder kann ihre Aufgaben erfüllen, jedoch nur mit zusätzlichem Aufwand. • Reichweite: Eine Abteilung oder ein Prozess ist betroffen. • Geschäftsauswirkung: Keine oder nur leichte Beeinträchtigung der Arbeitseffizienz oder kleiner Komfortverlust. • Finanziell/strategisch: Kein oder geringer Einfluss auf Kosten oder

		Produktivität. • Beispiel: In einer Abteilung funktioniert ein internes Reporting-Tool fehlerhaft
4	Keine	• Allgemeine Fragen zu Themen, die keine Auswirkungen auf den aktuellen Betrieb haben.

Die **Dringlichkeit** ('Urgency') ist ein Maß dafür, wie schnell der Incident gelöst werden muss.

Dringlichkeit		Beschreibung
1	hoch	• Der von dem Incident verursachte Schaden nimmt schnell zu. • Die Aufgaben, die von den Mitarbeitern nicht erfüllt werden können, sind sehr zeitkritisch. • Durch schnelles Handeln kann verhindert werden, dass aus einem Minor Incident ein Major Incident wird. • Mehrere Benutzer mit VIP-Status sind betroffen.
2	mittel	• Der von dem Incident verursachte Schaden nimmt im Verlauf der Zeit substantiell zu. • Die Aufgaben, die von den Mitarbeitern nicht erfüllt werden können, sind nur mäßig zeitkritisch. • Ein einzelner Benutzer mit VIP-Status ist betroffen
3	niedrig	• Der von dem Incident verursachte Schaden nimmt im Verlauf der Zeit nur unwesentlich zu. • Die Aufgaben, die von den Mitarbeitern nicht erfüllt werden können, sind nicht zeitkritisch

Anhand dieser vom Kunden vorgenommenen Klassifizierung wird dem Ticket eine entsprechende Priorität zugewiesen, nach der es behandelt wird:

		Dringlichkeit		
		1 (hoch)	2 (mittel)	3 (niedrig)
Auswirkung	1 (firmenweit)	P1	P2	P3
	2 (Benutzergruppen)	P2	P3	P4

	3 (einzelne User)	P3	P4	P5
	4 (keine)	P5	P5	P5

5.3 Service-, Reaktions- und Entstörungszeiten

Eine Bearbeitung der Tickets durch die Techniker des Auftragnehmers erfolgt **Mo. – Fr. jeweils von 8:00 Uhr bis 18:00 Uhr**.

Reaktionszeit ist die Zeitspanne zwischen der Annahme einer Störungsmeldung und dem Beginn aktiver Bearbeitung durch den Service-Desk.

Entstörungszeit ist die Zeitspanne zwischen Annahme der Störungsmeldung im Ticketsystem des Auftragnehmers und der Wiederherstellung des Service bzw. Bereitstellung eines tragfähigen Workarounds.

Die verbindlichen Zielzeiten lauten:

Priorität	Servicezeit	Reaktionszeit Erstreaktion	Reaktionszeit Folgereaktion	Entstörungszeit
1 (kritisch)	5x10	≤ 8 Stunden	≤ 8 Stunden	entfällt*
2 (hoch)	5x10	≤ 8 Stunden	≤ 8 Stunden	entfällt*
3 (mittel)	5x10	Next Business Day	Next Business Day	entfällt*
4 (niedrig)	5x10	Next Business Day	Next Business Day	entfällt*
5 (niedrigste)	5x10	Within 2 Business Days	Within 2 Business Days	entfällt*

**) Eine garantierte Entstörungszeit kann auf Grund der bestehenden Abhängigkeiten des Infinigate Security Awareness Service von der Mitwirkung des Kunden und bei Eskalationsfällen von der des Herstellers (Keepnet) nicht final benannt werden.*

Sollte eine Entstörung innerhalb der Zielzeit nicht möglich sein, wird ein funktionaler Workaround bereitgestellt, bis die endgültige Lösung erfolgt.

Sollte es sich bei der Störung um einen Fehler in einem Produkt oder Service eines Drittherstellers handeln, ist dessen Entstörung nicht Bestandteil dieses SLAs, sondern diese wird zwischen dem Vertragspartner und dem Hersteller der Lösung nach deren Vereinbarung direkt behandelt.

Nicht im Auftragsumfang enthalten ist eine Gewährleistung der Verfügbarkeit und Performance für die Internetanbindungen und die lokale Infrastruktur der Standorte des Kunden. Diese

Gewährleistungspflicht liegt beim jeweiligen Internetprovider bzw. Netzwerkbetreiber des Kunden. Dem Auftragnehmer entstandene Kosten durch Störungen, Fehler und/oder Ausfälle der Internetleitungen oder lokalen Netzwerke in den Standorten des Kunden sind vom Vertragspartner nach den gültigen Stunden- und Spesensätzen des Auftragnehmers zu tragen.

5.4 Verfügbarkeit & Ausfallzeit

Die Verfügbarkeit beschreibt den Zeitraum, in dem alle beauftragten Dienste dem Kunden vertragsgemäß zur produktiven Nutzung zur Verfügung stehen muss. Verfügbarkeit ist die Fähigkeit des Gesamtsystems oder einzelnen Komponenten, diejenigen Aufgaben zu erfüllen, für die es/sie vorgesehen ist/sind.

Die garantierte **Serviceverfügbarkeit** beträgt im Jahresmittel **99,9 %** während der Servicezeiten.

Die Verfügbarkeit wird wie folgt berechnet:

$$\text{Verfügbarkeit pro Monat} = 100 \times \frac{\text{Servicezeit} - \text{ungeplante Ausfallzeit im Kalendermonat}}{\text{zugesagte Servicezeit im Monat}}$$

Die Zeit, in der die beauftragten Dienste nicht vertragsgemäß zur produktiven Nutzung bereitstehen, ist die Ausfallzeit. Geplante Ausfallzeiten (z. B. Wartungsarbeiten) werden dabei nicht auf die Verfügbarkeit angerechnet, sofern sie gemäß den Wartungsregelungen (siehe unten) angekündigt wurden.

5.5 Wartungsfenster

Regelmäßige, geplante Wartungsarbeiten werden durchgeführt, um die Stabilität, Sicherheit und Leistungsfähigkeit der Systeme zu gewährleisten. Diese liegen im Regelfall in der Nacht von Freitag auf Samstag und Mittwoch auf Donnerstag zwischen 20:00 und 06:00 Uhr.

Zur schnellen notwendigen Entstörung von Systemen bei akuten Problemen im Netzwerk kann der Auftragnehmer Reparaturfenster auch außerhalb der üblichen Wartungsfenster vorsehen.

Sollten von Auftragnehmer Arbeiten außerhalb der Wartungsfenster in Anspruch genommen werden müssen, so werden die betroffenen Kunden im Regelfall fünf Kalendertage im Voraus informiert. Während der Wartungszeit können die technischen Einrichtungen im notwendigen Umfang außer Betrieb genommen werden. Kritische Sicherheitsupdates können kurzfristig auch außerhalb der regulären Wartungsfenster erfolgen; in diesem Fall wird der Kunde so früh wie möglich informiert.

5.6 Zeitangaben

Alle Uhrzeiten beziehen sich auf mitteleuropäische Zeit.

Feiertage sind nur einheitliche, gesetzliche Feiertage des jeweiligen Landes, in dem die Leistungen des Auftragnehmers erbracht werden.

5.7 Sprache

Der Support des Auftragnehmers wird in deutscher und englischer Sprache erbracht.

5.8 Weitere Leistungen

Über die in dieser Leistungsbeschreibung hinausgehenden Leistung erbrachten Dienstleistungen können zu den jeweils aktuellen Stundensätzen des Auftragnehmers gemäß Preisliste abgerechnet werden. Hierbei handelt es sich um Professional Services, für die der Auftragnehmer auf Wunsch auch eine individuelle Aufwandsschätzung samt gesondertem Angebot erstellen kann.

6. Allgemeinregelungen

Es gelten die in den Allgemeinen Servicebedingungen geregelten Bestimmungen zu Rangfolge und Änderungsbefugnis.