



Infinigate External Attack Surface Management

Leistungsbeschreibung

Version	Date	Amends	Author
V1.0	01-08-2026		Christian Ederer

Content

- 1. Kurzbeschreibung4
- 2. Leistungsumfang.....4
 - 2.1 Service-Umfang.....4
 - 2.2 Onboarding 5
 - 2.3 Dashboard-Zugriff 6
 - 2.4 Kontinuierliche Überwachung externer Systeme 6
 - 2.5 Erkennung neuer Risiken und Veränderungen 6
 - 2.6 Analyse der DNS-, Mail-, Zertifikats- und Web-Infrastruktur..... 6
 - 2.7 Kontextbasierte Risikoanalyse & Priorisierung..... 7
 - 2.8 Bereitstellung, Auswertung und Benachrichtigung der Ergebnisse..... 7
 - 2.9 Einschränkungen & Ausschlüsse..... 7
- 3. Voraussetzungen & Rahmenbedingungen.....8
 - 3.1 Vertragspartner 8
 - 3.2 Unmittelbare Mitwirkungspflichten..... 8
 - 3.3 Empfohlene organisatorische und technische Mitwirkung 9
- 4. Inbetriebnahme & Bereitstellung 9
 - 4.1 Beauftragung des Service..... 9
 - 4.2 Telefonische Abstimmung/Beratung 9
 - 4.3 Vertragslaufzeit und Kündigung 10
- 5. Service Level Agreement (SLA)..... 10
 - 5.1 Qualitäts- und Sicherheitsmanagement..... 10
 - 5.2 Annahme & Kategorisierung von Störungen 10
 - 5.3 Service-, Reaktions- und Entstörungszeiten 12
 - 5.4 Verfügbarkeit & Ausfallzeit 13
 - 5.5 Wartungsfenster 14
 - 5.6 Zeitangaben 14
 - 5.7 Sprache 15
 - 5.8 Weitere Leistungen 15
- 6. Allgemeinregelungen..... 15

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.

Das Infinigate External Attack Surface Management (EASM) ist ein IT-Sicherheitsservice zur kontinuierlichen Überwachung der von außen erreichbaren Angriffsfläche eines Unternehmens. Der Service wird gemeinsam mit unserem Technologiepartner Antago erbracht.

Ziel des Service ist die frühzeitige Erkennung von Schwachstellen und Fehlkonfigurationen exponierter Systeme, Dienste und Subdomains, sowie neuer externer Risiken und sicherheitsrelevanter Veränderungen – als permanente Ergänzung zu punktuellen Prüfungen wie Penetrationstests. Die Ergebnisse werden über ein zentrales Dashboard bereitgestellt.

EASM unterstützt die Einhaltung von NIS2, ISO 27001 und DORA im Bereich Schwachstellen- und Risikomanagement. Die Leistung wird über die in Deutschland entwickelte und gehostete Antago Fusion Plattform erbracht; Serviceerbringung, Hosting und Datenhaltung erfolgen in Deutschland gemäß DSGVO.

Der Service dient ausschließlich der frühzeitigen Identifikation potenzieller externer Risiken und ersetzt keine bestehenden Schutzmaßnahmen (z. B. Firewalls, EDR, SIEM). Ein absoluter Schutz vor Cyberangriffen wird nicht gewährleistet.

2. Leistungsumfang

2.1 Service-Umfang

Das Infinigate External Attack Surface Management wird als einheitliches Service-Paket erbracht und umfasst folgende Module:

- Onboarding
- Dashboard-Zugriff (Antago Fusion Plattform)
- Kontinuierliche Überwachung externer Systeme
- Erkennung neuer Risiken und Veränderungen
- Analyse der DNS-, Mail-, Zertifikats- und Web-Infrastruktur
- Kontextbasierte Risikoanalyse & Priorisierung
- Export- und API-Schnittstellen

Verrechnungseinheit ist ein Asset, wobei ein Asset einer Domain oder einer IP-Adresse entspricht. Die angegebene Pauschale gilt pro Asset und wird monatlich abgerechnet. Maßgeblich ist die jeweils gültige Preisliste Infinigate TechServices.

2.2 Onboarding

Nach Beauftragung des Service sind folgende Informationen notwendig:

- Welche Domains und/oder IP-Adressen (Assets) sollen in die Überwachung aufgenommen werden?
- Gewünschter Beginn der Überwachung? Die Lizenzlaufzeit beginnt generell am nächsten Monatsersten; soll die Überwachung sofort beginnen, kann die Laufzeit auf Wunsch rückdatiert werden.
- Wer ist der Ansprechpartner für diesen Service beim Reseller (Vorname, Name, Mailadresse)? Dieser Ansprechpartner erhält den Zugriff auf das Dashboard für die beauftragten Assets.
- Wenn darüber hinaus weitere Personen – auf Wunsch des Partners auch beim Endkunden – Zugriff auf das Dashboard für die beauftragten Assets erhalten sollen, benötigen wir für jeden weiteren Zugang folgende Informationen: Vorname, Nachname, Mailadresse.

Der Zugriff auf das EASM Portal erfolgt über Microsoft EntraID als zentralen Identity Provider. Die Anmeldung ist durch Multi-Faktor-Authentifizierung (MFA) abgesichert. Nach erfolgreicher Authentifizierung wird die Benutzeridentität auf ein internes Authentifizierungs- und Autorisierungssystem abgebildet. Darüber werden Rollen, Berechtigungen sowie Mandanten- und Objektzuordnungen gesteuert. Auf diese Weise wird sichergestellt, dass Nutzer ausschließlich Zugriff auf die für sie vorgesehenen Inhalte und Funktionen erhalten.

Zu diesem Zeitpunkt ist für uns noch nicht relevant, ob der externe Nutzer selbst über eine Microsoft-365-Identität verfügt oder nicht. Beim anschließenden Login gibt es dann zwei Varianten für die Authentifizierung über Microsoft Entra ID:

- Nutzer mit eigenem Microsoft-365 / Azure-AD-Account: In diesem Fall authentifiziert sich der Nutzer über seinen bestehenden Tenant. Beim ersten Login erfolgt einmalig eine Freigabe, bei der der externe Tenant die Anmeldung gegenüber dem Entra-Tenant unseres Partners Antago autorisiert.
- Nutzer ohne eigenen Microsoft-365-Account: Hier wird ein dedizierter Gastaccount in dem Entra-Tenant unseres Partners Antago angelegt, ebenfalls abgesichert über Multi-Faktor-Authentifizierung.

2.3 Dashboard-Zugriff

Das Dashboard der Antago Fusion Plattform zeigt die überwachten Assets, aktuelle Funde, erkannte Veränderungen und deren Bewertung. Zudem können die Ergebnisse exportiert und – abhängig von der jeweiligen Ausprägung – über Schnittstellen (API) in bereits bestehende Systeme integriert werden.

Der Login erfolgt über die im Rahmen des Onboardings angelegten Zugänge. Der Zugriff wird nach Wunsch des Partners eingerichtet – wahlweise für den Partner, den Endkunden oder beide. Werden weitere Zugänge benötigt, können diese schriftlich bei support@infinigate.de beantragt werden. Hierbei ist die Angabe von Vorname, Nachname und Mailadresse notwendig.

Innerhalb der Plattform können alle freigeschalteten Nutzer sämtliche für die entsprechenden Assets verfügbaren Informationen einsehen.

Hinweis zur datenschutzrechtlichen Einordnung: Aus datenschutzrechtlicher Sicht ist bei der Nutzung des Infinigate External Attack Surface Management das berechtigte Interesse klar durch den Schutz der Infrastruktur sowie das Erfüllen regulatorischer Anforderungen (insbesondere NIS2 & DORA) gegeben. Wichtig ist dabei vor allem, dass keine Leistungsbeurteilung von Mitarbeitern erfolgt.

2.4 Kontinuierliche Überwachung externer Systeme

Das EASM überwacht kontinuierlich öffentlich erreichbare Systeme, Dienste und potenzielle Angriffsvektoren der externen Infrastruktur. Im Gegensatz zu punktuellen Prüfungen wird die externe Angriffsfläche fortlaufend analysiert, sodass neue Risiken zeitnah erkannt werden können, bevor diese aktiv ausgenutzt werden.

2.5 Erkennung neuer Risiken und Veränderungen

Geänderte Konfigurationen oder unerwartet erreichbare Systeme werden zeitnah erkannt und können nachvollzogen werden. So werden sicherheitsrelevante Veränderungen innerhalb der externen Infrastruktur frühzeitig sichtbar, und der Kunde erhält Transparenz über exponierte Systeme, Dienste, Subdomains und potenzielle Fehlkonfigurationen.

2.6 Analyse der DNS-, Mail-, Zertifikats- und Web-Infrastruktur

Neben klassischen Schwachstellenscans berücksichtigt das EASM zusätzlich externe Infrastrukturkomponenten wie DNS-, Mail-, Zertifikats- und Web-Infrastrukturen, um Risiken ganzheitlich sichtbar zu machen. Auch auffällige Konfigurationen, exponierte Dienste und sicherheitsrelevante Infrastrukturmerkmale werden berücksichtigt – die Sichtbarkeit geht damit über bekannte Schwachstellen hinaus.

2.7 Kontextbasierte Risikoanalyse & Priorisierung

Erkannte Findings werden technisch eingeordnet, um potenziell kritische Expositionen schneller identifizieren und priorisieren zu können. Die Analyse kombiniert KI-Technologien mit klassischem Sicherheitshandwerk und Fachwissen und unterstützt Unternehmen dabei, externe Risiken schneller zu erkennen und Sicherheitsmaßnahmen gezielter umzusetzen.

2.8 Bereitstellung, Auswertung und Benachrichtigung der Ergebnisse

Ergebnisse werden über die Antago Fusion Plattform bereitgestellt und können abhängig von der jeweiligen Ausprägung über Schnittstellen oder Exportformate weiterverarbeitet werden.

Regelmäßige Reports sowie Service-Review-Meetings sind nicht Bestandteil des Service; die Auswertung der bereitgestellten Informationen erfolgt durch den Partner bzw. den Endkunden. Weitergehende Leistungen können als Professional Services gesondert beauftragt werden.

2.9 Einschränkungen & Ausschlüsse

Der Service ersetzt keine Sicherheitslösungen (z. B. Firewalls, EDR, SIEM), sondern ergänzt das IT-Security-Gesamtkonzept um einen weiteren Baustein.

Trotz kontinuierlicher und sorgfältiger Überwachung kann keine vollständige Erkennung sämtlicher Risiken, Systeme oder Schwachstellen garantiert werden. Der Service dient der Unterstützung bei der frühzeitigen Identifikation potenzieller Risiken und ergänzt bestehende Sicherheitsmaßnahmen wie Penetrationstests und interne Sicherheitsprozesse.

Der Service basiert auf der kontinuierlichen Analyse öffentlich erreichbarer Systeme und Dienste. Abhängig von Zielsystemen, Konfigurationen und Schutzmechanismen kann es in Einzelfällen zu technischen Nebenwirkungen wie erhöhtem Logging, automatisierten Schutzmaßnahmen oder temporären Beeinträchtigungen einzelner Dienste kommen.

Die Durchführung der Analysen erfolgt ausschließlich auf Grundlage der durch den Auftraggeber bereitgestellten oder dem Auftraggeber zurechenbaren Zielsysteme, Domains und IP-Adressen. Der Auftraggeber stellt sicher, dass er zur Beauftragung der jeweiligen Prüfungen berechtigt ist. Sollten durch fehlerhafte Zuordnungen, Weiterleitungen, gemeinsam genutzte Infrastrukturen oder sonstige technische Gegebenheiten unbeabsichtigt Drittsysteme betroffen sein oder hieraus Ansprüche entstehen, werden daraus resultierende Ansprüche an den jeweiligen Auftraggeber weitergeleitet.

Der Service kann in verschiedenen Modulen personenbezogene Daten (z. B. E-Mail-Adressen in Zertifikaten oder DNS-Einträgen) anzeigen. Aus datenschutzrechtlicher Sicht ist das berechnigte Interesse klar durch den Schutz der Infrastruktur sowie das Erfüllen regulatorischer Anforderungen (insbesondere NIS2 & DORA) gegeben; wichtig ist hierbei vor allem, dass keine Leistungsbeurteilung von Mitarbeitern erfolgt.

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

Verzögerungen oder Ausfälle, die durch höhere Gewalt, Netzwerkausfälle außerhalb des Verantwortungsbereichs von Infinigate oder unvollständige/fehlerhafte Kundendaten entstehen, sind von den SLA-Verpflichtungen ausgenommen.

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 External Attack Surface Management Service durch Endkunden ist nicht möglich.

Zur Erbringung des Service bedient sich Infinigate der antago GmbH als Subunternehmer, insbesondere für Plattform, Datalake und Analystenleistungen. Ein eigenständiges Vertragsverhältnis zwischen antago und dem Reseller oder dem Endkunden kommt dabei nicht zustande. Vertragspartner ist in der gesamten Kette (Endkunde <-> Reseller <-> Infinigate <-> antago) ausschließlich die jeweils vorgelagerte Vertragspartei; dies gilt in gleicher Weise für etwaige Auftragsverarbeitungsverträge (AVV).

3.2 Unmittelbare Mitwirkungspflichten

Damit das Infinigate External Attack Surface Management (EASM) ordnungsgemäß und effektiv erbracht werden kann, sind seitens des Kunden folgende Mitwirkungspflichten erforderlich:

- Bereitstellung und Pflege einer aktuellen Liste der zu überwachenden Domains, Subdomains und IP-Adressen.
- Sicherstellung, dass die gemeldeten Assets dem eigenen Unternehmen zuzurechnen sind und die

Berechtigung zur Beauftragung der Prüfungen vorliegt.

- Umsetzung der aus den Ergebnissen abgeleiteten Maßnahmen in der eigenen Infrastruktur.
- Benennung erreichbarer Ansprechpartner für Rückfragen und Abstimmungen.

3.3 Empfohlene organisatorische und technische Mitwirkung

Darüber hinaus trägt der Kunde durch folgende Maßnahmen wesentlich zur Effektivität und Aussagekraft des EASM bei:

- Einheitliche Domain- und IP-Strategie: Konsolidierung und transparente Verwaltung der genutzten Domains, Subdomains und IP-Adressbereiche, um eine möglichst vollständige Abdeckung zu ermöglichen.
- Starke Authentifizierungsverfahren: Einsatz von Multifaktor-Authentifizierung (MFA) insbesondere für externe und privilegierte Zugänge.
- Gehärteter Perimeter: Regelmäßige Überprüfung durch Pentests und Härtung von extern erreichbaren Systemen, insbesondere Firewalls, Gateways, Webanwendungen und weiterer Endpunkte.
- Sicheres Identitäts- und Zugriffsmanagement: Härtung und kontinuierliche Prüfung des lokalen Active Directory sowie eine sichere und überwachte Anbindung an Microsoft 365 bzw. Microsoft EntraID.
- Kontinuierliche Tests & Audits: Durchführung regelmäßiger Sicherheitsüberprüfungen, um sicherzustellen, dass bekannte Schwachstellen zeitnah geschlossen werden und empfohlene Sicherheitsmaßnahmen nachhaltig umgesetzt sind.

4. Inbetriebnahme & Bereitstellung

4.1 Beauftragung des Service

Für die Beauftragung eines Infinigate External Attack Surface Management reicht eine schriftliche Bestellung an den zuständigen Vertriebsmitarbeiter oder unsere TechServices Abteilung (techservices@infinigate.de) aus.

4.2 Telefonische Abstimmung/Beratung

Anschließend nimmt ein Mitarbeiter unserer TechServices Abteilung mit dem bei der Bestellung genannten Ansprechpartner telefonisch Kontakt auf, um die Details zur Einrichtung abzusprechen. Die Abstimmung kann wahlweise mit dem Partner oder direkt mit dem Endkunden erfolgen.

Im Rahmen der telefonischen Abstimmung werden folgende Punkte festgelegt:

- Ansprechpartner und deren Kontaktdaten
- Festlegung des genauen Umfangs (Domains, IP-Adressen, Dashboard-Zugänge)
- Definition eventuell erforderlicher Vorarbeiten durch Infinigate, den Partner und den Endkunden
- Vereinbarung eines entsprechenden Termins für die Einrichtung (eine gewisse Vorlaufzeit kann notwendig sein)

Die Ergebnisse werden von Infinigate schriftlich festgehalten und an die entsprechenden Ansprechpartner übermittelt.

4.3 Vertragslaufzeit und Kündigung

Für den Infinigate EASM Service 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.

5. Service Level Agreement (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.

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 Entstörungszeiten, regelt den Umgang mit Ausfallzeiten sowie die Durchführung geplanter Wartungsfenster. Darüber hinaus enthält es weitere Bestimmungen zur Sicherstellung einer transparenten und verlässlichen Serviceerbringung.

5.2 Annahme & Kategorisierung von Störungen

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

Der Service ist für den Partner 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 Partner wird über den Eingang der Meldung automatisch informiert.

Eine Bearbeitung der Tickets durch die Techniker des Auftragnehmers erfolgt innerhalb der unter 5.3 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 Partner 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 Partner 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 Supports von der Mitwirkung des Kunden, des Partners und bei Eskalationsfällen von der des Herstellers nicht final benannt werden.*

Sollte eine Entörung 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 Entörung 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 Vertragsnehmers. Diese Gewährleistungspflicht liegt beim jeweiligen Internetprovider bzw. Netzbetreibers des Vertragsnehmers. Dem Auftragnehmer entstandene Kosten durch Störungen, Fehler und/oder Ausfälle der Internetleitungen oder lokalen Netzwerke in den Standorten des Vertragsnehmers 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 Vertragsnehmer vertragsgemäß zur produktiven Nutzung zur Verfügung stehen muss. Verfügbarkeit ist die Fähigkeit des

Gesamtsystem 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 Vertragsnehmer 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.