A1 Telekom Austria AG Lassallestraße 9, 1020 Wien

Service und Leistungsbeschreibung A1 Business Secure Gate

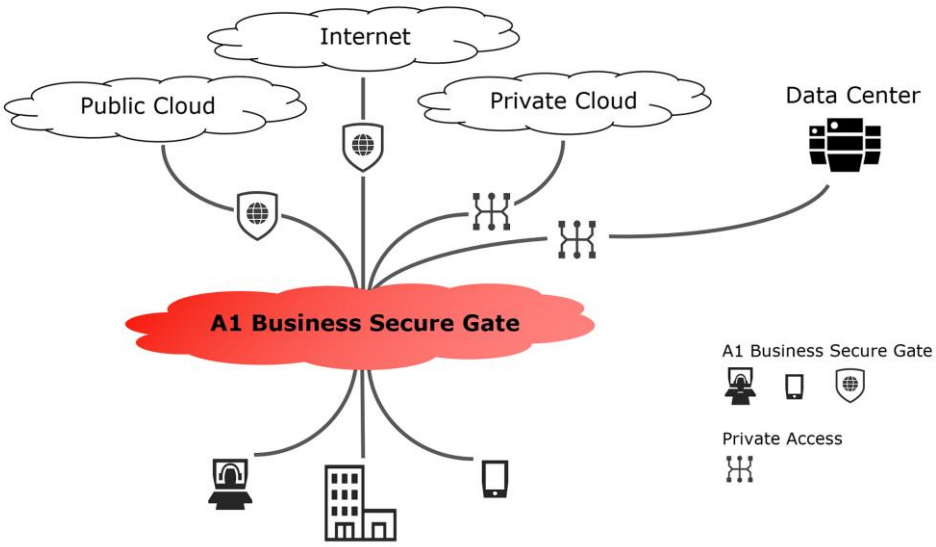
Gültig für Bestellungen ab 15.1.2026.

Inhalt

1. Einleitung

A1 Telekom Austria AG (A1) erbringt das Service „A1 Business Secure Gate" im Rahmen ihrer technischen und betrieblichen Möglichkeiten nach den Allgemeinen Geschäftsbedingungen für Solutions von A1 in der jeweils geltenden Fassung, insoweit hier keine von diesen abweichenden oder ergänzenden Regelungen getroffen werden, samt allfälligen Individualvereinbarungen. Diese Servicebeschreibung gilt für Unternehmen im Sinne von § 1 Konsumentenschutzgesetz in der geltenden Fassung.

1.1. Allgemeine Produktbeschreibung



A1 Business Secure Gate wird als skalierbare SaaS-Plattform über die weltweit größte Security Cloud von Zscaler Inc. (mit Sitz in Kalifornien, USA; im Folgenden kurz „Zscaler") bereitgestellt und ersetzt Legacy-Netzwerksicherheitslösungen mit dem Ziel, komplexe Bedrohungen abzuwehren und Datenverluste zu verhindern. Der Kunde erwirbt pro User eine Lizenz und kann damit Endgeräte und Standorte (nur Ausprägung Enterprise) vor Bedrohungen aus dem Internet schützen. Um den Cloud Service nutzen zu können muss auf jedem Endgerät die Zscaler Client Applikation oder zum Schutz eines Standortes ein geeignetes Gerät, welchen einen GRE oder IPsec Tunnel zur Zscaler Cloud aufbauen kann, installiert werden.

Kernfunktionen des „A1 Business Secure Gate "

Cloud-first-Architektur

Die Architektur unterstützt einen beschleunigten Wechsel in die Cloud. Durch Konsolidierung und Vereinfachung der Sicherheitsservices wird die IT entlastet und Spannungspotenzial abgebaut. Zscaler kombiniert Risikominderungsfunktionen in einer zentralen Plattform zum Schutz aller User innerhalb und außerhalb des Firmen-Netzwerks. Dadurch entfällt der Aufwand für die Verwaltung von Appliances und Unternehmen profitieren von niedrigeren IT-Kosten und geringerer Komplexität.

Vollständige und umfassende Inline-SSL-Überprüfung

Angesichts des heutzutage hohen Anteils an verschlüsseltem Traffic kann nur eine skalierbare Proxy-basierte Architektur einen effektiven Schutz vor Bedrohungen und Datenverlusten gewährleisten.

Private Access "Zero Trust Network Access"

Zscaler bietet einen nutzer- und anwendungszentrierten Anwendungszugriff. Als komplett in der Cloud bereitgestellter Service ermöglicht Zscaler eine native Anwendungssegmentierung. Nach erfolgreicher Authentifizierung werden User anhand unternehmensspezifischer Richtlinien direkt mit der jeweils benötigten Anwendung verbunden, ohne jemals Zugang zum Netzwerk zu erhalten.

Schnelle, konsistente Sicherheitserfahrung

Durch Bereitstellung der Schutzmechanismen in unmittelbarer User-Nähe über eine global verteilte Cloud wird ein einheitliches Sicherheitsniveau mit identischen Richtlinien sowie gleichem Bedrohungs- und Datenschutz für alle Verbindungen zwischen Usern und Anwendungen gewährleistet.

Keinerlei Angriffsoberfläche

Angreifer können nur Ressourcen ins Visier nehmen, die für sie sichtbar sind. Die Zscaler-Architektur verhindert dies, indem IP-Adressen verschleiert und Unternehmensnetzwerke sowie Ressourcen nicht im Internet offengelegt werden.

Das A1 Business Secure Gate basiert auf den Produkten Zscaler Internet Access (ZIA), Zscaler Private Access (ZPA) und/oder Zscaler Digital Experience (ZDX) von Zscaler.

Es beinhaltet eine umfassende Suite KI-gestützter Sicherheits- und Datenschutzservices zum Schutz vor Cyberangriffen und Datenverlust. Da es sich um eine vollständig in der Cloud bereitgestellte SaaS-Lösung handelt, können neue Funktionen ohne zusätzliche Hardware oder langwierige Bereitstellungszyklen hinzufügt werden.

2. Produkt Packages und Produktdetails

A1 Business Secure Gate nutzt als Basis Zscaler Internet Access (IA) und kann in drei unterschiedlichen Produkt Packages bestellt werden.

2.1. A1 Business Secure Gate - Standard

Für Kunden ab 10 User. Dieses Paket beinhaltet folgende Features:

- Authentification lokal über DB bei Zscaler oder IDP des Kunden
- Content Filtering
- Antivirus & Anti-spyware
- SSL Inspection
- Cloud Application Control
- Advanced Threat Protection
- Inline Web DLP für Internet, Saas, Private und Gen AI-Apps
- Cyber Browser Isolation Standard
- Firewall & Sandbox Standard
- Guest Wi-Fi using DNS Control
- Monitoring Preset
- 6month Logging & Reporting
- Client connector only
- Co-Management

2.2. A1 Business Secure Gate - Advanced

Für Kunden ab 10 User. Dieses Paket beinhaltet folgende Features und kann mit den Optionen Privileged Remote Access und Monitoring Advanced erweitert werden. Um Private Access verwenden zu können müssen die Voraussetzungen unter Punkt 4 erfüllt werden.

- Alle Features vom Standard Package
- Authentication mit IDP
- Monitoring Standard mit 6 Probes
- NSS Logging to SIEM (on-premises)
- Private Access User to App Access
    - Health Monitoring
    - Log Streaming Service
    - Standard Device Posture
    - Source IP Anchoring
    - Browser Access
    - 10 App Segments, 20 App Connectors
    - 14 Day Logging and Reporting (PA)

Optional:

- **Privileged Remote Access**
- **Monitoring Advanced**
- **Einrichtungspaket Advanced**

2.3. A1 Business Secure Gate - Professional

Für Kunden ab 10 User. Dieses Paket beinhaltet folgende Features und kann mit den Optionen Privileged Remote Access und Monitoring Advanced erweitert werden. Um Private Access verwenden zu können müssen die Voraussetzungen unter Punkt 4 erfüllt werden.

- Alle Features vom Advanced Package
- Firewall Advanced
- Sandbox Advanced
- Browser Isolation Advanced Plus

Optional:

- **Privileged Remote Access**
- **Monitoring Advanced**
- **Einrichtungspaket Professional**

2.4. A1 Business Secure Gate – Enterprise

Für Kunden ab 50 User. Das Paket nutzt Zscaler Internet Access (ZIA), Zscaler Private Access (ZPA) und Zscaler Digital Experience (ZDX) als Basis und wird individuell aus dem Produktkatalog von Zscaler zusammengestellt. Die jeweiligen inkludierten Features gelten laut Auftragsbestätigung.

Optional:

- **Einrichtungspaket - A1 Business Secure Gate – Enterprise**
- **Security Performance Assessment & Health Check - A1 Business Secure Gate – Enterprise**

3. Optionale Pakete

3.1. Monitoring Advanced

Mit den optionalen Lizenzen für Monitoring Advanced (mindestens 10 User Lizenzen) können bis zu 30 Anwendungen überwacht und gemonitort werden. Zusätzlich können bis zu 25 Alarm Regeln eingerichtet werden.

3.2. Privileged Remote Access

Mit dieser optionalen Lizenz (mindestens 5) können privilegierte Fernzugriffe für Administratoren und externe Partner bereitgestellt werden. Über identitäts- und kontextbasierte Zero-Trust-Policies wird ausschließlich der Zugriff auf klar definierte Anwendungen und Admin-Protokolle ermöglicht. Zielsysteme benötigen keine Agenten; interne App-Konnektoren initiieren ausgehende, verschlüsselte Verbindungen zur Zscaler-Cloud.

Dieses Paket beinhaltet folgende Features:

- Full protocol isolation für SSH, RDP und VNC, support für Interactive authentication, Clipboard controls (text copy and paste)
- Sandboxed file transfer mit Advanced Sandbox inspection (benötigt A1 Business Secure Gate -Professional – Sandbox Advanced)
- Credential Mapping & Injection, Session Sharing (Read-only)
- Session recording & playback (up to 10 hours recording/system per month)
- Emergency Access

3.3. Einrichtungspaket - A1 Business Secure Gate – Advanced

In diesem Einrichtungspaket sind folgende Leistungen inkludiert.

- Architekturworkshop
- Vorstellung der Cloudportale
- Definition der Security Policies
- App Discovery und Definition der App Segmentierung
- Gemeinsames Testen der Einstellungen
- Definition der Einstellungen des Client Connectors (Zscaler Applikation am Endgerät)
- Abnahmeprotokoll

Alle oben genannten Leistungen werden ausschließlich remote durchgeführt. Alternativ können diese Leistungen vor Ort stattfinden. Die dadurch zusätzlich anfallenden Kosten werden separat in Rechnung gestellt. In dem Einrichtungspaket A1 Business Secure Gate - Advanced sind Leistungen in der Höhe von insgesamt 15 Stunden enthalten. Sind zusätzliche Leistungen erforderlich, so werden diese separat angeboten und in Rechnung gestellt.

3.4. Einrichtungspaket - A1 Business Secure Gate – Professional

In diesem Einrichtungspaket sind folgende Leistungen inkludiert.

- Architekturworkshop
- Vorstellung der Cloudportale
- Definition der Security Policies
- App Discovery und Definition der App Segmentierung
- Gemeinsames testen der Einstellungen
- Definition der Einstellungen des Client Connectors (Zscaler Applikation am Endgerät))

- Abnahmeprotokoll

Alle oben genannten Leistungen werden ausschließlich remote durchgeführt. Alternativ können diese Leistungen vor Ort stattfinden. Die zusätzlichen anfallenden Kosten werden separat in Rechnung gestellt. In dem Einrichtungspaket A1 Business Secure Gate - Professional sind Leistungen in der Höhe von insgesamt 20 Stunden enthalten. Sind zusätzliche Leistungen erforderlich, so werden diese separat angeboten und in Rechnung gestellt.

3.5. Einrichtungspaket - A1 Business Secure Gate – Enterprise

Mit diesem Einrichtungspaket können folgende Leistungen erbracht werden.

Design:

- Architektur-Workshop
- Bedarfsanalyse
- Bestandsaufnahme
- Definition Use-Cases
- Testszenarien und -kriterien

Konfiguration/Implementierung:

- Partner-Integrationen
- Richtlinien- und Regelwerkskonfiguration
- Applikationsdefinition (Private Access only)
- Konfiguration von Infrastrukturkomponenten (Service Edge, Branch/Cloud/App Connector)

Test und Validierung:

- Funktionstests

Schulung & Dokumentation:

- Einführung in Cloudportal
- Dokumentation

Rollout:

- Rollout-Planung
- Optimierung/Feinabstimmung
- Feedback-Evaluierung
- Betriebsübergabe

Alle oben genannten Leistungen werden ausschließlich remote durchgeführt. Alternativ können diese Leistungen vor Ort stattfinden. Die dadurch zusätzlich anfallenden Kosten werden separat in Rechnung gestellt. In dem Einrichtungspaket A1 Business Secure Gate - Enterprise sind Leistungen in einem Stundenausmaß von (siehe dazugehörigem Angebot) enthalten. Sind zusätzliche Leistungen erforderlich, so werden diese separat angeboten und in Rechnung gestellt.

3.6. Security Performance Assessment & Health Check - A1 Business Secure Gate – Enterprise

Optional können pro Quartal dem Kunden anhand von Workshops Einblicke und Empfehlungen zu folgenden Kernbereichen der bestehenden A1 Business Secure Gate Lösung gegeben werden:

- Nutzungsstatistiken
- Bedrohungsanalyse
- Sicherheitsvorfälle und -maßnahmen
- Leistungskennzahlen (KPIs)
- Konfigurationsanalyse
- Best-Practice Ansätze
- Technische Fortschritte & Innovationen

Alle oben genannten Leistungen werden ausschließlich remote durchgeführt, alternativ können diese Leistungen vor Ort stattfinden. Die dadurch zusätzlich anfallenden Kosten werden separat in Rechnung gestellt. Die Workshops sind auf 2 Stunden pro Quartal begrenzt, werden zusätzliche Leistungen benötigt werden diese separat angeboten und in Rechnung gestellt.

4. Voraussetzungen

Voraussetzungen für die Nutzung von A1 Business Secure Gate sind:

- Für den Schutz der Endgeräte
  Ein installierter Zscaler Client (Client Connector) und dem dementsprechenden Zertifikat auf dem jeweiligen Endgerät (unterstütze Betriebssysteme: Windows, OSX, IOS oder Android)

- Für den Schutz eines Standortes (nur bei der Ausprägung Enterprise möglich)
  Diese dafür benötigten Einstellungen müssen kundenseitig durchgeführt werden. In Abstimmung mit dem A1 Service Techniker können diese Leistungen auch von A1 übernommen werden, diese werden separat angeboten und in Rechnung gestellt.

- Für den Zugriff auf die Management-Oberfläche
  Ein Internetzugang und ein unterstützter Web-Browser

- Für die Verwendung von Private Access (bei Ausprägung Advanced, und Professional) sowie alle Zscaler Private Access Modelle (bei Ausprägung Enterprise) müssen ein Identity Provider sowie virtuelle Ressourcen für die App Konnektoren, oder bei Verwendung von Private Service Edges sowie Cloud- und Branch Konnektoren vom Kunden bereitgestellt werden.

5. Leistungen und Abgrenzungen

5.1. Leistungsabgrenzung

- Für jeden einzelnen, namentlich genannten Benutzer ist eine Lizenz für die Benützung des Services erforderlich, sollte es zu einer Diskrepanz zwischen erworbenen Lizenzen und der Anzahl der tatsächlichen Benutzer kommen, werden die Lizenzen für die Differenz nachbestellt und nachverrechnet.

- Der Kunde ist für den Download sowie für die Installation des Zscaler Client (Client Connector) verantwortlich. A1 kann keinen Support der dafür benötigten Hard- und Software anbieten.

- Durch die Nutzung des Services können einige Online-Dienste in Folge der Sicherheitseinstellungen nicht oder nur eingeschränkt genutzt werden. Werden dafür kundenindividuelle Sicherheitseinstellungen benötigt so können diese über unser Service Portal eingemeldet werden und je nach Aufwand werden diese Anpassungen (siehe Punkt 6) in Rechnung gestellt.

- Logdaten werden innerhalb des Services für die dort festgelegte Zeit gespeichert. Es besteht die Möglichkeit, die Logdaten zur weiteren Auswertung und längerfristigen Speicherung an einem anderen Ort zu speichern. Dieser Speicher ist nicht Teil des Services. Rechtliche Rahmenbedingungen, insbesondere zum Schutz personenbezogener Daten, sind dabei vom Kunden zu beachten.

- Die Pakete A1 Business Secure Gate – Standard, Advanced und Professional werden mit Private Service Edges im A1 Datencenter realisiert. Werden Public Service Edges (weltweite öffentliche Datencenter von Zscaler) benötigt können zusätzliche Kosten durch den verursachten Datentraffic (1 GB pro User und Monat inkludiert) nachverrechnet werden. Das Datenvolumen ist als Datenpool zu verstehen welches sich mit der Anzahl der User jeweils um 1 GB erhöht.

- Bei Private Access im Paket Advanced und Professional inkludiert, (wird standardmäßig mit Public Service Edges in Zscaler Datencentern realisiert) ist ein maximales Datenvolumen von 3 GB pro User und Monat inkludiert, zusätzlich benötigtes Datenvolumen kann nachverrechnet werden. Das Datenvolumen ist als Datenpool zu verstehen, welches sich mit der Anzahl der User jeweils um 3 GB erhöht.

- Im Paket A1 Business Secure Gate – Enterprise gelten die Datenvolumina laut Angebot und Auftragsbestätigung. Im Falle einer Überschreitung des Datenvolumens kann es zu einer Nachverrechnung kommen.

5.2. Einmalige Leistungen

Inbetriebnahme

Die Inbetriebnahme des Service umfasst bei der Ausprägung

Standard:
- Einrichtung des Kundentenants und eines Zugangs für einen User zur Management-Oberfläche oder Anbindung an einen IDP (Identity Provider) des Kunden (keine Useranlage)
- Konfiguration der Grundeinstellungen nach Best-Practice Ansätzen

Advanced:
- Einrichtung des Kundentenants und eines Zugangs für einen User zur Management-Oberfläche oder Anbindung an einen IDP (Identity Provider) des Kunden (keine Useranlage)
- Konfiguration der Grundeinstellungen nach Best-Practice Ansätzen oder einer Individuellen Konfiguration bei Beauftragung des Einrichtungspaketes Advanced.

Professional:
- Einrichtung des Kundentenants und eines Zugangs für einen User zur Management-Oberfläche oder Anbindung an einen IDP (Identity Provider) des Kunden (keine Useranlage)
- Konfiguration der Grundeinstellungen nach Best-Practice Ansätzen oder einer Individuellen Konfiguration bei Beauftragung des Einrichtungspaketes Professional.

Enterprise:
- Einrichtung des Kundentenants und eines Zugangs für einen User zur Management

Oberfläche oder Anbindung an einen IDP (Identity Provider) des Kunden (keine Useranlage)
- Verpflichtende Beauftragung des Einrichtungspakets – Enterprise für die individuelle Konfiguration.

Darüberhinausgehende Anpassungen, welche nicht in Betrieb und Wartung (siehe Punkt 6) inkludiert sind, werden nach Aufwand (siehe Punkt 7.7 Standard Changes) verrechnet.

Darunter fallen zum Bespiel folgende Leistungen:
- Anbindung an ein SIEM (Security Information and Event Management / Cloud und on-premises) Produkt für eine sofortige Reaktion und Alarmierung im Falle von Anomalien
- Einbindung anderer unterstützter Log-Datenspeicher

6. Betrieb und Wartung

Im Service ist die Aufrechterhaltung des aktuellen Betriebszustandes sowie folgende Leistungen in einem Umfang von maximal 15min pro Change enthalten. Darüberhinausgehende Leistungen sind nicht inkludiert, und werden gesondert nach Aufwand im Rahmen von Standard Changes (siehe Punkt 7.7) durchgeführt.

inkludierte Leistungen im Betrieb (je nach Featureset)	**nicht inkludierte Leistungen (Standard Changes) im Betrieb**
Policy Anpassungen (max. 15min pro Change) der eingerichteten Features laut beauftragter Produktausprägung im Zuge der Ersteinrichtung. Mögliche Beispiele: - URL Filtering Policy - Cloud Application Policy - SSL-Überprüfungsrichtlinie - Malware Protection Policy - Advanced Threat Policy - Sandbox Policy - Browser Isolation Profiles - Filetype Control Policy - Bandwidth Control Policy - Data Loss Prevention Policy - Out of band CASB Policy - Mobile Malware Protection Policy - Mobile Appstore Control Policy - Firewall Control Policy - DNS Control Policy - Intrusion Prevention Policy - Mobile Portal Adjustments - Application Segments - Access Policy - Timeout Policy - Client Forwarding Policy - Privileged Policy - Redirection Policy - API - Adjustments Cloud and Branch Connector Dashboard - Digital Experience Applications	Die nachträgliche Beauftragung von zusätzlichen Features oder Freischaltungen die nicht bei der Ersteinrichtung implementiert wurden. Mögliche Beispiele: - SSL Inspection - Sandbox - Data Loss Prevention - Filetype Control - NSS Logging - Customized Reports - Browser Isolation - Bandwidth Control - Out of band CASB - Mobile Appstore Control - Firewall Control - DNS Control - Intrusion Prevention - Virtual Service Edge - Partner Intregations - User Portals - App Connectors - Private Service Edges - Cloud Connector - Branch Connector
Incident Management - Störungseingrenzung (per Remote) - Wiederherstellung der Ausgangssituation im Kundennetzwerk	Anpassungen, die durch nicht servicekonforme Änderungen oder Fehlkonfigurationen des Kunden notwendig sind.

6.1. Co-Management

Der Kunde wird ausschließlich für seine Komponenten und Services freigeschalten, damit dieser einzelne Änderungen durchführen kann.

Der Kunde benötigt sowohl das Knowhow zur Bedienung des Cloud Portals als auch das Wissen über die Folgen getätigter Anpassungen. Vom Kunden getätigte Anpassungen und seine Folgen fallen in die Verantwortung des Kunden. Sämtliche Aufwände, die infolge fehlerhafter Bedienung durch den Kunden entstehen, sind von diesem zu tragen.

Jegliche Änderungen, Anpassungen oder Ergänzungen werden im Cloud Portal aufgezeichnet und es kann jederzeit ermittelt werden, welcher User Konfigurationen durchgeführt hat. Im Falle erheblicher, schadhafter Konfigurationen, die vom Kunden selbst verursacht wurden, hält sich A1 schad- und klaglos. Zudem behält sich A1 jederzeit das Recht vor, dem Kunden den Zugriff auf das Cloud Portal zu entziehen, wenn durch sein Verhalten die Serviceverfügbarkeit gefährdet wird.

7. Service Level Agreement (SLA)

Der SLA regelt den vereinbarten Servicezeitraum, in welchem die Dienstleistung entstört wird, sowie die Verfügbarkeit des Systems.

7.1. Allgemeine Begriffsdefinitionen

Servicezeit: Zeitraum, in dem Leistungen wie z.B. Herstellungen oder Fehlerbehebungen erbracht werden. Zur Berechnung der Dauer von definierten Zeiten wie z.B. der Reaktionszeit oder der Lösungszeit werden nur Zeiträume innerhalb der Servicezeit berücksichtigt.

Hemmzeiten: Alle Zeiträume außerhalb der Servicezeiten.

Fremdverzögerungen: Zeiträume, in denen die Leistungserbringung aus nicht von A1 zu vertretenden Gründen unterbleibt. Dazu gehören insbesondere auch Zeiträume, in denen eine Störungsbehebung auf Grund gesetzlicher Vorschriften nicht durchgeführt werden darf.

Werktags: Im Serviceelement angegebene Wochentage exklusive Sonntage, österreichische gesetzliche Feiertage sowie 24.12. und 31.12.

Arbeitstag: Kalendertage der im Serviceelement angegebenen Servicezeit.

7x24: Zeitraum Montag bis Sonntag von 00:00 Uhr bis 24:00 Uhr

Ihre Mitwirkung: Beschreibt die von Ihnen zu erbringenden Leistungen und Pflichten. Erfolgt keine ausreichende Mitwirkung ist A1 für Abweichungen vom Servicelevel nicht verantwortlich. Die aus der Nichterfüllung der Mitwirkung entstanden Aufwendungen sind A1 zu ersetzen.

7.2. Serviceelement Service Desk

Der Service Desk nimmt Störungsmeldungen, Anforderungen für Changes und Standard Changes unter

Telefon	International +43 50 664 8 501 511	National in Österreich (kostenlos) 0800 501 511
E-Mail		Ict.smc-cn@a1.at

entgegen.

Servicezeiten Service Desk – Störungsannahme: Mo–So, 0–24 Uhr
Servicezeiten Service Desk – Change / Standard Changes: Mo–Fr, 8–17 Uhr, werktags

7.3. Serviceelement Betrieb / Wartung

Das Service wird von Zscaler im Auftrag von A1 betrieben. Der beschriebene Service-Level bezieht sich auf die Verfügbarkeit des A1 Business Secure Gate.

Nutzungszeit: Mo-So, 0 – 24 Uhr
Beobachtungszeitraum: Kalendermonat

Servicelevel Betrieb	Verfügbarkeit
A1 Business Secure Gate	99,999%

Beginn des Service: Die Qualitätskriterien von Betrieb und Wartung gelten ab Fertigstellung des Service.

Ort der Erbringung: Zscaler-Datacenter und A1 Datacenter.

Ihre Mitwirkung
Sie nominieren kompetente Ansprechpartner (IT-Administratoren) für den Betrieb. Die Ansprechpartner verfügen über ausreichende Sprachkenntnisse in Deutsch oder Englisch

7.4. Begriffsdefinitionen im Serviceelement Betrieb /Wartung

Nutzungszeit: Zeitraum, in dem die vereinbarte Leistung dem Kunden zur Nutzung zur Verfügung steht.

Beobachtungszeitraum
Der Beobachtungszeitraum ist der kalendarische Zeitraum, in dem die Verfügbarkeit gemessen wird.

Verfügbarkeit
Die Verfügbarkeit ist das in Prozent ausgedrückte Verhältnis zwischen der Zeit, in welcher das Service nutzbar war, und dem Beobachtungszeitraum. Ein mehrfach abgesichertes Service ist verfügbar,

wenn zumindest ein Zweitsystem zur Nutzung zur Verfügung steht. Für die Verfügbarkeitsberechnung werden Systeme Dritter, die nicht Subunternehmer von A1 oder von A1 beauftragte Dritte sind, nicht berücksichtigt.

Wartungszeit: Zeit, in der tatsächliche Wartungsarbeiten durchgeführt werden, die Auswirkungen auf Qualitätslevels haben.

Wartungsfenster: Regelmäßig wiederkehrender Zeitraum, zu dem Wartungen grundsätzlich durchgeführt werden können. Unterbrechungen innerhalb des Wartungsfensters werden für die Berechnung der Verfügbarkeit nicht berücksichtigt.

Außerordentliche Wartungsarbeiten: Die außerhalb des Wartungsfensters betriebsnotwendig sind, werden dem Kunden vorangekündigt, wobei diese Arbeiten, wenn möglich, in die betriebsschwache Zeit des Kunden gelegt werden. Durchgeführte außerordentliche Wartungsarbeiten werden für die Berechnung der Verfügbarkeit nicht berücksichtigt.

Vorankündigungszeit: Minimale Frist, unter deren Einhaltung der Kunde eine Information über Wartungsarbeiten, die Auswirkungen auf seine Qualitätslevel haben, erhält.

Nichtverfügbare Zeit: Die nichtverfügbare Zeit ist die Summe aller vom Anbieter verschuldeten Ausfallszeiten im definierten Beobachtungszeitraum. Bei der Ermittlung der nichtverfügbaren Zeit werden somit z.B. Hemmzeiten und Wartungszeiten abgezogen.

Berechnung der Verfügbarkeit:

$$\text{Verfügbarkeit [\%]} = \frac{(\text{Beobachtungszeitraum} - \text{nicht verfügbare Zeit})}{\text{Beobachtungszeitraum}} \times 100$$

7.5. Serviceelement Fehlerbehebung

Fehlerbehebung (SLA: Serviceelement Fehlerbehebung)

Fehler können über den Service Desk gemeldet werden. Die Fehlerrückmeldung erfolgt je nach Fehlerkategorie innerhalb der folgenden Zeiten:

Allgemeine Parameter Fehlerbehebung

Störungsannahme: Mo-So, 0 – 24 Uhr

Service Level Agreement – SLA

Service Level	Fehlerkategorie	Servicezeit	Fehlerrückmeldezeit	Lösungszeit
7x24	Kritische Fehler	7x24	2 Stunden	6h
	Hauptfehler	5x9	4 Stunden	NBD
	Nebenfehler	5x9	NBD	4BD

Wir stufen die von Ihnen gemeldeten Störungen aufgrund Ihrer Angaben in kritische Fehler, Hauptfehler oder Nebenfehler ein. Stellt sich die Einstufung der Störung im Zuge der Fehlerbehebung als falsch heraus, so können wir diese jederzeit anpassen.

Kritischer Fehler

Die vertragsmäßige Nutzung des Service ist nicht möglich, der Service ist nicht verfügbar.
Funktionsbezogene Beispiele:

- Einschränkungen welche zur Aufrechterhaltung des Geschäftsbetriebes notwendig sind (App Konnektor ausgefallen, Cloud nicht erreichbar)

Hauptfehler

Die vertragsmäßige Nutzung des Service ist stark eingeschränkt. Das heißt, dass der Fehler u.a. wesentlichen Einfluss auf die Abwicklung der Geschäftsprozesse oder auf die Sicherheit hat, aber eine eingeschränkte Weiterarbeit zulässt. Der Service ist aber grundsätzlich verfügbar.
Funktionsbezogene Beispiele:

- Hohe Latenzzeiten, Webseiten oder Applikationen werden verzögert aufgebaut

Nebenfehler

Die vertragsmäßige Nutzung des Service ist leicht eingeschränkt. Das heißt, dass der Fehler u.a. unwesentlichen Einfluss auf die Abwicklung der Geschäftsprozesse oder die Sicherheit hat. Eine uneingeschränkte oder leicht eingeschränkte Weiterarbeit ist möglich.
Funktionsbezogene Beispiele:

- Nicht geschäftskritische Webseiten oder Applikationen funktionieren nicht.

A1 antwortet auf die E-Mail mit der Störungsmeldung innerhalb der Fehlerrückmeldezeit nach interner Prüfung. Mit der Bestätigung der Fehlermeldung ist die Störung von A1 angenommen.

Kann das Service nicht oder nur eingeschränkt genutzt werden, erbringen wir diese Leistungen:

- Wir nehmen Ihre Störungsmeldung entgegen
- Wir teilen Ihnen eine Trouble-Ticket Nummer mit
- Wir analysieren die Störung
- Nachdem die Störung behoben ist, geben wir Ihnen dies mit einer Gutmeldung bekannt

Erfordert die Lösung einer Störung ein Update oder einen Patch von Zscaler, wird A1 einen Support Case bei Zscaler eröffnen, um das Update oder den Patch bereitzustellen. Sollten auf Seiten von Zscaler Verzögerungen bei der Bereitstellung des Patches auftreten, beispielsweise weil dieser noch entwickelt oder freigegeben werden muss, wird der SLA für diesen Zeitraum durch A1 ausgesetzt. Eine daraus resultierende Überschreitung der vereinbarten SLA-Zeiten stellt in diesem Fall keine SLA-Verletzung dar. A1 verpflichtet sich, alle zumutbaren Maßnahmen zu ergreifen, um eine Lösung so schnell wie möglich herbeizuführen.

Ihre Mitwirkung
Die Ansprechpartner verfügen über ausreichende Sprachkenntnisse in Deutsch oder Englisch.

Für eine qualifizierte Störungsmeldung benötigen wir folgende Informationen:

- Kundenname, Kundennummer
- Fehlerbild
- Fehlereingrenzung

7.6. Begriffsdefinitionen im Serviceelement Fehlerbehebung

Störungsbeginn
Bei allen Services ist der Störungsbeginn der Zeitpunkt, zu dem ein Incident Ticket von A1 geöffnet wird.

- Bei allen nicht explizit von A1 proaktiv überwachten Services wird das Incident Ticket nach Eingang einer vertragskonformen Störungsmeldung angelegt.
- Bei allen proaktiv überwachten Systemen wird das Incident Ticket automatisiert geöffnet, ohne dass es einer Störungsmeldung bedarf.

Der Kunde wird von A1 per E-Mail über das Eröffnen eines Incident Tickets informiert.

Störungsmeldung
Die Störungsmeldung ist die in den Serviceelementen definierte Mitteilung des Kunden an eine vom Anbieter bekannt gegebene Stelle unter exakter Angabe des Fehlerbildes.

Proaktive Störungserkennung
Bei proaktiver Störungserkennung durch A1 wird ein Fehler unabhängig von einer Störungsmeldung des Kunden erkannt und bearbeitet.

Reaktionszeit
Die Reaktionszeit ist der Zeitraum zwischen dem Zeitpunkt der Bestätigung der Störungsannahme und dem Beginn der Störungsbehebung.

Störungspriorität
Die Störungspriorität ergibt sich aus der Bewertung der Auswirkung und der Dringlichkeit.

- Dringlichkeit (Urgency) ist ein Maß dafür, wie schnell der Incident gelöst werden muss.
- Auswirkung (Impact) drückt aus, wie umfangreich der Incident ist und welcher (potenzielle) Schaden durch den Incident verursacht werden kann.

Lösung
Lösung ist der Zeitpunkt, zu dem die Störung behoben ist.

Gutmeldung
Die Gutmeldung ist eine Information von A1 an den Kunden über die erfolgte Lösung.

Lösungszeit
Die Lösungszeit ist der Zeitraum zwischen der Bestätigung der Störungsannahme auf Grund der reaktiven Störungsmeldung des Kunden oder des vom Anbieter pro aktiv erkannten Störungsbeginns und der Lösung. Im Falle unterschiedlicher Qualitätslevel für Lösungszeiten kommt der Qualitätslevel

für die Servicezeit zur Anwendung, in der die Lösungszeit beginnt. Bei der Ermittlung der Lösungszeit werden Hemmzeiten und Wartungszeiten abgezogen.

Fehlerannahmebestätigung: A1 bestätigt den Erhalt der Störungsmeldung und gibt Ihnen die Trouble Ticket Nummer bekannt

Fehlerrückmeldezeit: Maximale Zeit zwischen dem reaktiven Störungsmeldungseingang durch den Kunden oder bei proaktiver Störungserkennung durch A1 und der Fehlerannahmebestätigung seitens A1.

7.7. Serviceelement Standard Changes

Unter einem Standard Change versteht A1 eine vorab genehmigte, vertraglich eingeschränkte oder definierte Anforderung an ein Service mit geringem Risiko und routiniertem Ablauf, welcher häufig eingesetzt wird. Standard Changes werden vom A1 Betriebsteam aus der Ferne (per remote Einsatz) vorgenommen.

Die Bestellung von vordefinierten Standard Change Leistungen werden ausschließlich von autorisierten Personen des Kunden abgesetzt. Standard Changes sind nicht im Service inkludiert und werden ausschließlich gesondert nach Aufwand abgerechnet (z.B. über einen zusätzlichen Stundenpool). Zeitfenster für die Durchführung und eventuell nötige Zeitfenster für Abschaltungen von Systemen werden gemeinsam mit dem Kunden geplant.

Servicezeit: Mo-Fr, 8 – 17 Uhr, werktags / NBD

Der maximale Arbeitsaufwand für Standard Changes beträgt 2 Stunden.

7.8. Ihre Mitwirkung

- Beim Schutz von Endgeräten (PC, Laptop oder Mobilen Devices)
  - Der Rollout des Zscaler Client Connector erfolgt durch den Kunden

- Bei Verwendung des Services über ein PAC-File (Proxy)
  - Das Setzen des Proxy-Eintrages für den Intelligent Proxy erfolgt durch den Kunden
  - Die Installation des Root SSL-Zertifikate am Client erfolgt durch den Kunden

- Bei Verwendung des Zscaler App Connectors (Private Access)
  - Für die Konfiguration notwendigen Vorarbeiten (Installation, Zugang auf den App Connector) müssen durch den Kunden durchgeführt werden oder alle notwendigen Angaben dazu bereitgestellt werden.
  - Identity Provider-Anbindung: Für die Integration notwendigen Vorarbeiten (wie die Anlage eines Users mit den notwendigen Rechten oder die Installation der eventuell benötigten Software) müssen durch den Kunden durchgeführt werden. Für die Einrichtung muss eine betriebsfertige Konfiguration des Identity Provider-Services durch den Kunden bereitgestellt werden.
  - Für eine optimale und ausfallsichere Konfiguration ist es empfehlenswert, zwei redundante Varianten des App Connectors im Kundennetz bereitzustellen. A1 ist nicht für den Betrieb des App Connectors im Kundennetz verantwortlich.

Der Kunde verpflichtet sich notwendige Vorarbeiten (wie Systemzugänge und Konfigurationen auf zusammenwirkende Systeme und Schnittstellen) durchzuführen und funktionstüchtig zur Verfügung zu stellen. Sollten Vorarbeiten nicht ordnungsgemäß oder unvollständig durchgeführt sein, so werden die dadurch anfallenden Aufwände seitens A1 in Rechnung gestellt.

8. End User Subscription Agreement (EUSA)

A1 weist ausdrücklich darauf hin, dass Nutzungsrechte an der Software dem Kunden ausschließlich durch den Hersteller gewährt werden. Inhalt und Geltungsbereich solcher Nutzungsrechte sind in den Lizenzbestimmungen (EUSA) des Herstellers, die der Kunde mit Abschluss dieses Vertrages akzeptiert.

Die EUSA des Herstellers sind unter folgendem Link abrufbar:
https://www.zscaler.com/legal/end-user-subscription-agreement

9. Leistungsänderung

A1 ist berechtigt, das angebotene Service jederzeit durch technologisch weitgehend gleichwertige Lösungen zu ersetzen, sofern das vertraglich zugesagte Service unberührt bleibt.