Leistungsbeschreibung für A1 Business Firewall (LB A1 Business Firewall)

Diese Leistungsbeschreibung gilt ab 18. März 2021 für neue Bestellungen.

A1 Telekom Austria AG (A1) erbringt das Service „A1 Business Firewall“ im Rahmen ihrer technischen und betrieblichen Möglichkeiten nach den Allgemeinen Geschäftsbedingungen für Solutions von A1 (AGB Solutions) in der jeweils geltenden Fassung, insoweit hier keine von diesen abweichende oder ergänzende Regelungen getroffen werden, samt allfälligen Individualvereinbarungen. Diese Leistungsbeschreibung gilt für Unternehmen im Sinne von § 1 Konsumenten-schutzgesetz in der geltenden Fassung.

Voraussetzungen

Voraussetzung für die Nutzung der A1 Business Firewall ist ein Internet-Zugang mit einer freien fixen öffentlichen IP-Adresse. Wird die Firewall mit einem Internet-Zugang kombiniert, der nicht von A1 stammt, muss die fixe IP-Adresse des Internet-Zuganges vom Kunden im Zuge der Herstellung an A1 übermittelt werden. Auch eventuell notwendige Freischaltungen am Internet-Zugang sind in diesem Fall vom Kunden durchzuführen oder zu veranlassen.

Durch den Kunden ist die Stromversorgung für das Firewall-Endgerät bereit zu stellen:

- die elektrische Energie in der nach ÖVE-Vorschriften vorgesehenen Spannung, Frequenz, Stromstärke und Polung für die Installation, für den Betrieb und für die Instandhaltung
- gegebenenfalls der erforderlichen Potentialausgleich einschließlich der zugehörigen Erdung

1 Grundleistung A1 Business Firewall

Im Rahmen des Service wird das Firmennetzwerk des Kunden über eine Firewall mit zusätzlichen Security Features („Next Generation Firewall“) vor Gefahren aus dem Internet geschützt. Die Firewall wird vor Ort zwischen den Internet-Zugang von A1 und das Firmennetz des Kunden geschalten.

Das Service ist für einen Internet-Zugang mit einer maximalen **Summenbandbreite (Summe aus Up- und Downloadgeschwindigkeit)** von **350 Mbit/s** ausgelegt, der von **max. 50 Benutzern** verwendet werden kann.

Bei Überschreitung dieser Grenzen kann es zu Einschränkungen oder Ausfällen kommen. Bei einer Entstörung durch A1 werden die dafür anfallenden Kosten nach Aufwand entsprechend der Liste der sonstigen Dienstleistungen, abrufbar unter A1.net, gesondert verrechnet.

1.1 Inkludierte Firewall-Features

In der A1 Business Firewall sind folgende Firewall-Features enthalten:

Firewall Paketfilter: Es wird nur erwünschter Datenverkehr zwischen dem Firmennetz und dem Internet zugelassen. Auf Wunsch wird eine oder mehrere DMZ (Demilitarisierte Zonen) eingerichtet.

VPN (Site-to-Site): Außenstellen werden über Site-to-Site-VPNs an die Firewall angebunden. Voraussetzung ist, dass die Außenstellen das VPN-Protokoll des verwendeten Firewall-Herstellers unterstützen.

VPN (Client-to-Site): Mit verschlüsseltem Datenaustausch können Mobile- und Home User (Client) auf Ressourcen in Ihrem Firmennetzwerk zugreifen (Site). Die dafür notwendige Client-Software wird von A1 zur Verfügung gestellt. Zugänge ohne Clientsoftware wie z.B. über L2TP sind von Ihnen in Eigenverantwortung einzurichten.

Die Anzahl der möglichen Client-to-Site-Verbindungen ist mit der maximalen Anzahl von Usern in der jeweiligen Leistungsstufe limitiert. Mit der Option „Advanced Remote Access“ können die Verbindungsmöglichkeiten erweitert werden.

URL-Filter: Verhindert den Zugriff auf Internet-Seiten mit schädlichen Inhalten und auch auf Seiten, die von Mitarbeitern nicht aufgerufen werden sollen. In der Standard Konfiguration sind gängige unerwünschte Kategorien gesperrt. Das Sperren oder Freigeben von weiteren Kategorien oder einzelner Adressen wird zusätzlich verrechnet. Die Sperrlisten werden durch den jeweiligen Hersteller gepflegt, wodurch Seiten auch nachträglich gesperrt werden könnten. Eine gesperrte Seite wird nicht als kritischer Fehler bewertet und kann im Rahmen eines Standard Changes entsperrt werden.

Malware Schutz: Schützt beim Surfen (unverschlüsselte Zugriffe über http oder ftp) vor Schadprogrammen wie Viren, Trojanern oder Programmen, die Ihre Daten verschlüsseln (Ransomware).

Applikations-Kontrolle: Schützt vor Schaden, der durch den Zugriff unsicherer oder unerwünschter Programme aus dem Netzwerk des Kunden auf das Internet entstehen kann. In der Standard Konfiguration sind gängige unerwünschte Kategorien gesperrt.

Denial Of Service Schutz: Schutz gegen Protokollangriffe, die darauf abzielen die Erreichbarkeit der Internet-Services des Kunden lahmzulegen. Ein Schutz vor „Volumsangriffen" ist nicht gegeben, für diese Distributed Denial-of-Services-Angriffe wird das Produkt „A1 Cleanpipe" empfohlen.

Intrusion Detection System (IDS): Erkennt Netzwerkangriffe auf das Firmennetzwerk des Kunden.

Intrusion Prevention System (IPS): Schützt aktiv vor Angriffen auf das Firmennetzwerk des Kunden. Es werden automatisch Abwehrmaßnahmen zu erkannten Bedrohungen ergriffen – z.B. gefährliche Datenverbindungen unterbrochen. In der Standard-Konfiguration ist IPS ausgeschalten, da die Einstellungen auf das Firmennetzwerk des Kunden abgestimmt werden müssen.

Antibot: Schützt das Firmennetzwerk des Kunden vor bekannten „Bot-Netzwerken".

Es gelten folgende Limits:

- VPN-Zugang Client-to-Site
  Es sind maximal 20 Client-to-Site Verbindungen inkludiert. Für VPN-Verbindungen (Client-to-Site und Site-to-Site) steht eine Summenbandbreite von max. 50 Mbit/s zur Verfügung.

- VPN Zugang Site-to-Site
  Es sind maximal 10 Site-to-Site Verbindungen inkludiert. Für VPN-Verbindungen (Client-to-Site und Site-to-Site) steht eine Summenbandbreite von max. 100 Mbit/s zur Verfügung.

1.2 Einmalige Leistungen

Installation

Die Firewall wird am Kundenstandort durch A1 installiert und mit dem Internet-Anschluss sowie dem Firmennetzwerk des Kunden verbunden.

Inbetriebnahme

Die Inbetriebnahme des Service erfolgt auf Basis einer Standard-Konfiguration. Die einmalige Anpassung der Standard-Konfiguration an die speziellen Anforderungen des Kunden ist bis zu einem Aufwand von max. 2 Stunden inkludiert und wird per Fernwartung („remote") durchgeführt. Darüberhinausgehende Anpassungen werden nach Aufwand entsprechend der Liste der Sonstigen Dienstleistungen der A1 verrechnet.

Einrichtung im Management-System
Die Verwaltung des Service erfolgt über ein zentrales Management-System, das in einem A1 Datacenter betrieben wird. Dazu wird das Service einmalig im Management-System angelegt.

1.3 Betrieb und Wartung

Im Service ist die Aufrechterhaltung des aktuellen Betriebszustandes enthalten.

Inkludierte Leistungen	Leistungen nicht inkludiert (Standard Changes - gesondert nach Aufwand abzurechnen)
Patch & Releasemanagement – A1 übernimmt für die Systemerhaltung bei Bedarf die Durchführung des Major Software Releasewechsels – Aktuell von A1 freigegebene Versionen von Stable Release, Minor Release werden beim Kunden eingespielt – Aktuell von A1 freigegebene Versionen von Hotfixes/Patches zur Behebung von möglichen „**kritischen Incidents**“ werden beim Kunden umgehend installiert/gepatcht	**Anpassungen/Erweiterungen Standard Features** – Application Control – DHCP Service – DHCP Relay – DNS Forwarding – Quality of Service Einstellungen – Netzwerkanpassungen – User Authentication gegen Active Directory für VPN/Firewall Policies – Erweiterung der VLAN Netzwerkstruktur – IP-Adressänderungen / Subnet Mask Router Interface – Änderung der generellen Interfacekonfiguration – Hinzufügen/ändern/entfernen von ACLs – Änderung von NAT/PAT Eintragungen – Änderungen der Routingeinstellungen – LAN-Segmentierung (DMZ, mehrere VLANs, etc)
Incident Management – Störungseingrenzung bei Hardware/Software Problemen (Remote oder mit "On Site" Unterstützung) – Wiederherstellung der Ausgangsituation im Kundennetzwerk	**Anpassungen/Erweiterungen Features gewählte Securitystufe** – Basic Firewalling – URL Filter – VPN Client2Site – VPN Site2Site – SSL Interception – SSL VPN – User Authentication gegen Active Directory für VPN/Firewall Policies – Ausnahmen von URL-Filtern - IDS/IPS Änderungen am Ruleset
Problem Management – Systematische Analyse von Wiederholungsstörungen – Nachhaltige Behebung von Fehlerursachen	**Port Anpassungen** – Aktivierung oder Deaktivierung von Ports – Port up/down, Duplex – VLAN Portzuweisung – Portkonfiguration verschieben – Einrichtung eines zusätzlichen VLANs
	Zugriffe für Management Funktionen – SNMP, Managementsoftware

Serviceportal – Mein A1 Business
Das A1 Kundenportal Mein A1 Business ist die zentrale Dateninformationsquelle. Das Portal stellt wichtige Informationen rund um den Service bereit.

1.4 Fehlererkennung – NMS Reaktiv

Die im Service enthaltenen Endgeräte sind in das A1 Network Management System (NMS) eingebunden. Dadurch können reaktiv gemeldete Störungen innerhalb kürzester Zeit behoben werden.

- Configuration Management
- Fault Management
- Security Management

1.5 Fehlerbehebung – 5x9/8h

Die SLA-Klasse 5x9/8h ist inkludiert (siehe Punkt “3.3 Serviceelement Fehlerbehebung”).

1.6 Komponenten der Leistungserbringung

Die beschriebenen Leistungsmerkmale stehen im Vordergrund. Die verwendeten Komponenten zur Leistungserbringung (Hardware, Software und Lizenzen) dienen lediglich zur Realisierung der Leistungsmerkmale. Es besteht keinerlei Anspruch auf bestimmte Typen, Softwarepakete oder Lizenzen. Die Auswahl der Komponenten liegt allein bei A1 und kann jederzeit – ohne Einfluss auf die vertraglich vereinbarten Services – geändert werden.

Alle Komponenten zur Leistungserbringung werden von A1 für die Dauer der Serviceerbringung bereitgestellt und verbleiben im Eigentum von A1. Nach Beendigung der Services werden alle Konfigurationen gelöscht. Eine Übernahme oder ein Kauf der Komponenten ist nicht möglich.

Hardware Komponenten werden nach Nutzungsende durch A1 Personal abgebaut und an A1 retourniert. Die Kosten dafür sind bereits pauschal im Produkt A1 Business Firewall enthalten. Sollte der Kunde die Komponenten selbst abbauen und an A1 retournieren wollen, so ist dies durch den Kunden zeitgerecht vor Vertragsende oder im Zuge der Kündigung dem für Sie zuständigen Vertriebsansprechpartner bei A1 zu melden. Da diese Kosten pauschal im Service enthalten sind, können diese nicht gutgeschrieben werden.

Bei Rückgabe von stark verschmutzten und/oder beschädigten Komponenten, bei denen die Beschädigung und/oder Verschmutzung einen für die Art der Nutzung üblichen Verschmutzungs- und/oder Beschädigungsgrad übersteigt, behält sich A1 vor, die Kosten für Reinigung, Reparatur und/oder Ersatz in Rechnung stellen.

A1 ist berechtigt, die angebotenen Leistungsinhalte jederzeit durch technologisch weitgehend gleichwertige Lösungen zu ersetzen, sofern die vertraglich zugesagten Funktionalitäten unberührt bleiben.

2 Optionen

Bei Inanspruchnahme von Optionen werden verschiedene zusätzliche Dienstleistungen (gegen zusätzliches Entgelt gemäß den maßgeblichen Entgeltbestimmungen) zum Standardpaket entsprechend den folgenden Bestimmung angeboten.

2.1 Advanced Remote Access

Der VPN Zugang Client-to-Site wird um zusätzliche Leistungen erweitert:

- CudaLaunch App
  Für den VPN Zugang Client-to-Site kann zusätzlich die Applikation CudaLaunch verwendet werden. CudaLaunch vereinfacht den Zugriff auf das Firmennetzwerk und ist auch für iOS und Android Geräte erhältlich.

- SSL-VPN Portal
  Sicherer Zugang zum Firmennetzwerk per Web-Browser

- „Zero-Trust“ Zugriff
  Der User kann nur auf bestimmte Applikationen zugreifen und nicht auf das gesamte für VPN freigegebene Netzwerk. Diese Steuerung ist nicht für alle Applikationen möglich.

2.2 Fehlererkennung – NMS Proaktiv

Die im Service enthaltenen Endgeräte sind in das A1 Network Management System (NMS) eingebunden. Dadurch können Störungen innerhalb kürzester Zeit proaktiv erkannt und behoben werden.

- Configuration Management
- Fault Management
- Security Management

2.3 Fehlerbehebung – 6x12/8h

Optional kann die SLA-Klasse 6x12/8h gewählt werden (siehe Punkt “3.3 Serviceelement Fehlerbehebung”).

2.4 Features mit Herstellung nach Aufwand

Folgende Features werden im Zuge der Herstellung oder im Nachhinein gegen Verrechnung des angefallenen Aufwandes (entsprechend der „Liste für sonstige Dienstleistungen der A1“) hergestellt:

Dual Internet
Die Firewall wird mit einem zweiten Internet-Anschluss verbunden, über den ein definierter Teil des Internet-Traffics geleitet wird. So kann z.B. der Datenverkehr eines „Gäste-

WLANs“ über den zweiten (mobilen) Internet-Anschluss abgeführt werden, damit der erste Internet-Anschluss für geschäftskritische Anwendungen zur Verfügung steht.

Der Aufbau von SD-WANs (Software-Defined Wide Area Networks) wird innerhalb des Service nicht unterstützt.

Quality Of Service (QoS)
QoS wird eingesetzt, um bestimmten Datenverkehr (wie Voice-Over-IP Traffic oder die Daten wichtiger Business-Anwendungen) bei ausgelastetem Netzwerk bevorzugt zu übertragen. Die Priorisierung kann dabei u.a. nach Anwendung oder Protokoll erfolgen.

Quality Of Services ist nur für Internet-Anbindungen mit stabiler und bekannter Bandbreite möglich, und damit für mobile Internet-Anbindungen nicht geeignet.

Active Directory (AD)-Integration

Ein vom Kunden betriebenes Authentification-Service wird an die Firewall angebunden, um User und Gruppen für folgende Anwendungen zu authentifizieren:

- VPN-User für den Client-to-Site VPN-Zugang
  Es können alle von der Firewall unterstützten Authentification-Services verwendet werden. Informationen zu den unterstützten Services stellt A1 bei Bedarf gerne zur Verfügung.

- Erstellung von User & Gruppen basierten Firewall-Regeln
  Als Authentification-Service kann nur Microsoft Active Directory verwendet werden.

Voraussetzung für die Einrichtung ist, dass der Kunde über ein geeignetes Authentification-Service verfügt und dieses Service für A1 erreichbar ist. Die für die Integration notwendigen Vorarbeiten (wie die Anlage eines Users mit den notwendigen Rechten oder die Installation der event. benötigten Software) müssen durch den Kunden durchgeführt werden.

2.5 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 (kleine Änderungsaufträge) werden vom A1 Betriebsteam aus der Ferne vorgenommen (per remote Einsatz).

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 evtl. nötige Zeitfenster für Abschaltungen von Systemen werden gemeinsam mit dem Kunden geplant.

Inkludierte Leistungen und nicht inkludierte Standard Changes bei Erstinstallation und Betriebsführung sind in Punkt „1.2 Einmalige Leistungen“ und Punkt „1.3 Betrieb und Wartung” näher ausgeführt.

3 SLA (Service Level Agreement)

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

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.

3.1 Serviceelement Service Desk

Der Service Desk nimmt Störungsmeldungen und Anforderungen für Standard Changes unter 0800 501 511 entgegen.

Servicezeiten Service Desk – Störungsannahme: Mo–So, 0–24 Uhr

Servicezeiten Service Desk – Standard Changes: Mo–Fr, 8–17 Uhr, werktags

3.2 Serviceelement Betrieb

Im Rahmen des Service wird die Firewall am Kundenstandort und das zugehörige Management-Systeme im Rechenzentrum von A1 betrieben.

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

Servicelevel Betrieb	Verfügbarkeit
A1 Business Firewall	99 %

Messung: A1 setzt eine branchenübliche Lösung für die Überwachung und das Management ein. Die erhobenen Daten werden über den Beobachtungszeitraum mit relevanten Trouble-Tickets aggregiert und statistisch ausgewertet. Es werden nur kritische Fehler in der Bestimmung der nichtverfügbaren Zeit berücksichtigt.

Reports: Ein auf Ihre Bedürfnisse abgestimmtes Reporting kann auf Anfrage – im Rahmen unserer technischen und betrieblichen Möglichkeiten – eingerichtet werden.

Merkmale des Serviceelementes: Der Betrieb erfolgt 0 bis 24 Uhr als dedizierte Firewall am Kundenstandort und dem Management-System im A1 Datacenter.

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

Ort der Erbringung: Kundenstandort (Firewall), A1 Datacenter (Management-System)

Ihre Mitwirkung
A1 kann Sie zu einer Abnahme oder Teilabnahme einladen. Diese muss innerhalb von 7 Tagen erfolgen. Bloß geringfügige Mängel berechtigen Sie nicht zur Verweigerung der Abnahme. Die Abnahme wird dadurch dokumentiert, dass beide Parteien ein Abnahmeprotokoll unterschreiben.

Nimmt auf Grund der Größe des Auftrags die Herstellung mehr als 12 Wochen in Anspruch, kann A1 die Leistungen in mehreren Teilen abnehmen lassen.

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

Begriffsdefinitionen im Serviceelement Betrieb

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

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

Wartungsfenster: Regelmäßig wiederkehrender Zeitraum, während 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.

Beobachtungszeitraum: Kalendarischer Zeitraum, in dem die Verfügbarkeit gemessen wird.

Verfügbarkeit: In Prozent ausgedrücktes Verhältnis zwischen der Zeit, in der eine vereinbarte Leistung vertragskonform nutzbar war und dem Beobachtungszeitraum.

Nichtverfügbare Zeit: Summe aller von A1 verschuldeten Ausfallszeiten im definierten Beobachtungszeitraum. Bei der Ermittlung der nichtverfügbaren Zeit werden somit z.B. Fremdverzögerungen, Hemmzeiten und Wartungszeiten nicht berücksichtigt.

Berechnung der Verfügbarkeit:

Verfügbarkeit [%]=	(Beobachtungszeitraum – nicht verfügbare Zeit) / Beobachtungszeitraum	x 100

3.3 Serviceelement Fehlerbehebung

Fehlerbehebung (**SLA: Serviceelement Fehlerbehebung)**
Fehler können über den Service Desk gemeldet werden oder sie werden proaktive durch Monitoring-Systeme von A1 erkannt. Die Behebung des Fehlers erfolgt je nach Fehlerkategorie innerhalb der folgenden Zeiten:

Allgemeine Parameter Fehlerbehebung

Störungsannahme: Mo-So, 0 – 24 Uhr
Fehlerrückmeldezeit: 30 min.

Service Level Agreement – SLA – 5x9/8h

Fehlerbehebung

ServiceLevel	Fehlerkategorie	Servicezeit	Reaktionszeit	Lösungszeit
5x9/8h	Kritische Fehler	Mo-Fr, 8-17 Uhr, werktags	2h	8h
	Hauptfehler			nächster Werktag
	Nebenfehler	Mo-Fr, 8-17 Uhr, werktags	Nächster Werktag	5 Werktage

Service Level Agreement – SLA – 6x12/8h

Fehlerbehebung

ServiceLevel	Fehlerkategorie	Servicezeit	Reaktionszeit	Lösungszeit
6x12/8h	Kritische Fehler	Mo-Sa, 7-19 Uhr, werktags	2h	8h
	Hauptfehler			nächster Werktag
	Nebenfehler	Mo-Fr, 8-17 Uhr, werktags	nächster Werktag	5 Werktage

Messung

A1 misst die Fehlerbehebung über das Ticketing System auf Basis der erfassten Störungstickets. Im Trouble Ticket System erfasst A1 Störungsgeschäftsfälle

- proaktiv durch Störungserkennung durch das Alarm Management Systems von A1 oder
- reaktiv auf Grund Ihrer Störungsmeldung

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

- Wir erkennen Fehler proaktiv oder 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

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:

- Ausfall der Internetverbindung für länger als 10 Minuten.
- Systemstillstand ohne Wiederanlauf

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:

- Verbindungsprobleme bei VPN-Clients, langsame WAN-Verbindung
- Häufung von kurzfristigen Störungen des Betriebs

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:

- Zertifikatswarnungen

Beginn der Fehlerbehebung: Beginn der Fehlerbehebung ist die proaktive Erkennung durch Monitoring-Systeme von A1 oder die qualifizierte Störungsmeldung durch Ihre Mitarbeiter an den von A1 bekannt gegebenen Service Desk.

Wird die Störung elektronisch eingemeldet, z.B. per E-Mail, antwortet A1 innerhalb der Fehlerrückmeldezeit nach interner Prüfung. Mit der Bestätigung der Fehlermeldung ist die Störung von A1 angenommen.

Ort der Erbringung: Standorte und Einrichtungen von A1.

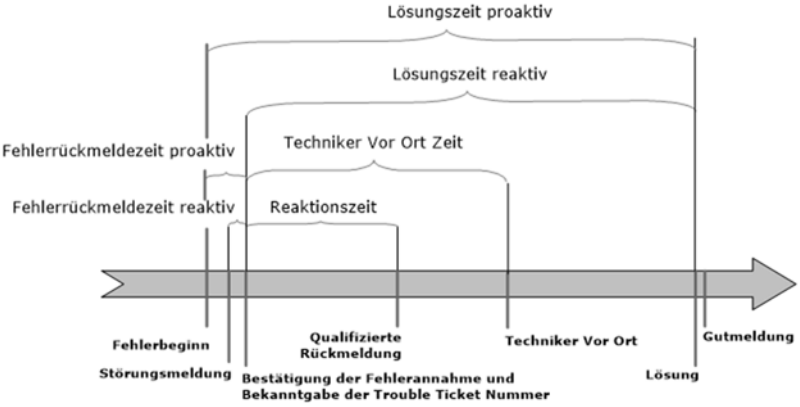
Ihre Mitwirkung
Ein System gilt dann als verfügbar, wenn die Systemfunktionalitäten wiederhergestellt sind. In die Lösungszeit nicht eingerechnet werden Zeiten, die für die Rückeinspielung von Backups notwendig sind und Zeiten, die für die Bereitstellung von Bugfixes seitens Software-Hersteller notwendig sind.

Die Ansprechpartner verfügen über ausreichende Sprachkenntnisse in Deutsch oder Englisch.

Für eine qualifizierte Störungsmeldung benötigen wir von Ihrem IT Administrator folgende Informationen:

- Kundenname
- Fehlerbild
- Fehlereingrenzung

Abbildung 4: Begriffsdefinitionen im Serviceelement Fehlerbehebung



Fehlerbeginn: Zeitpunkt des Auftretens eines Fehlers.

Störungsmeldung: In den Serviceelementen definierte Mitteilung des Kunden an eine von A1 bekannt gegebene Stelle unter exakter Angabe des Fehlerbildes.

Proaktive Störungserkennung: A1 erkennt und bearbeitet Fehler unabhängig von einer Störungsmeldung des Kunden.

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.

Qualifizierte Rückmeldung: Erste Diagnose der Problemursache mit Bekanntgabe des weiteren Lösungsweges an den Kunden.

Reaktionszeit: Zeitraum zwischen Beginn der Lösungszeit und dem Beginn der Fehleranalyse.

Techniker vor Ort: Zeitraum zwischen Beginn der Lösungszeit und dem Eintreffen eines Technikers vor Ort.

Lösung: Zeitpunkt, zu dem die Störung behoben ist.

Lösungszeit: Zeitraum zwischen Bestätigung der Fehlerannahme auf Grund der reaktiven Störungsmeldung des Kunden oder proaktiver Störungserkennung und der Lösung. Bei der Ermittlung der Lösungszeit werden Fremdverzögerungen, Hemmzeiten und Wartungszeiten abgezogen.

Gutmeldung: Information über die erfolgte Lösung.

3.4 Serviceelement Standard Changes

Servicezeit: Mo-Fr (werktags), 08.00 – 17.00 Uhr

Der maximale Arbeitsaufwand für Standard Changes beträgt 2 Stunden.

3.5 Serviceelement Wartung

Wir führen Anpassungen der Firewall- und Betriebssystem-Software an den aktuellen Entwicklungsstand des Herstellers innerhalb des Wartungsfenster durch. In Notfällen werden Software-Fixes sofort eingespielt

Wartungsarbeiten
Wartungsfenster: Werktags, Do 19 – Fr 4 Uhr

Das Service beinhaltet die Wartung des im Angebot definierten Leistungsumfangs.

Geplante Wartungsarbeiten / Standard Wartungsfenster: Regelmäßige Wartung von Services durch A1 im Voraus definierten Zeitraum, dem so genannten Wartungsfenster

Fremdverzögerungen können zu einer Verlängerung der Wartungsarbeiten führen, für die A1 nicht haftet.

Beginn des Service Wartung: Die Qualitätskriterien von Betrieb und Wartung gelten ab abgeschlossener Lieferung durch A1.

Ihre Mitwirkung

Die Aufrechterhaltung der Interoperabilität der von Ihnen selbst betriebenen Systeme, welche an das von A1 bezogene Service anschließen, liegt in Ihrer Verantwortung. Informationen für die entsprechende Wartung Ihrer Systeme – wie erforderliche Software-Release oder Hersteller Support-Matrix – werden von uns jeweils aktuell bereitgestellt und sind bei Ihren eigenen Wartungsarbeiten zu berücksichtigen. Bei Wartungsarbeiten kann die Mitwirkung des IT Administrators des Kunden erforderlich sein.

Begriffsdefinitionen im Serviceelement Wartung

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

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

Außerordentliche Wartungsarbeiten: 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.