TERRA CLOUD

Leistungsbeschreibung Firewall VM

Stand: 11/2023

Powered by intel Cloud Technology

Microsoft Cloud OS Network Partner

WORTMANN AG

IT. MADE IN GERMANY.

Inhaltsverzeichnis

1 Produktbeschreibung

Die TERRA CLOUD GmbH stellt dem Kunden, sofern im Basispaket enthalten oder sofern gebucht, eine private Firewall VM zur Verfügung. Diese Firewall VM verbindet das öffentliche Internet mit dem privaten Netzwerk, das dem Kunden dediziert als eigener VLAN Abschnitt zur Verfügung gestellt wird. Dabei verwendet der Kunde in seinem privaten Netzwerk ausschließlich private IP-Adressen nach RFC 1918. Die zentrale Aufgabe der Firewall VM ist der Schutz des Kundennetzwerkes mit verschiedenen Mechanismen.

2 Leistungselemente

2.1 Network Address Translation

Dieser Dienst dient zur Umsetzung der privaten IP-Adressen des Kundennetzwerkes in öffentliche IP-Adressen des Internets (Source NAT) und der Umsetzung von öffentlichen IP-Adressen, die am externen Interface der Firewall VM anliegen, auf private IP-Adressen im Kundennetzwerk (Destination NAT). Die Umsetzung basiert auf Teilen der RFCs 2663, 2766 und 3022.

2.2 Paket-Filter (mit Stateful Packet Inspection)

Um steuern zu können, welche öffentlichen IP-Adressen mit welchen IP-Adressen des Kundennetzwerkes kommunizieren dürfen (IPv4-Pakete miteinander austauschen dürfen), ist der Paket-Filter vorhanden. Dabei stehen folgende Entscheidungskriterien für die Auswahl einer Regel zur Verfügung:

- Quell-IPv4-Adresse einer Kommunikation
- Ziel-IPv4-Adresse einer Kommunikation
- Das verwendete Transportprotokoll (TCP, UDP, ESP und ICMP)

Bei den Transportprotokollen TCP und UDP können zusätzlich die in diesen Protokollen verwendeten Quell- und Zielports der Kommunikation ausgewertet werden. Die Firewall unterstützt bis zu 500 solcher Regeln je Firewall VM. Das Regelwerk wird von Zeile 1 abwärts abgearbeitet. Sobald eine Regel zutrifft, wird deren Aktion durchgeführt und es werden keine weiteren Regeln mehr für dieses Paket berücksichtigt.

Als Aktion steht dem Kunden zur Verfügung:

- „Accept“ – das Paket und die damit zusammenhängende Kommunikation wird erlaubt
- „Drop“ – das Paket wird verworfen (es gibt keine Rückmeldung der Firewall an den Absender)
- „Reject“ – das Paket wird mit einem ICMP Paket „Destination Unkown“ beantwortet und verworfen.
- „Stateless“ – die Verbindungen werden Statusunabhängig zugelassen (empfohlen für VOIP Verbindungen)
- „QoS“ – die Bandbreite der Regel kann dadurch limitiert werden

2.3 Implizite Regeln

Innerhalb der Firewall VM gibt es so genannte implizite Regeln. Diese Regeln erlauben oder verbieten den Netzwerktraffic diverser Protokolle. Die impliziten Regeln können durch den Kunden nur aktiviert oder deaktiviert, jedoch nicht verändert werden.

2.3.1 VPN Funktion - OpenVPN

Für den verschlüsselten Zugriff des Kunden auf seine Geräte (inklusive der Firewall VM) im Kundennetzwerk stellt die Firewall eine sogenannte VPN-Verbindung zur Verfügung.

Diese VPN-Verbindung basiert auf der VPN-Software OpenVPN und nutzt in der Standardeinstellung zum Transport der gesamten Verbindung (Steuerung und Daten) UPD als Transportprotokoll.

Damit der Kunde eine VPN-Verbindung mit der Firewall VM aufbauen kann, muss ein OpenVPN-fähiger Client für das eingesetzte Betriebssystem installiert sein. Die zugehörige Konfigurationsdatei, sowie die Zugangsdaten (Benutzername und Passwort) werden nach dem Abschluss der Bestellung im TERRA CLOUD Center hinterlegt. Außerdem muss der Kunde sicherstellen, dass dieser Rechner standardmäßig bis zur Firewall VM des Kundennetzwerkes uneingeschränkt das Transportprotokoll UDP von einem beliebigen Quellport auf den Zielport 1194 verwenden kann.

Der Administrator kann weitere OpenVPN-Konten konfigurieren und verwenden. Diese Anbindung ist sowohl für einzelne Arbeitsplätze als auch für eine sogenannte LAN-LAN-Kopplung geeignet. Als Gegenstellen für eine LAN-LAN-Kopplung sind Firewalls von der Wortmann AG und von Securepoint freigegeben. Firewalls weiterer Hersteller müssen vom Kunden auf ihre Kompatibilität mit der Firewall VM des Kundennetzwerkes auf eigene Kosten und Risiko getestet werden.

2.3.2 VPN-Funktion – IPSec VPN

Für die Anbindung von Endgeräten und für die LAN-LAN Kopplung steht auch das VPN-Protokoll IPSec zur Verfügung.

Für die Anbindung von Endgeräten empfehlen wir die Verwendung von OpenVPN.

Als Gegenstellen für eine LAN-LAN Kopplung mit IPSec sind Firewalls von der Wortmann AG und von Securepoint freigegeben. Firewalls weiterer Hersteller müssen vom Kunden auf ihre Kompatibilität mit der Firewall VM des Kundennetzwerkes auf eigene Kosten und Risiko getestet werden.

2.3.3 Administration / Administrationsverantwortung

Sobald dem Kunden die Administration der Firewall übergeben wurde, ist er auch für verschiedene vorkonfigurierte Dienste selbst verantwortlich. Eine Fehlkonfiguration kann ihn z.B. auch von der Administration seines Netzwerkes abschneiden. Die Administration ist nicht Bestandteil der Leistung der Firewall VM, kann jedoch optional dazu gebucht werden (siehe hierzu 3.1.2).

2.4 Leistungserweiterungen/-änderungen

Die Erweiterung und Änderung von Leistungen erfolgt über das TERRA CLOUD Center aus einem vordefinierten Leistungskatalog.

Die Änderungen werden zu einem mit dem Kunden individuell vereinbarten Termin durchgeführt und sind abhängig von der Dauer des Umbaus sowie der Verfügbarkeit der benötigten Komponenten.

Änderungen und Erweiterungen können zu einer kurzfristigen Nichtverfügbarkeit des Systems bzw. zu einem Neustart des Systems führen. Diese geplante Ausfallzeit ist von der Verfügbarkeitsberechnung des Hauptproduktes ausgenommen und wird mit Einverständnis des Kunden primär in den fest definierten Wartungsfenstern durchgeführt.

2.5 Einmalleistungen

Einmalleistungen können über das TERRA CLOUD Center oder den Service Desk beauftragt werden. Diese Leistungen werden als Pauschale verrechnet, ein Katalog der verfügbaren Einmalleistungen kann dem TERRA CLOUD Center entnommen werden.

2.6 Sichere Datenlöschung

Bei Beendigung des Einzelauftrags werden nach 14 Tagen automatisch die Festplatten des Servers, die zugeordneten Storage-Volumes und die entsprechenden Userlaufwerke gelöscht. Das Löschen der Userdaten erfolgt nach DOD 5220.22-M. Eventuell vorhandene Backup-Daten werden ebenfalls gelöscht. Nach erfolgreichem Löschvorgang erhält der Kunde eine Löschbestätigung.

Bei Beendigung des Rahmenvertrags wird der Zugriff auf die remote Anbindung an das TERRA CLOUD Rechenzentrum deaktiviert. Zur Verfügung gestellte Hardware, wie z. B. der TERRA CLOUD Connector müssen an die TERRA CLOUD innerhalb von 14 Tagen zurückgegeben werden.

3 Zusatzoptionen

3.1 Verwaltung der Firewall

Die Firewall VM wird dem Kunden grundsätzlich zur Selbstverwaltung eigenverantwortlich übergeben. Die Verwaltung und Administration der Firewall VM ist nicht Bestandteil der TERRA CLOUD Leistungen.

3.1.1 Erstkonfiguration

Die Firewall VM wird mit einer vorkonfigurierten Konfiguration geliefert und dann durch das NOC Team der TERRA Cloud GmbH auf eine mit dem Kunden abgestimmte Konfiguration gebracht. Dafür wird dem Kunden ein Fragebogen zur Verfügung gestellt, den dieser ausgefüllt zur Verfügung stellen muss. Die einstellbaren Konfigurationsteile der Firewall VM entsprechen den Möglichkeiten, die aus dieser Leistungsbeschreibung ergehen. Nicht aufgeführte Dienste können nach Einzelüberprüfung entgeltlich zusätzlich konfiguriert werden. Ein Anrecht auf Konfigurationen außerhalb der Leistungsbeschreibung besteht nicht.

Die Firewall VM wird inkl. Konfiguration an den Kunden übergeben und mit diesem zusammen getestet. Nach erfolgreichem Test geht die Firewall in den Status „Self Managed“ über, somit gelten die Bedingungen unter 3.1.

Die Erstkonfiguration ist beschränkt auf 40 Netzwerkobjekte und 40 Portfilterregeln, sowie die Einrichtung einer IPSEC LAN-LAN Kopplung und dem Anlegen von drei OpenVPN-Zugängen für Road-warrior. Weitere Konfigurationen sind gegen Aufpreis verfügbar.

3.1.2 Full Managed Firewall

Die gesamte Konfiguration und Verwaltung der Firewall VM wird durch die TERRA CLOUD GmbH und dessen Dienstleistern vorgenommen. Hierbei wird nach der Bereitstellung der Firewall VM diese entsprechend der mit dem Kunden abgestimmten Daten konfiguriert. Für die Konfiguration wird dem Kunden ein Fragebogen zur Verfügung gestellt, den dieser entsprechend ausgefüllt der TERRA CLOUD GmbH zur Verfügung stellen muss.

Die Option der full managed Firewall kann nur in Kombination mit der Erstkonfiguration gebucht werden. Die Erstkonfiguration wird gemäß Beschreibung in 3.1.1 erbracht.

Für Änderungen (Changes) im Betrieb steht dem Kunden ein Kontingent von einzelnen Aktionen zur Verfügung.

Der Kunde kann:

- 40 Netzwerkobjekte
- 40 Portfilterregeln
- eine IPSEC LAN-LAN-Kopplung
- bis zu 3 OpenVPN Zugänge für Roadwarrior

neu einrichten oder ändern lassen.

Weitere Konfigurationen sind gegen Aufpreis verfügbar. Das Kontingent wird alle zwölf Monate wieder auf die obenstehenden Werte aufgefüllt. Alte Kontingente sind damit verfallen.

3.2 Zusätzliche Schutzfunktionen

3.2.1 Internet-Schutz

Der Internet-Schutz vereint die Funktionen des Content-, sowie Antiviren-Pakets und kann optional kostenpflichtig hinzugefügt werden.

Das Content-Filter-Paket dient zur Analyse und Kontrolle von HTTP- und HTTPS-Datenströmen aus dem Kundennetzwerk ins öffentliche Internet. Dabei kann HTTP und HTTPS automatisch (transparent) aus dem Netzwerkverkehr herausgefiltert oder der HTTP-Proxy fest in der Software innerhalb des Kundennetzwerks hinterlegt werden.

Das Content-Filter-Paket bietet folgende Funktionen:

- Zugriffssteuerung anhand von Benutzern (nur bei aktiver Authentifizierung), Netzwerkobjekten und Netzwerkgruppen
- Freigabe/Sperrung einzelner Webseiten
- Freigabe/Sperrung von Website-Kategorien
- Freigaben gelten immer vor Sperrungen

Zur Analyse der Zugehörigkeit einer URL zu einer Kategorie wird diese zum Hersteller der Firewall VM Software übertragen.

Beim Antivirus-Paket prüft der HTTP-Proxy bei umgeleitetem Traffic diesen auch auf Viren, dabei kann zwischen zwei Virenscannern gewählt werden. Das Antivirus-Paket ersetzt keine Antiviren-Software auf dem Server- oder Clientsystem.

3.2.2 E-Mail-Schutz

Der E-Mail-Schutz vereint die Funktionen des Spam-, sowie Antiviren-Pakets und kann optional kostenpflichtig hinzugefügt werden.

Mit dem Spamfilter-Paket kann der Kunde SMTP-Datenströme von unerwünschten Emails befreien. Dafür ist es notwendig, dass der Kunde zu filternde Email-Daten mittels des SMTP-Protokolls über das Mailrelay der Firewall routet. Hier kann der Kunde definieren für welche Domains er Emails entgegen nimmt und wohin diese nach der

Prüfung weitergeleitet werden sollen. Dafür ist es notwendig, dass der Kunde in seinem Kundennetzwerk einen Mailserver mit SMTP-Schnittstelle betreibt.

Zur Spamabwehr verfügt die Firewall VM über folgende Mechanismen:

3.2.2.1 Greeting Pause

Beim Beginn der Kommunikation legt die Firewall VM eine Pause in der von SMTP vorgesehenen Begrüßung (Greeting) ein. Wenn die Gegenstelle in dieser Zeit weitere Daten schickt, wird die Verbindung unterbrochen. Diese Funktion kann an- und abgeschaltet werden.

3.2.2.2 Greylisting

Mittels Greylisting erfolgt die Annahme einer Email per SMTP nur, wenn der Absender schon einmal eine Email an den Empfänger vom gleichen Absenderserver geschickt hat. Schickt ein Mailserver das erste Mal eine Email an einen Empfänger des Kunden, so wird diese Verbindung mit einem temporären Fehler abgelehnt. Die Firewall VM merkt sich nun die IP-Adresse des sendenden Servers, die Emailadresse des Absenders und die Emailadresse des Empfängers und setzt diese für eine eingestellte Zeit (z. B. 7 Tage) auf eine Whitelist. Beim nächsten Zustellungsversuch des gleichen Absender-Servers wird die Email dann angenommen. Diese Funktion kann an- und abgeschaltet werden.

Die Funktion Greylisting entspricht nicht dem RFC 2821 (SMTP) und kann bei eingehenden Emails zu Verzögerungen auch im gewünschten Mailverkehr führen.

3.2.2.3 Message Identifikation Verfahren

Aus dem Inhalt einer zu prüfenden Email wird eine Message ID generiert. Diese wird zur zentralen Datenbank des Herstellers übertragen und die Firewall VM erhält einen Status zu dieser Email zurück. Der Email-Inhalt wird dabei in keinem Fall an den Hersteller übertragen. Der Status dieser Email kann lauten:

- „Clean“ - Email ist unverdächtig
- „Probably Spam“ – Email ist möglicherweise unerwünscht (hierunter fallen oft auch abonnierte Newsletter)
- „Spam“ – Die Email ist ein Spam

Eine SPAM-Email wird definiert als eine Email deren Zustellung der Kunde nicht angefordert hat.

Ausdrücklich kein SPAM sind Newsletter, die der Kunde abonniert hat und Geschäfts- oder private Emails von korrekt arbeitenden Unternehmen oder sich korrekt verhaltenden Privatpersonen.

Die Spamerkennungsquote liegt bei Aktivierung aller Funktionen mindestens bei 98% im Jahresmittel. Die Fehlerquote, also die Deklarierung erwünschter Emails als SPAM, liegt bei weniger als 1% im Jahresmittel.

Bei aktiviertem Antivirus-Paket prüft die Firewall VM die durchgeleiteten Emails auch auf Viren, dabei werden beide integrierten Virenscanner nacheinander verwendet. Das Antivirus-Paket ersetzt keine Antiviren-Software auf dem Server- oder Clientsystem.

4 Voraussetzungen und Mitwirkungspflichten

Voraussetzung für die Nutzung einer Firewall VM ist die Nutzung eines Produktes aus den Bereichen:

- TERRA CLOUD Housing
- TERRA CLOUD Hosting
- TERRA CLOUD IaaS
- TERRA CLOUD PaaS

- Es besteht eine aktive Internetverbindung (hierdurch können weitere Kosten entstehen).
- Der Kunde hat Zugriff auf das TERRA CLOUD Center und das TERRA CLOUD Netzwerk.
- Der Kunde stellt einen kompetenten und entscheidungsbefugten Ansprechpartner zur Verfügung.
- Der Kunde meldet pro aktiv die Mitarbeiter, deren Zugänge in das TERRA CLOUD Center in Zukunft nicht mehr benötigt bzw. genutzt werden, damit diese gelöscht werden können.
- Der Kunde akzeptiert die Löschung infizierter Dateien innerhalb der Datenablagen.
- Der Kunde trägt die Verantwortung für die Datenqualität der zur Verfügung gestellten Personen- und Organisationsdaten.
- Der Kunde stellt sicher, dass die Rufnummern von den Anwendern inkl. Durchwahl korrekt hinterlegt werden.

Trifft eine der hier beschriebenen Voraussetzungen nicht zu, ist die TERRA CLOUD nicht verpflichtet, den beschriebenen Service mit den vereinbarten Service Leveln zu erbringen.

Diese Mitwirkungspflichten werden grundsätzlich in einer Qualität erbracht, die es der TERRA CLOUD erlaubt, ohne Mehraufwand die vertraglichen Verpflichtungen zu erfüllen. Verzögerungen der Leistungserbringung und/oder Verletzungen der vereinbarten Service Level, die auf die Nichterfüllung der Mitwirkungspflichten durch den Kunden zurückzuführen sind oder die nicht von der TERRA CLOUD zu vertreten sind, gehen nicht zu Lasten der TERRA CLOUD.

5 Preise

Die TERRA CLOUD stellt ihre Leistungen indirekt über den Fachhandel der WORTMANN AG zur Verfügung. Sämtliche Preise entnehmen Sie bitte der aktuellen Preisliste oder erhalten Sie über Ihren TERRA Fachhändler.

6 Vertragslaufzeit

Der Vertrag beginnt mit Übergabe der Zugangsdaten an den Kunden. Es besteht keine Mindestvertragslaufzeit. Der Vertrag verlängert sich automatisch um einen Monat sofern er nicht mit einer Frist von 4 Wochen zum Ende der Mindestvertragslaufzeit bzw. zum Ende der Folgelaufzeit gekündigt wird.

7 Abrechnung

Die Berechnung erfolgt ab Übergabe der Zugangsdaten an den Kunden. Abrechnungszeitraum ist monatlich. Angefangene Monate werden als volle Monate berechnet. Die Rechnungsstellung für alle feststehenden Artikel erfolgt am ersten Werktag des Folgemonats. Alle verbrauchsbasierenden Artikel werden zum 15. des Monats ermittelt und am ersten Werktag des Folgemonats in Rechnung gestellt, sofern der Verbrauchsmessung nicht binnen 14 Tagen schriftlich widersprochen wird.

8 Service Paket

Die TERRA CLOUD betreibt ein Systems Management Center (SMC), in dem alle Aufgaben des täglichen Betriebes abgewickelt werden. Das SMC ermöglicht den Betrieb von Kunden-Systemen an 365 Tagen im Jahr, 24 Stunden pro Tag (7*24 Stunden).

Das Systems Management Center betreibt und administriert die Server- und Storage-Systeme im vereinbarten Umfang. Der bediente Betrieb findet von Montag bis Freitag 8:00 – 17:00 Uhr (ausgenommen bundeseinheitliche Feiertage) statt.

8.1 Servicezeiten und Kontaktdetails

Die Call-Annahme erfolgt 24/7, auch an Sonn- und Feiertagen. Calls können per Email oder über das Ticketsystem abgesetzt werden.

Service Zeiten	Allgemeine Ticket Annahme: 24x7x365 Ticket Annahme mit Support-Unterstützung: 12x7x365 (Montag bis Sonntag 08:00 – 20:00 Uhr)
Verfügbare Sprachen	Deutsch, Englisch
Call-Annahme über:	
Telefon	+49 5744 944-850
Email	support@terracloud.de

8.2 Call-Annahme

Die Call Annahme nimmt die Anfrage via Telefon oder Email innerhalb der vereinbarten Servicezeiten entgegen. Für die Call Annahme muss die Kundennummer, Paketnummer und die System ID des Servers angegeben werden. Anhand der angegebenen Daten identifiziert der Service Desk Mitarbeiter den Kunden mit den im System hinterlegten Kontaktdaten und führt die Validierung des Anspruchs auf die betroffene Service Leistung durch.

Jede Email oder Telefongespräch wird automatisch als Service Request in einer Datenbank erfasst. Jede eingehende Meldung wird im Ticketsystem als ein Ticket mit einer eindeutigen Ticketnummer (ID) erstellt. Die Ticketnummer wird dem Melder als Referenznummer mitgeteilt. Anschließend führt der Service Desk Mitarbeiter eine Kategorisierung und Priorisierung der Anfrage durch. Anhand der Priorisierung wird eine angemessene Support-Reaktionszeit festgelegt, die innerhalb der bedienten Arbeitszeiten liegt.

In Abhängigkeit der Klassifizierung nach Change Request oder Incident (Unterbrechung des Service/technischer Defekt) kommen weiter Prozessschritte zum Tragen.

8.3 Incident Management (Unterbrechung des Service/technischer Defekt)

Im Falle eines Incidents wird der Service Desk Mitarbeiter die technische Diagnose durchführen und versuchen mit Hilfe einer Knowledge Datenbank sofort eine Lösung zu finden. Die erfolgreiche Lösung sowie die durchgeführten Lösungsschritte werden dokumentiert und nach Beseitigung der Störung wird der Incident geschlossen. Der Kunde wird über die Behebung der Störung informiert. Sollte eine sofortige Lösung nicht möglich sein, werden alle bisherigen Maßnahmen dokumentiert und der Vorgang an nachgelagerte Instanzen (2nd Level Support oder System Management Center) weitergeleitet. Bei einer Weiterleitung wird der Incident vom Service Desk über die gesamte Service Zeit proaktiv überwacht, um anhand eines definierten Eskalationsprozesses die Einhaltung der vereinbarten Service Level sicherzustellen. Nach erfolgreicher Lösung eines Incidents und Schließung des Tickets im System wird der Kunde darüber informiert.

8.4 2nd Level Support

Der 2nd Level Support bearbeitet Incidents und Fragen zum vereinbarten Produktumfang, die nicht im First Level Support gelöst werden konnten. Die Leistungen des 2nd Level Supports beinhalten:

- Bearbeiten von Anfragen vom Service Desk durch Spezialisten der TERRA CLOUD sofern Sie nicht durch andere Serviceprovider bearbeitet werden.
- Ggf. Nachstellen der Fehlersituation und Durchführen von Incident-Analysen.
- Ggf. Rückruf des Incident-Melders beim Kunden durch einen Spezialisten der TERRA CLOUD.
- Ggf. telefonische Unterstützung des Kunden bei Incidents und Bedienerfragen zum vereinbarten Produktumfang.
- Weiterleiten der nicht gelösten Anfragen an nachgelagerte Instanzen.

9 SLA

Es gelten die SLAs des Hauptproduktes.

9.1 Service Level

Die Vereinbarung von Service Level Agreements (SLA) bildet eine vertragliche Basis zwischen dem Auftraggeber und der TERRA CLOUD bzgl. der Leistungserbringung Firewall.

Service-Betrieb: 24/7

Bediente Service-Zeit: Mo-Fr 8:00-20:00 MEZ

Service Level Verfügbarkeit: Die Verfügbarkeit der Infrastruktur im Rechenzentrum der TERRA CLOUD. Messpunkt der Verfügbarkeit ist der Ausgang des TERRA CLOUD Rechenzentrums (außerhalb der Wartungszeiten). Die Service Level Verfügbarkeit wird pro Kalendermonat für die bereitgestellte Leistung gemessen.

Um eine Wartung der zugrundeliegenden Systeme durch die TERRA CLOUD zu ermöglichen ist ein wöchentliches Wartungsfenster eingerichtet.

Geplante Wartungsfenster:	Mo.-Fr.: 18:30 – 22:30 Uhr
	Sa.: 6:00 – 10:00 Uhr

Ein Firewall Paket gilt als betriebsfähig bereitgestellt, wenn dem Kunden durch die TERRA CLOUD die zur Einrichtung nötigen Informationen mitgeteilt wurden. Entsprechend der Bestellung werden zu diesem Zeitpunkt ggf. die Authentifizierungsdaten übergeben.

Die Verfügbarkeit einer Firewall gilt als gegeben, wenn die entsprechende Serverinfrastruktur aus dem Netz der TERRA CLOUD erreichbar ist bzw. das Volume läuft. Die Messung der Verfügbarkeit erfolgt auf Basis der Performance- und Statusüberwachung der Serversysteme über das System Management der TERRA CLOUD.

Die TERRA CLOUD kann Änderungen an der Software und/oder Hardware Systemen außerhalb der Wartungsfenster durchführen, wenn diese nicht zur Beeinträchtigung der vereinbarten Verfügbarkeit führen.

10 Sonstige Bestimmungen

Es gelten die Allgemeinen Geschäftsbedingungen der TERRA CLOUD die jeweils aktuelle Preisliste und die Leistungsbeschreibungen.