Leistungsbeschreibung

Multi-ISP Internet Connect inkl. DDoS-Protection

für die
Techniker Krankenkasse

Inhaltsverzeichnis

Präambel

(1) Die Techniker Krankenkasse („TK“ oder „AG“) ist mit ca. 12,2 Millionen Versicherten die größte gesetzliche Krankenkasse Deutschlands und verfügt über rund 230 bundesweit verteilte Standorte unterschiedlicher Größe. Als gesetzliche Krankenversicherung ist der AG eine Körperschaft des öffentlichen Rechts mit Selbstverwaltung. Zum neunzehnten Mal in Folge wurde der AG als "Deutschlands beste Krankenkasse" ermittelt (Focus-Money Ausgabe 07/2025).

(2) Der AG plant im Zuge der kontinuierlich wachsenden Bedeutung von resilienter Internetkonnektivität den Aufbau einer Multi-ISP Internet Access Lösung, welche die zwei Rechenzentren des AG innerhalb von Hamburg durch einen Generalunternehmer („AN“) mit hochverfügbarer Internetanbindung über zwei verschiedene Internet Service Provider (ISPs) versorgt. Ein zentrales Merkmal der geforderten Lösung ist, dass die Internetanbindung auch einen DDoS-Protection Service durch einen vom Bundesamt für Sicherheit in der Informationstechnik (BSI)-zertifizierten DDoS-Mitigation-Dienstleister beinhaltet. Alternativ zur Liste der BSI-zertifizieren DDoS- Mitigation -Dienstleister kann der AN schriftlich nachweisen, dass er eine BSI-zertifizierte DDoS-Mitigations-Lösung in seiner Hoheit betreibt. Der Generalunternehmer übernimmt die vollständige Verantwortung für den Aufbau, die Bereitstellung und den störungsfreien Betrieb der Lösung inkl. Managed-Router-Hardware in beiden RZs des AG.

(3) Die vorliegende Leistungsbeschreibung definiert die Anforderungen an den Multi-ISP Internet Access mit höchsten Sicherheits- und Verfügbarkeitsanforderungen. Die Kombination aus redundanter ISP-Anbindung, BSI-zertifiziertem DDoS-Schutz und professionellem Router-Management stellt sicher, dass kritische Geschäftsprozesse auch bei Ausfällen oder Cyberangriffen kontinuierlich verfügbar bleiben.

1. Ausgangssituation & Netzwerk-Architektur

(4) Der AG hat einen modularen Netzwerkaufbau. Dabei werden Systeme, abhängig von ihrer Funktion und Klassifizierung, in verschiedenen Netzwerk-Modulen angeschaltet. Die einzelnen Module (logische Einheiten) werden über die zentrale Core-Infrastruktur miteinander verbunden und das Routing zwischen den Modulen wird ebenfalls über den Core über ein dynamisches Routingprotokoll sichergestellt. Für die IP-Kommunikation wird ein privates Netz (10.0.0.0/8) verwendet. Das installierte IP-Netz gehorcht den Vorgaben eines vorhandenen Adressierungs- und Routing-Konzeptes. Next-Generation-Firewall-Systeme inkl. Intrusion Prevention Systeme (IPS)-Technik werden eingesetzt. Das Datacenter-Netzwerk des AG erstreckt sich über zwei physisch getrennte Rechenzentren (RZ), welche über Dense Wavelength Division Multiplexing (DWDM)-Strecken miteinander verbunden sind. Die Redundanz über Rechenzentren zeigt sich in der untenstehenden Abbildung durch eine Spiegelung auf der X-Achse.

(5) Zur Terminierung der Internet-Anbindungen hat der AG das Netzwerkmodul DMZ aufgebaut (sog. DMZ (Demilitarisierte Zone)). Der Aufbau des Moduls ist schematisch in Abbildung 1: dargestellt.

(6) Die heute vorhandene Single-Homed-Anbindung erreicht tagsüber ca. 3 Gbit/s eingehend und 5 Gbit/s ausgehend, nachts 0,5 Gbit/s ein- und ausgehend.

(7) Die dargestellten Dienste und Systeme werden in der Regelarbeitszeit (Montag bis Freitag, von 6 Uhr bis 17 Uhr) von Spezialisten des AG betreut, die auch in Störungsfällen den Second Level Support (SLS) stellen. Das Network Operation Center (NOC) des AG stellt den First Level Support und ist 24 Stunden am Tag erreichbar. Die Betriebsbereitschaft einzelner Anwendungen und Systeme beträgt 7x24 h an 365 Tagen (Servicezeitraum). Alle Störungen werden in einem AG-internen Ticketsystem dokumentiert.

(8) Der AG nutzt heute ein „Provider-gesponsertes AS (Autonomes System)“ für seinen "Provider Independent" (PI)-Address Space „193.22.180.0/22“ beim Réseaux IP Européens (RIPE). Der PI-Address Space des AG wird heute durch AS8881 von 1&1 Versatel per Border Gateway Protocol (BGP), bekanntgegeben. Die Anbindung dient dem AG heute als redundante Anbindung für beide Rechenzentren.

2. Leistungsgegenstand und dessen Abgrenzung

(9) Pflicht des AN sind die Planung, der Aufbau, die Bereitstellung und der störungsfreie Betrieb einer redundanten Internetanbindung auf Basis von zwei voneinander unabhängigen ISPs für die Rechenzentren des AG in Hamburg. Weiterhin stellt der AN sicher, dass die Internetanbindung gegen volumenbasierte DDoS-Angriffe auf Layer 3 & Layer 4 des ISO-OSI-Modells geschützt ist.

(10) Die technische Realisierung des IP-Routings und die Erreichbarkeit der öffentlichen IP-Adressen des AG erfolgt über das BGP, welches dafür sorgt, dass die Konnektivität des AG mit dem Internet auch bei Ausfällen einzelner Leitungen, ganzer ISPs oder des DDoS-Protection-Dienstes automatisiert gewährleistet wird.

(11) Konkret bedeutet dies, dass der PI-Address Space des AG per BGP über ein eigenes AS an die AS der beiden ISPs und damit dem Internet bekanntgegeben wird.

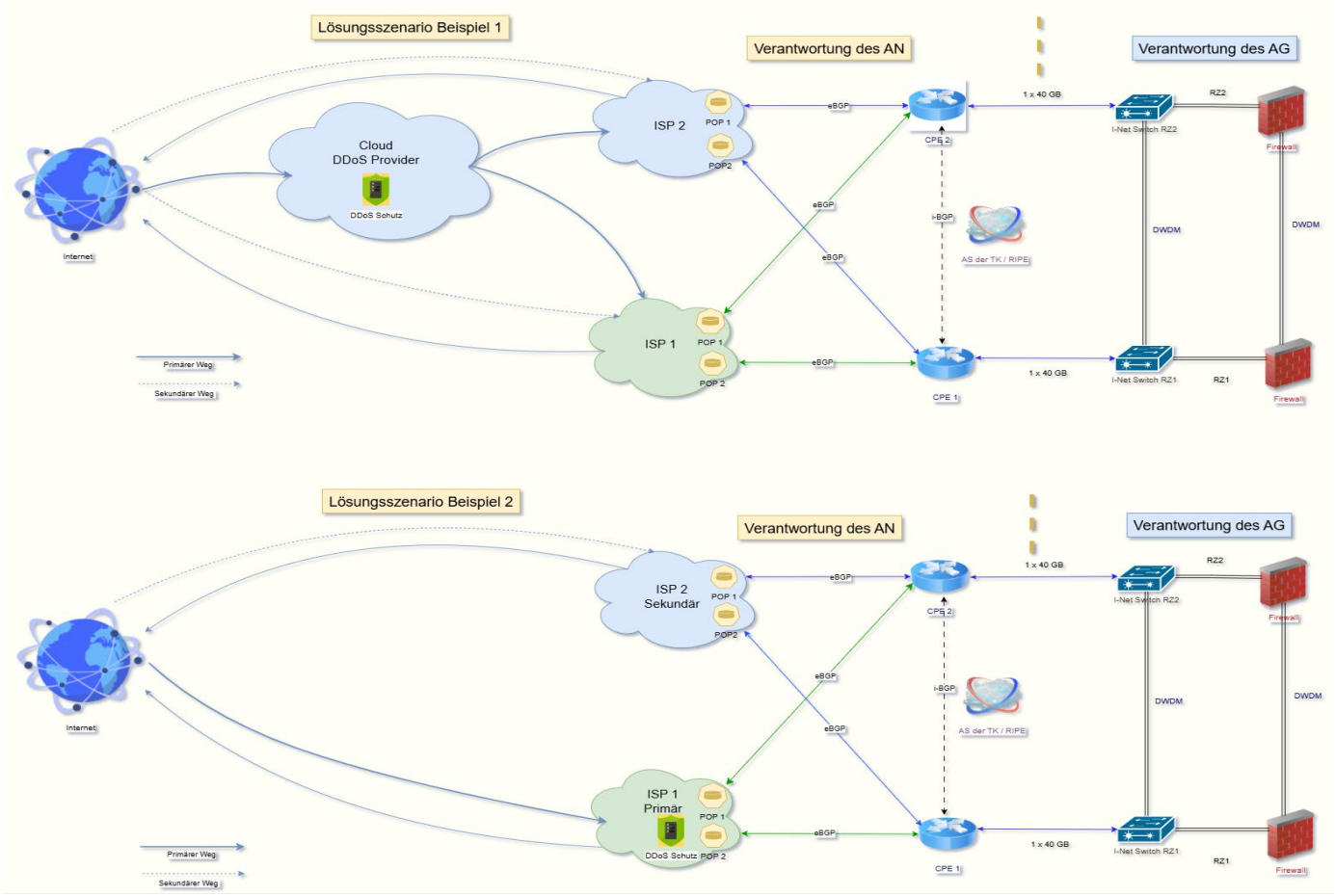

Abbildung 1: Mögliche Lösungsszenarien

(12) Hinweise:

(13) Die oben dargestellten Abbildungen stellen mögliche Lösungsszenarien dar und dienen dazu eine mögliche Realisierung der Anforderungen grafisch aufzuzeigen bzw. das Verständnis zu erleichtern.

(14) Ein Detailkonzept wird zwischen AG und AN im Rahmen des Projektes (vgl. Kapitel 6.1.2 Feinkonzeption) ausgearbeitet und vom AN dokumentiert, wobei alle Anforderungen der LB erfüllt sein MÜSSEN.

2.1. Realisierungskonzept

(15) Der AN hat die in der Leistungsbeschreibung genannten Anforderungen an die technische Realisierung des Multi-ISP Internet Connect inkl. DDoS-Protection auf der Grundlage des von ihm mit dem Angebot eingereichten Realisierungskonzepts (siehe Anlage A3) umzusetzen.

3. Aufbau der Internetanbindung

(16) Im folgenden Kapitel werden die Leistungsmerkmale der geforderten Internetanbindung und Anforderungen an die ISP's beschrieben.

3.1. Leistungsmerkmale der Internetanbindung

(17) Die Anbindung des AG an das Internet MUSS über zwei verschiedene ISP's realisiert sein, wobei jeder der beiden ISPs an jedes der beiden RZ angebunden wird (insgesamt 4 Leitungen).

(18) Für jeden der beiden ISP's MÜSSEN die Leitungen in die beiden RZ des AG in geografisch getrennten Trassen geführt sein.

(19) ISP 1 und ISP 2 MÜSSEN technisch, wirtschaftlich, rechtlich und organisatorisch vollständig getrennte Organisationen sein, sodass es keinerlei Abhängigkeiten bei einer Störung eines ISPs geben darf (vgl. auch § 2 Abs. 1 des Vertrags).

(20) Jeder der beiden ISP's MUSS mehrfach (d.h. mindestens zwei Mal) an zentrale, öffentliche Peering Points (auch Internet Exchange Points (IXPs) genannt) wie z.B. DE-CIX Hamburg, DE-CIX Frankfurt oder AMS-IX Amsterdam mit Bandbreiten jeweils ≥ 100 Gbit/s angebunden sein. Mindestens zwei dieser Peering Points MÜSSEN in Europa und einer davon in Deutschland sein.

(21) Zusätzlich zu öffentlichen Peering Points MUSS jeder ISP über mindestens 50 private Peerings mit anderen ISPs, Firmen bzw. Content Providern in Deutschland verbunden sein.

(22) Jeder der beiden ISP's MUSS über private Peering mit Cloud Anbieter wie zum Beispiel Microsoft, Amazon, Oracle, IBM und Google mit Bandbreiten von jeweils ≥ 100 Gbit/s verbunden sein. Insgesamt MUSS jeder ISP mindestens 3 Cloud Anbieter über private Peerings angebunden haben und Microsoft Azure MUSS darunter sein.

(23) Der AN MUSS die Hochverfügbarkeit seiner Leistung sicherstellen. Der AN stellt durch die redundante Auslegung der Internet-Access-Kommunikationsinfrastruktur sicher, dass es beispielsweise durch einen einfachen Ausfall (z.B. eines Knotens oder einer Kante) zu keiner Beeinträchtigung der Service-Verfügbarkeit des Internet-Access kommt.

(24) Die technische Realisierung der redundanten Provideranbindung erfolgt pro ISP über geografisch getrennte Points of Presence (POPs). Die beiden POPs der ISP's MÜSSEN sich an zwei unterschiedlichen Standorten befinden, die mindestens 100 Kilometer (Luftlinie) voneinander entfernt sind. Diese Anforderung MUSS für jeden der beiden ISP's erfüllt sein. Hierbei kann z.B. jeder ISP einen POP in Hamburg und einen in Hannover haben.

(25) Die Standorte der beiden RZs lauten:

- RZ1: Bramfelder Str. 140, 22305 Hamburg
- RZ2: q.beyond AG, Grasweg 62-66, 22303 Hamburg

(26) Alle aktiven Komponenten, welche an der Multi-ISP Internet Connect inkl. DDoS-Protection Leistung beteiligt sind (z.B. Netzabschluss, Router, Switches, Appliances etc.), sind mit einer internen Redundanz auszustatten. Dies umfasst insbesondere die Ausstattung mit redundanten Netzteilen. Alle Komponenten in den Räumlichkeiten des AG bzw. der q.beyond AG MÜSSEN von dem AN in 19-Zoll Racks (maximale Einbautiefe 105 cm) eingebaut werden.

(27) Die Lösung MUSS ein DDoS-Protection Service enthalten. Dabei kann entweder ein Cloud-basierter DDoS-Protection Service Provider eingesetzt werden oder der DDoS-Protection Service wird von einem der beiden ISPs selbst erbracht.

(28) Der AG kann für die CPE-Systeme zwischen den beiden RZs eine transparente Layer-2 Verbindung auf Basis einer vorhandenen DWDM Switching-Infrastruktur mit Bandbreiten bis zu 100Gbit/s zur Verfügung stellen.

(29) Weitere Anforderungen hinsichtlich der Verfügbarkeit während des Betriebs finden sich im Kapitel 5.

3.2. Bandbreite

(30) Der AN legt die notwendige Hard- und Software und damit die mögliche Bandbreite von Vertragsbeginn an auf mindestens 40 Gbit/s aus.

(31) Der AG ruft zunächst eine Bandbreite der Anbindung von mind. 20 Gbit/s für jede Leitung zu den PoPs ab. Auf Anforderung des AG wird der AN während des Vertragslebens Bandbreitenerhöhungen durchführen (vgl. §2 Abs. 15 des Vertrages).

(32) Seitens des AN handelt es sich bei der zur Verfügung gestellten Bandbreite um eine Datenübertragungsflatrate. Alle Bandbreitenangaben sind symmetrisch (Upload- und Downloadgeschwindigkeiten sind identisch) und beziehen sich bei dem Wert auf eine Richtung (Beispiel: 20 Gbit/s bedeutet eine Bandbreite von 20 Gbit/s in Download- und gleichzeitig 20 Gbit/s in Upload-Richtung).

(33) Die für den AG nutzbare Bandbreite der Leitungen MUSS der vertraglich festgelegten Bandbreite entsprechen und jederzeit (24/7) mit voller Kapazität zur Verfügung stehen.

3.3. Performance

(34) Der AN hat die Hard- und Software der Internet-Access Anbindung so zu dimensionieren, dass die vereinbarten Netzgüteparameter sowie Bandbreiten vollumfänglich erfüllt werden. Der AG behält sich vor, diese Werte durch eine Integration in seine eigenen (Performance) Monitoring Systeme regelmäßig zu überprüfen.

(35) Der AN gewährleistet die unten genannten Netzgüteparameter auf Basis einer bis max. 10% ausgelasteten Leitung und Ping-Paketen von 100 Byte.

(36) Jeder ISP stellt in seinem Backbone dauerhaft mindestens ein Testsystem z.B. einen iPerf Server bereit, mit dem die Performance (Round Trip Time, Jitter und Paketverlust) der Anbindung von dem AG regelmäßig überprüft werden kann.

3.3.1. Round Trip Time (RTT)

(37) Da sich sowohl die Internetanbindung des AG über die beiden RZ, als auch die Gegenseite für ein- bzw. ausgehende IP-basierte Kommunikation zum weitaus überwiegenden Teil in Deutschland befinden, werden kleine Latenzen für alle innerdeutschen Verbindungen im Backbone des jeweiligen ISPs gefordert:

(38) Der AN MUSS sicherstellen, dass das Round Trip Time für solche Verbindungen im Durchschnitt maximal **15 ms** beträgt. Gemessen wird die Strecke zwischen einem der CPE Systeme in Hamburg und einem Messpunkt im Backbone des ISP. Diese Strecke MUSS mind. 400 km (Luftlinie) Entfernung betragen.

3.3.2. Jitter

(39) Der AN MUSS sicherstellen, dass die Jitter-Paketverzögerung für die RZ-Anbindung maximal **5 ms** beträgt. Gemessen wird wie im Absatz Round Trip Time beschrieben.

3.3.3. Frameverlustrate

(40) Der AN MUSS sicherstellen, dass die Frameverlustrate für die RZ-Anbindung **<1%** beträgt. Gemessen wird wie im Absatz Round Trip Time beschrieben.

3.4. Managed Router

(41) Der AN stellt an beiden Rechenzentrumsstandorten des AG professionelle Router/Switches der Enterprise-Klasse (nachfolgend CPE-Systeme genannt) zur Verfügung. Alle ISP-Leitungen, die in einem Rechenzentrum terminieren, MÜSSEN auf einem CPE-System angeschaltet sein. Diese MÜSSEN für Multi-Homing-Szenarien ausgelegt sein und folgende Mindestanforderungen erfüllen:

- ASIC-basierte Switching-/Routing-Kapazität ≥ 40 Gbit/s, folgende SFP-Module sind möglich: **QSFP-40G-SR-BD** (40G BiDi, MMF-SR, LC Connector) oder **QSFP-40/100-SR-BD** (40G / 100G BiDi, MMF-SR, LC Connector). Die Anbindung an die Switching-Infrastruktur des AG erfolgt mit wahlweise 40 Gbit/s oder 100 Gbit/s.
- BGPv4 und IPv6-Unterstützung mit Multi-Path-Routing (Unterstützung von BGP-Multipath und sowohl AS-Path Länge als auch weiterer BGP-Attribute zur zielnahen Weiterleitung mit Präferenz bevorzugter Wege).
- Routing-Tabelle: ≥ 50.000 für IPv4 und IPv6-Routen
- Unterstützung sowohl der BGP-Attribute "AS Path Length" und „MED“ als auch weiterer Metriken, um Präferenzen für ein- als auch ausgehende Wege zu konfigurieren.
- Hot-Standby und Failover-Funktionalität (HSRP/VRRP), um für die Firewalls und andere Systeme des AG ausgehend in Richtung Internet ein statisches IP-Routing zu ermöglichen
- Redundante Stromversorgung (zwei interne Netzteile, C13 - C14 Kaltgerätestecker oder C14 - C15 Warmgerätestecker, keine externen Steckernetzteile)
- Redundante Lüftereinheiten (Luftrichtung Front to Back)

(42) Der AN SOLL dem AG via SNMP v3 lesenden Zugriff auf System- und Interfacestatistiken der CPE-Systeme bieten.

(43) Der AN MUSS entweder dem AG via SSH lesenden Zugriff auf die CPE-Systeme bieten, um bestimmte „show“-Befehle ausführen zu dürfen ODER alternativ MUSS der AN ein „Looking Glass“ per Webinterface zur Verfügung stellen, um solche „show“-Befehle ausführen zu können.

(44) Die via „Looking Glass“ oder SSH zur Verfügung gestellten Befehle MÜSSEN die nachfolgend aufgeführten Informationen des jeweiligen CPE-Routers anzeigen. Eine vergleichbare Alternative ist zulässig. In Klammern ist als Erläuterung der entsprechende CLI-Befehl angegeben, der von marktführenden Herstellern im Bereich Routing und Switching verwendet wird, um die jeweiligen Informationen

anzuzeigen. Alle aufgeführten Befehle MÜSSEN sowohl für IPv4 als auch IPv6 zur Verfügung stehen.

- Anzeige aller IP-Routen mit nächstem Hop (show ip route)
- Detaillierte Anzeige der IP-Route für ein(e) gegebene IP-Adresse bzw. Netzwerk (show ip route a.b.c.d)
- Übersicht der BGP-Nachbarn und deren Status (up/down), Remote AS, Anzahl empfangene und gesendete Prefixe, Uptime. (show ip bgp summary)
- Detaillierte Informationen zu einem bestimmten BGP-Nachbarn mit Status (up/down, Prefix-Anzahl, Uptime). (show ip bgp neighbors a.b.c.d)
- Anzeige der BGP Routing Tabelle mit BGP Attributen wie z.B. AS-Path, best path, LocalPref und MED (show ip bgp)
- Detaillierte Anzeige der BGP Routing Tabelle für ein(e) gegebene IP-Adresse bzw. Netzwerk (show ip bgp a.b.c.d)
- ICMP-Echo vom CPE-Router zu einer angegebenen IP-Adresse (Zielhost), um Erreichbarkeit und RTT zu prüfen. (ping a.b.c.d)
- Anzeige der Hops vom CPE-Router zu einer angegebenen IP-Adresse (Zielhost) inkl. Latenzen je Hop (traceroute a.b.c.d)

(45) Über Features wie z.B. IP SLA-Monitoring in Kombination mit BGP Routing MUSS die Erkennung und eine passende Reaktion bei "Brown Out"-Szenarien möglich sein, bei denen eine Verbindung zwar physisch besteht, aber degradiert ist. In diesem Fall SOLLen automatisch nur die verbleibenden stabilen und nicht beeinträchtigten Verbindungen genutzt werden.

(46) Falls die oben spezifizierte Erkennung eines „Brown Out“ Szenarios nicht funktioniert, MUSS auf Anforderung des AG über das Management der CPE-Systeme eine manuelle Abschaltung von Leitungen möglich sein.

(47) Das Management der CPE Systeme MUSS so konzipiert sein, dass die Administration durch den AN bzw. den eingebundenen Dienstleister auch bei einer Störung im Netzwerk möglich ist (Out-of-Band Management).

(48) Die Details zur Anbindung und Konfiguration mit Präferenzen, o.a. Features werden zwischen AG und AN im Rahmen des Projektes (vgl. Kapitel 5.11.2 Feinkonzeption) ausgearbeitet und vom AN dokumentiert.

3.5. Öffentliche IP-Adressen des AG und derzeitiges IP-Routing

(49) Der AG verfügt mit dem Netz 193.22.180.0/22 bereits über öffentliche IPv4-Adressen, die providerunabhängig geroutet werden können (PI Address Space).

(50) Derzeit werden diese öffentlichen IPv4-Adressen durch den ISP 1&1 Versatel und dessen AS 8881 im BGP-Routing bekanntgegeben.

(51) Der AG ist Mitglied der RIPE und in der Lage, ein eigenes AS zu beantragen. Der AG verfügt über einen Zugang zum LIR Webportal des RIPE.

(52) Die bereits vorhandenen providerunabhängigen öffentlichen IPv4-Adressen und neue providerunabhängige öffentliche IPv6-Adressen des AG MÜSSEN diesem neuen AS zugeordnet werden. Der AG beantragt vor oder während des Realisierungszeitraumes entsprechende IPv6 Adressen.

(53) Der AN unterstützt und berät den AG bei den erforderlichen Schritten und notwendigen Einträgen im Webportal des RIPE, um eine reibungslose Migration bei der Inbetriebnahme zu ermöglichen.

(54) Der AG übernimmt die Kommunikation mit dem bestehenden ISP 1&1 Versatel und unterstützt den AN bei der Migration. Siehe Kapitel 5.11.5 Migration der operativen Umgebung.

(55) Sofern für die Realisierung der vom AG gewünschten Hochverfügbarkeit oder für die Überwachung von Leitungen und Wegen o.ä. weitere IPv4 Adressen benötigt werden, werden diese vom AN zur Verfügung gestellt. Diese IPv4 Adressen sind öffentlich, sofern dies für die Umsetzung erforderlich ist.

3.6. IP-Adressierung & IP-Routing für CPE-Systeme

(56) Für die Anbindung der Systeme des AG (z.B. Firewalls, VPN-Gateways oder Load-Balancer) an die CPE-Systeme stellt der AG für IPv4 ein öffentliches IP-Netz bereit, welches aus einem Subnetz des öffentlichen IP-Netzes des AG besteht. Für dieses Netz stellt der AG in jedem RZ einen Layer 2 Switch bereit, an den die CPE-Systeme physikalisch angebunden werden. Diese beiden Switches sind über DWDM-Technik miteinander breitbandig und hochverfügbar gekoppelt.

(57) Der AG stellt auf Anforderung dem AN z.B. für eine Koppelung der beiden CPE-Systeme weitere IP-Transfernetze bzw. VLANs zur Verfügung.

(58) Das ausgehende IPv4-Routing von Systemen des AG (z.B. Firewalls, VPN-Gateways oder Load-Balancer) auf die CPE-Systeme erfolgt statisch. Hierfür stellt der AN auf den CPE-Systemen zwei HSRP bzw. VRRP-Gruppen mit zugehörigen virtuellen IP-Adressen bereit, wobei die eine virtuelle IP-Adresse bevorzugt über CPE 1 und die andere IP-Adresse über CPE 2 geroutet wird. Die notwendigen IP-Adressen werden vom AG aus dem o.a. öffentlichen IPv4-Netz des AG bereitgestellt. Bei Ausfall eines CPE-Routers MUSS die virtuelle IP-Adresse inkl. Virtueller MAC-Adresse auf den verbleibenden CPE-Router innerhalb von 3 bis maximal 10 Sekunden umschwenken. Die virtuelle IP-Adresse MUSS ebenfalls in dieser Zeitspanne umschwenken, sofern ein CPE-System die Verbindung zu dem oder den ISP's verliert.

(59) Das eingehende IPv4-Routing von den CPE-Systemen zu den Systemen des AG (z.B. Firewalls, VPN-Gateways oder Load-Balancer) erfolgt ebenfalls statisch. Hierfür konfiguriert der AN auf den CPE-Systemen statische Routen zu IP-Subnetzen aus dem öffentlichen IP-Netzes des AG nach Vorgabe.

(60) Der AN ermöglicht dem AG eine Überwachung der Verfügbarkeit der einzelnen Leitungen per ICMP.

(61) Alle Details zum IP-Routing und zur IP-Adressierung für die öffentlichen IP-Adressen des AG werden sowohl für IPv4 als auch für IPv6 gemeinsam von dem AG und dem AN im Rahmen des Projektes (vgl. Kapitel 5.11.2 Feinkonzeption) ausgearbeitet und vom AN dokumentiert.

3.7. BGP-Routing

(62) Das IP-Routing für die öffentlichen IP-Adressen des AG erfolgt dynamisch über BGP. Der AN konfiguriert BGP auf den CPE-Systemen nach Vorgaben des AG. Alle Details (wie z.B. Equal Cost Multi-Path (ECMP) oder Routing Präferenzen bestimmter Leitungswege) werden gemeinsam von dem AG und dem AN im

Rahmen des Projektes (vgl. Kapitel 5.11.2 Feinkonzeption) ausgearbeitet und vom AN dokumentiert.

(63) Abhängig von der Einbindung eines dedizierten Providers für DDoS-Protection bzw. Erbringung des DDoS Schutzes durch einen der beiden ISPs kann z.B. über BGP Announcements von spezifischeren IP-Routen zu den öffentlichen IP-Adressen des AG für den präferierten und gewünschten Weg sichergestellt werden, dass im Normalbetrieb eingehende IP-Pakete z.B. immer über den Cloud DDoS Anbieter oder einen der beiden ISPs erfolgen. Die beiden ISPs MÜSSEN hierfür spezifischere IP-Routen für die öffentlichen IP-Adressen bei dem AG berücksichtigen, damit alle IP-Pakete zum AG an den Anbieter des DDoS Schutzes gesendet werden und ein vollständiger DDoS Schutz mit korrekter Erkennung von Schwellwerten möglich ist, obwohl eine direkte Koppelung zum Netz des AG besteht.

(64) Die BGP-Konfiguration MUSS so erfolgen, dass bei Ausfall einer ISP-Verbindung bzw. Ausfall beim Provider für DDoS Schutz automatisch auf die verbleibende Verbindung umgeschaltet wird. Die Konvergenzzeit darf dabei 180 Sekunden nicht überschreiten. Hierbei MUSS bei jedem möglichen Ausfallszenario (Ausfall des Providers für DDoS Schutz, des ISP 1 oder ISP 2) gewährleistet sein, dass der AG sowohl ein- als auch ausgehend mit dem Internet verbunden bleibt.

(65) Die öffentlichen IP-Adressen des AG sollen durch parallele Nutzung von RIPE Route Objects und RPKI ROA (Resource Public Key Infrastructure Route Origin Authorization) Einträgen vor Missbrauch geschützt werden. Daher MUSS der AN den AG bei der Implementierung und dem Betrieb von Route Origin Validation (ROV) unterstützen.

4. Aufbau der DDoS-Protection

(66) Die Lösung MUSS einen DDoS-Protection Service auf Layer 3 und 4 des OSI 7-Schichten Modells beinhalten, welcher die öffentlichen IP-Adressen (IPv4 + zukünftig auch IPv6) des AG gegen volumenbasierte Angriffe schützt. Ein Aufbrechen von TLS-Verbindungen im Netz des DDoS Anbieters oder ISPs ist nicht zulässig.

(67) Die DDoS-Protection MUSS volumetrische Angriffe automatisch erkennen und automatisch mitigieren, darunter mindestens nach heutigem Kenntnisstand: UDP-Floods, ICMP-Floods, TCP-basierte State-Exhaustion-Angriffe (insb. SYN-, ACK- und RST-Floods) sowie UDP-basierte Reflection/Amplification-Angriffe, u. a. über DNS, NTP, SSDP, rpcbind oder vergleichbare Protokolle bzw. Angriffe.

(68) Es kann entweder ein eigenständiger DDoS-Protection Service vom AN eingesetzt werden oder der DDoS-Protection Service wird von einem der beiden ISPs erbracht. Nachfolgend wird der DDoS-Protection Service erbringende ISP auch als primärer ISP bezeichnet, da der gesamte eingehende IP-Traffic im Normalfall über diesen ISP erfolgen muss, damit Schwellwerte korrekt erkannt werden können.

(69) Ausgehender IP-Traffic **darf** für die DDoS-Erkennung genutzt werden, es wird jedoch nur der eingehende Clean-Traffic für die Preisbildung einbezogen (siehe Preisblatt, Positionen 3.1 bis 3.7).

(70) Eine DDoS-Protection Lösung, welche zwei oder mehr unterschiedliche Monitoring-Portale (vgl. Kapitel 5.3.3) für DDoS Schutz enthält, ist **nicht** zulässig.

(71) Eine Lösung für DDoS-Protection, die keine aggregierte Sicht über ein Portal mit Summe aller eingehenden IP-Pakete in Statistiken und Grafiken enthält, ist **nicht** zulässig.

(72) Für die Erkennung eines Angriffes MÜSSEN von dem AG Schwellwerte sowohl für einzelne IP-Adressen als auch IP-Subnetze (sog. Zielobjekte) definiert werden können.

(73) Pro Zielobjekt MÜSSEN mindestens Schwellwerte für die Bandbreite granular in Mbit/s bzw. Gbit/s und Paketen pro Sekunde definierbar sein.

(74) Zur Vermeidung von Mitigationen bei kurzzeitigen Bursts SOLL das Messintervall pro Zielobjekt konfigurierbar sein.

(75) Weiterhin MUSS eine Nachlaufzeit für den DDoS-Schutz vom AG definiert werden können. Dieser Zeitraum beschreibt, wie lange die technischen Maßnahmen aktiv sein MÜSSEN, um die IP-Adressen bzw. IP-Subnetze nach Ende eines DDoS-Angriffs weiterhin zu schützen, auch wenn kein erneuter Angriff vorliegt. Der Zeitraum MUSS in Stundenschritten definiert werden können bis mindestens 12 Stunden. Vor Ablauf der Nachlaufzeit MUSS der AN erneut auf Schwellwertverletzungen prüfen und ggf. eine nahtlose Verlängerung einleiten.

(76) Falls in den beiden RZ des AG zusätzliche Systeme zur Analyse von Flows und/oder Scrubbing von eingehendem IP-Datenverkehr eingesetzt werden, dann sind diese Systeme als physikalische Appliances (nicht virtualisiert) bereitzustellen und es gelten die gleichen Anforderungen wie für CPE-Systeme (u.a. gilt dies für Stromversorgung und -kabel, Rackeinbau und SFPs, Redundante Stromversorgung siehe Kapitel 3.4 Managed Router).

(77) Die eingehende Verbindung vom Internet zum AN MUSS zwischen DDoS Anbieter und den beiden ISPs hochverfügbar und resilient aufgebaut sein, so dass Störungen im Netzwerk bei einem der ISPs erkannt werden und eingehende IP-Pakete vom Internet zum AG im Störungsfall ausschließlich über den verbleibenden, funktionalen Weg geroutet werden. Eine aktive Erkennung von Störungen und Verbindungsproblemen MUSS dabei z.B. über IP SLAs und Probing enthalten sein. Falls der DDoS Schutz durch einen der beiden ISPs erbracht wird, gelten die gleichen Anforderungen für die internen Verbindungen innerhalb des Netzwerkes des ISPs.

(78) Es dürfen bei der Verbindung zwischen DDoS Anbieter und ISP keine Tunneltechnologien eingesetzt werden, die die mögliche maximale IP-Paketgröße von 1500 Bytes (ohne MAC-Header) einschränken. Falls der DDoS Schutz durch einen der beiden ISPs erbracht wird, gelten die gleichen Anforderungen für die internen Verbindungen innerhalb des Netzwerkes des ISPs. Eingehend vom Internet zum AG MÜSSEN IP-Pakete mit einer Größe von 1500 Bytes immer unterstützt werden.

(79) Während einer aktiven Mitigation MUSS die Möglichkeit bestehen, gezielt einzelne Packet-Traces (z.B. PCAP) als Stichprobe eines DDoS-Angriffs zu erzeugen und zu speichern, um forensische Analyse und Angriffsklassifikation zu ermöglichen, ohne die laufende Mitigation zu unterbrechen oder negativ zu beeinflussen.

(80) Ein Packet-Trace SOLL während eines DDoS Angriffes von der DDoS Lösung automatisch erstellt werden. Das Packet-Trace soll dabei mindestens 1GB an Datenpaketen enthalten, um dem AN eine Analyse dieser Stichprobe zu ermöglichen.

(81) Der DDoS-Protection Service MUSS eine standardisierte Möglichkeit via HTTPs/TLS bieten, ein Security Information and Event Management System

(SIEM) des AG anzubinden. Der AN MUSS innerhalb von maximal fünf Minuten nach Mitigationsstart über die Anbindung ans SIEM ein Event mit entsprechender Meldung absetzen und SOLL ab dann fortlaufend alle 60 Sekunden über die laufende Mitigation erneut Events an das SIEM des AG absetzen. Nach Abschluss der Mitigation MUSS der AN ebenfalls ein Event zur Beendigung der Mitigation an das SIEM absetzen. Die Details der technischen Anbindung werden zwischen AN und AG im Rahmen der Feinkonzeptionsphase abgestimmt.

4.1. Bandbreite

(82) Unter dem Begriff „Clean-Traffic“ versteht der AG den legitimen, validen Datenverkehr, der nach der Filterung durch Sicherheitsmechanismen der DDoS-Protection wie Scrubbing-Center von schädlichem Traffic getrennt wurde. Im Rahmen der DDoS-Abwehr wird eingehender Netzwerkverkehr analysiert und anormale oder böswillige Pakete herausgefiltert, sodass nur der gewünschte, nicht-angreifende Verkehr zum Zielsystem weitergeleitet wird. "Clean-Traffic" umfasst dabei überwiegend Anfragen von authentischen Nutzern und Systemen, die den normalen Betriebsfluss repräsentieren, während DDoS-Komponenten, manipulierte Requests und sonstige Angriffsvektoren ausgefiltert werden.

(83) Im Fall von laufenden DDoS Angriffen MUSS eingehend zum AG die bei „Clean-Traffic“ angegebene Bandbreite (vgl. Preisblatt) gewährleistet sein. Der AN muss die Abwehrbandbreite entsprechend dimensionieren.

(84) Die Abwehrbandbreite bezeichnet die maximale Datenmenge pro Sekunde, die die DDoS-Protection-Lösung effektiv filtern, absorbieren und von legitimen Anfragen trennen kann, bevor die Schutzmechanismen oder die Infrastruktur des AN selbst überlastet werden.

(85) Die Abwehrbandbreite MUSS DDoS-Angriffe mit einem Volumen von mindestens 2 Tbit/s mitigieren können.

(86) Der AG ruft zunächst eine Clean-Traffic Bandbreite von 10 Gbit/s ab. Auf Anforderung des AG wird der AN während des Vertragslebens Bandbreitenerhöhungen durchführen (vgl. §2 Abs. 16 des Vertrages).

4.2. Aktivierung und Deaktivierung DDoS-Schutz

(87) Der DDoS-Schutz MUSS automatisch und damit ohne manuelle Interaktion aktiv werden. Um dies zu ermöglichen, MÜSSEN die zum AG eingehenden IP-Pakete z.B. über Flow-Daten kontinuierlich analysiert werden. Bei der Überschreitung von eingestellten Schwellwerten für eine öffentliche IP-Adresse oder eines IP-Netzes (Bandbreite oder Pakete pro Sekunde) MUSS der eingehende Datenverkehr an Scrubbing Engines weitergeleitet werden, die eine Filterung übernehmen und IP-Pakete von Angreifern verwerfen.

(88) Während einer laufenden Mitigation dürfen die definierten Performance-Metriken (vgl. Kapitel 3.3 Performance) überschritten werden. Die RTT darf um maximal 15 Millisekunden, Jitter um maximal 10 Millisekunden erhöht werden. Dem AG ist bewusst, dass in diesem Fall erhöhte Frameverlustraten auftreten können.

(89) Die Aktivierung der Schutzfunktionen, d.h. die Filterung eingehender Datenpakete über Scrubbing Engines MUSS automatisch nach Überschreitung der definierten Schwellwerte innerhalb von maximal einer („1“) Minute erfolgen. Zusätzliche BGP-

Konvergenzzeiten, die außerhalb des Einflussbereichs des AN liegen, werden nicht berücksichtigt bzw. nicht auf diesen Zeitraum angewandt.

(90) Neben der automatischen Mitigation MUSS eine manuelle Aktivierung des DDoS-Schutzes per Telefon beim Support oder über ein DDoS Web-Portal für bestimmte IP-Adressen oder IP-Adressbereiche möglich sein, um damit präventive Schutzmaßnahmen ergreifen zu können.

(91) Die Dauer der Schutzfunktionen bei manueller Aktivierung SOLL im Bereich von 1h bis 24h einstellbar sein.

(92) Eine laufende Mitigation MUSS per Telefon beim Support oder über ein DDoS Web-Portal manuell ausschaltbar sein.

5. Betrieb Multi-ISP Internet Connect inkl. DDoS-Protection

5.1. Managed Service

(93) Der AN erbringt für den AG einen vollständig gemanagten Internetzugangsdienst („Fully Managed Service“) auf Basis einer Multi-ISP-Architektur, wie in den vorhergehenden Kapiteln beschrieben. Ziel ist die Bereitstellung einer hochverfügbaren, skalierbaren und abgesicherten Internetanbindung mit integrierter DDoS-Protection. Der AN stellt hierzu sämtliche benötigten Komponenten, einschließlich der aktiven Netzwerktechnik (z.B. CPEs, Router), in den RZs des AG bereit, betreibt und überwacht diese im Rahmen der vereinbarten SLAs und beschriebenen Leistungen.

(94) Der Service wird durch den AN vollverantwortlich betrieben. Alle technischen und administrativen Aufgaben zur Sicherstellung der Verfügbarkeit, Performance und Sicherheit liegen im Verantwortungsbereich des AN. Der AG erhält Schnittstellen für Reporting und Eskalationen, bleibt jedoch von operativen Tätigkeiten vollständig entlastet.

(95) Der vollständige Lifecycle der Router-Hardware und -Software liegt daher auch in der Verantwortung des AN. Dies umfasst mindestens regelmäßige Firmware-Updates, Sicherheitspatches und Hardware-Monitoring. Der AN stellt durch einen Lifecycle-Prozess sicher, dass die eingesetzte Hard- und Software nach einer Bekanntgabe eines End of Sale (“EOS”) Datums durch den Hersteller nur noch so lange eingesetzt wird, wie für die Hard- und Software sowohl Support als auch Ersatzteile bzw. Sicherheitspatches vom Hersteller bereitgestellt werden. Der AN plant einen Austausch von Systemen ein und informiert den AG zeitnah.

(96) Alle Konfigurationsänderungen MÜSSEN dokumentiert und über ein Change Management System beim AN abgewickelt werden. Backup-Verfahren für Konfigurationen sind zu implementieren, wobei Änderungen zu neuen Backup-Versionen führen MÜSSEN. Jedes Backup MUSS mindestens 3 Monate und SOLL mindestens 12 Monate aufbewahrt werden.

5.2. Verfügbarkeit und Redundanz

(97) Es wird eine permanente Verfügbarkeit (24 Stunden am Tag, 365 Tage im Jahr) der Gesamtlösung gewährleistet.

(98) Dies bedeutet insbesondere, dass der AN Wartungsfenster und Supportintervalle und deren Anzahl, Dauer und Umfang so gering wie möglich zu halten hat.

Wartungsarbeiten sind dem AG vom AN mindestens zehn (10) Werktage im Voraus per E-Mail anzukündigen.

(99) Wartungsarbeiten dürfen **keine** Auswirkung auf die Service-Verfügbarkeit des gesamten Multi-ISP Internet Connect inkl. DDoS-Protection haben, sondern nur auf einzelne Bestandteile der Lösung, d.h. eine Verringerung der Redundanzen für den Wartungszeitraum.

(100) Wartungsarbeiten sind nur außerhalb des geltenden Arbeitszeitkorridors des AG zulässig (Arbeitszeitkorridor des AG: Montag bis Samstag 5:00 bis 23:00 Uhr). Ausnahmen bedürfen der individuellen Absprache mit AG.

(101) Der AN gewährleistet für die gesamte Lösung eine kalendermonatliche Verfügbarkeit von mindestens **99,97% (maximal 13 Minuten Ausfallzeit pro Monat)**, wobei sich die kalendermonatliche Verfügbarkeit nach folgender Formel berechnet:

$$Verfügbarkeit = \frac{Messperiode\ [Minuten] - Ausfallzeit\ [Minuten]}{Messperiode\ [Minuten]} * 100\%$$

Die Messperiode in Minuten ergibt sich durch die Multiplikation der Anzahl der Tage des Monats x 24 Stunden x 60 Minuten. Die Ausfallzeit in Minuten bezieht sich wiederum auf die Dauer der Nichtverfügbarkeit im betrachteten Monat.

(102) Der AN MUSS für jeden Kalendermonat in tabellarischer Form einen SLA-Report erstellen und per E-Mail an den AG senden. Dieser MUSS bis zum fünften Werktag des folgenden Kalendermonats dem AG zur Verfügung gestellt werden. Der SLA-Report MUSS folgende Informationen beinhalten:

- Störungstyp (Teilausfall/Totalausfall)
- Beginn der Störung (Datum und Uhrzeit)
- Ende der Störung (Datum und Uhrzeit)
- Beschreibung
- Lösung
- Vergütungsminderung § 7 des Vertrags
- Maßnahmen zur Prävention zukünftiger Ausfälle

(103) Die SLA-Reports der abgeschlossenen Kalendermonate seit dem letzten Service Meeting bilden die Grundlage für das jeweils nächste Service-Meeting (vgl. Kapitel 5.11.7 Regelmäßige Service Meetings).

(104) Der AN MUSS zur Inbetriebnahme durch Redundanz- und Performancetests die Qualität seiner Leistung nachweisen (vgl. Kapitel 5.11.4 Tests Parallelaufbau)

(105) Während des Vertragslebens hat der AG das Recht, Redundanz- und Performancetests der Anbindung durchzuführen. Dies erfolgt in lastarmen Zeiten und in engster Abstimmung mit dem AN.

5.2.1. Service-Level

(106) In der nachfolgenden Tabelle sind die Service-Level aufgeführt, die der AN im Rahmen der Störungsbearbeitung einhalten MUSS.

	Störungstyp	
	Teilausfall nach u.a. Definition	**Totalausfall nach u.a. Definition**
Servicebereitschaft	Montag bis Freitag (mit Ausnahme von Feiertagen (Bundesland Hamburg)) 06:00 bis 18:00	7 x 24 Stunden (inkl. aller Feiertage)
Reaktionszeit	1 Stunde	15 Minuten
Zwischenmeldung	bei Statusänderung	alle 30 Minuten
Einhaltung vereinbarter Termine	+ 1 Stunde	+ 1 Stunde
Wiederherstellungszeit	nächster Arbeitstag (Mo. – Fr.)	4 Stunden
Rückmeldungsfrist nach Beendigung der Störung	1 Stunde	1 Stunde

Tabelle 1: Störungstypen in der Übersicht

(107) Die Begriffe werden wie folgt definiert:

Teilausfall

Ein Teilausfall definiert sich dadurch, dass die Gesamtfunktion der Lösung nicht beeinträchtigt ist, jedoch ein Teil der Lösung gestört und dadurch beispielsweise die Redundanz eingeschränkt ist. Dies sind insbesondere aber nicht abschließend:

- Störung oder Ausfall einer Leitung
- Störung oder Ausfall eines redundanten CPE-Equipments (inkl. Interfaces zum AG)
- Störung oder Ausfall eines ISPs
- Beeinträchtigung der Internetanbindung von bzw. zum AG
- Reduzierte Bandbreite der Internetanbindung zwischen 50% und 100%

- sporadische/temporäre Störungen. Solche Störungen können sich durch Verzögerungen, Paketverluste, Verbindungsabbrüche (von TCP-Verbindungen) oder kurzzeitige Unterbrechungen äußern und beeinträchtigen meist nur vorübergehend den normalen Netzwerkbetrieb.

Totalausfall

(108) Ein Totalausfall definiert sich dadurch, dass die Gesamtfunktion der Lösung oder eines Services nicht gegeben oder eingeschränkt ist. Dies sind insbesondere aber nicht abschließend:

- jegliche Ausfallkonstellation, bei der die Internetkonnektivität des AG gestört ist.
- Reduzierte Bandbreite der Internetanbindung unter 50%.
- Störung im IP-Routing, welche dafür sorgt, dass einige Ziele im Internet nicht erreichbar sind und Ursache der Störung im Verantwortungsbereich des AN.
- Störung im IP-Routing, welche dafür sorgt, dass mind. eine aktive IP-Adresse des AG aus dem Internet eingehend nicht mehr erreichbar ist und Ursache der Störung im Verantwortungsbereich des AN.
- Störung oder Ausfall des DDoS-Protection Service
- Gleichzeitiger Ausfall aller ISP-Anbindungen, beispielsweise durch großflächige Glasfaserunterbrechungen, Stromausfälle oder Routing-Störungen, die beide ISPs betreffen.

Servicebereitschaft

(109) Zeitrahmen, in dem Serviceleistungen erbracht werden MÜSSEN.

Reaktionszeit

(110) Frist, innerhalb der während der Servicebereitschaft nach Meldungseingang mit der Störungsbeseitigung begonnen wird.

Zwischenmeldung

(111) Der AN hat innerhalb des definierten Zeitraums Statusmeldungen zur Störung an der AG abzugeben.

Einhaltung vereinbarter Termine bei Technikereinsatz

(112) Durch den AN einzuhaltende Termintreue bei Vereinbarung eines Technikereinsatzes vor Ort.

Wiederherstellungszeit

(113) Zeit zur Wiederherstellung der vollständigen Betriebsbereitschaft durch den AN. Maßgebend für die Wiederherstellung sind die Zeitpunkte im Ticketsystem des AN, die die Öffnung des Supporttickets bzw. die Behebung der Störung angeben. Die Frist gilt nicht für eine von dem AG zu vertretende Beeinträchtigung oder bei vertragsgemäß angekündigten Wartungsarbeiten (vgl. Kapitel 5.2.1 Service-Level).

Rückmeldung nach Beendigung der Störung

(114) Pro Störungsmeldung sind vom AN Support-Tickets zu erstellen. Dem AG MUSS deren Verfolgung vom AN ermöglicht werden (via Lomnido-Schnittstelle im Ticket-System des AG, siehe Anlage L2 Kopplung Ticketsystem). Die tatsächlichen Störungs-, Reaktions- und Wiederherstellungszeiten sind vom AN zu dokumentieren.

Nichteinhaltung von Reaktions- und Wiederherstellungsfristen

(115) Bei Nichteinhaltung von Terminen, Reaktions- und Wiederherstellungsfristen ist eine schriftliche Stellungnahme durch den AN zu erstellen. Die schriftliche Stellungnahme MUSS zeitnah (d.h. maximal 7 Tage) nach Beendigung der Störung an den AG übergeben werden und folgende Sachverhalte darlegen:

- Ursache
- Lösung
- Prävention

5.3. Web-Portale

5.3.1. Allgemeine Anforderungen an Web-Portale

(116) Webportale MÜSSEN eine 2-Faktor Authentifizierung (TOTP-Token) zum Schutz der Anmeldung von lokalen Nutzerkonten bieten.

(117) Die 2-Faktor Authentifizierung MUSS entweder verbindlich für jeden User aktiviert sein oder über ein Audit MUSS der AG überprüfen können, dass alle registrierten User des AG für diesen Dienst die 2-Faktor Authentifizierung aktiviert haben.

(118) Der AN SOLL eine Anbindung der Web-Portale per SSO an Microsoft Entra ID des AG unterstützen (technische Details siehe Anlage Pflichtenheft, Kapitel „Identity und Access Management“).

(119) Es MÜSSEN mindestens 30 individuelle Userkonten des AG unterstützt werden.

5.3.2. Internetanbindungen

(120) Zur Optimierung des Betriebes und zur Überprüfung der definierten Netzgüteparameter hat der AN Echtzeit-Statistik-Daten über folgende Punkte auf elektronischem Wege (online und performant, z.B. durch Webportal, sog. „Monitoring-Portal“) dem AG in Form von Tages-, Wochen- und Monatscharts zur Verfügung zu stellen:

- Bandbreiten-Auslastung
- Performance-Parameter Frameverlustrate

(121) Die zur Verfügung gestellten Statistiken und Charts der Internetanbindungen MÜSSEN mindestens für die letzten 3 Monate online einsehbar sein.

(122) Für die statistische Erfassung von Ausfallzeiten gilt darüber hinaus Folgendes: Zum Nachweis der Einhaltung der im Vertrag geforderten Verfügbarkeiten hat der AN den AG über jeden Ausfall einer Leitung unverzüglich per E-Mail zu informieren, den Ausfall jeweils auf Tageschart-Basis minutengenau festzuhalten und in die entsprechende Statistik einzupflegen. Die zu benachrichtigende Mail-Adresse oder Mail-Adressen werden im Rahmen des Kickoff-Termins von dem AG mitgeteilt.

5.3.3. DDoS-Protection

(123) Für den Service DDoS-Protection MUSS der AN ein webbasiertes Portal anbieten, welches auch bei Störungen der Internet-Anbindung bzw. der DDoS-Protection des AG z.B. über einen unabhängigen Internetzugang (z.B. via LTE) erreicht werden kann.

(124) Die Konfiguration von Schwellwerten SOLL über ein Webportal für DDoS-Schutz durch den AG möglich sein.

(125) Falls eine Konfiguration von Schwellwerten nicht über ein Webportal möglich ist, MUSS der AG eine Änderung von Schwellwerten über ein Formular per E-Mail, Ticket-System oder telefonisch an den Support des DDoS Anbieters übermitteln können. Die Umsetzung wird vom AN nach der Konfiguration per E-Mail bestätigt.

(126) Die Änderung von Schwellwerten ist für den AG immer kostenneutral.

(127) Die konfigurierten Schwellwerte für einzelne IP-Adressen bzw. IP-Netze MÜSSEN im Webportal einsehbar sein. Jede konfigurierte IP-Adresse bzw. IP-Netz MUSS mit einem Bezeichner versehen werden können.

(128) Die konfigurierten Bezeichner (symbolische Namen) SOLLEN im Webportal in den Statistiken neben den IP-Adressen bzw. IP-Netzen angezeigt werden können. Dies kann z.B. über eine eingeblendete Legende, „Hover over“ per Maus o.ä. realisiert werden.

(129) Innerhalb des Webportals MÜSSEN Statistikdaten für eingehende IP-Pakete einsehbar sein. Diese MÜSSEN mindestens folgende Informationen jeweils für die

Top 10 auf Basis der eingehenden Bandbreite als einzelne Graphen darstellen oder vergleichbare Informationen:

- Bandbreite (Gbit/s) pro Ziel-IP des AG
- Pakete/s pro Ziel-IP des AG
- Pakete/s pro Herkunftsland der Quelle
- Pakete/s pro AS (Autonomes System) der Quelle
- Pakete/s pro Protokoll (z.B. TCP, UDP, ESP, ICMP)
- Pakete/s pro Ziel-Port
- Pakete/s pro Quell-Port

(130) Das Webportal MUSS eine Filtermöglichkeit bieten, um die angezeigten Statistiken auf eine einzelne Ziel IP-Adresse (statt den Top 10) zu beschränken und die o.a. Graphen spezifisch für diese IP-Adresse zu sehen.

(131) Das Webportal SOLL eine Filtermöglichkeit bieten, um die jeweils angezeigte Statistik auf einen einzelnen Graphen zu beschränken.

(132) Die Skalierung SOLL sich automatisch jeweils an die angezeigten Graphen anpassen.

(133) Das Webportal SOLL den gesamten eingehenden Datenverkehr mit Bandbreite (Gbit/s) als auch Pakete/s anzeigen.

(134) Das Intervall der angezeigten Zeitspanne MUSS granular konfigurierbar sein, so dass die Statistikdaten in mehrere Abstufungen zwischen 1h und 24h angezeigt werden können.

(135) Das Intervall SOLL z.B. über Heranzoomen oder Einstellung des Intervalls auf Minutenebene anpassbar sein.

(136) Das Start- oder Enddatum und -uhrzeit der angezeigten Statistiken MUSS konfigurierbar sein.

(137) Das Zeitintervall von Dashboards MUSS regelmäßig aktualisiert werden, sofern Live-Daten angezeigt werden.

(138) Genaue Werte zu einzelnen Punkten der Graphen SOLLEN z.B. durch „Hoover over“ mit der Maus angezeigt werden können.

(139) Die genannten Statistiken MÜSSEN als Rohdaten mit einer Genauigkeit von maximal einer Minute erfasst werden (mind. 1 Wert pro Minute).

(140) Die neusten Statistikdaten dürfen maximal 10 Minuten alt sein.

(141) Es MUSS eine Exportfunktion für die Statistikdaten als .csv mit einer Genauigkeit von maximal einer Minute vorhanden sein (mind. 1 Wert pro Minute).

(142) Die genannten Statistikdaten als Rohdaten SOLLEN für mindestens 30 Tage vorgehalten und exportierbar sein.

(143) Die genannten Statistikdaten als Rohdaten MÜSSEN für mindestens 14 Tage vorgehalten und exportierbar sein.

(144) Das Webportal MUSS den Status von Mitigationsmaßnahmen anzeigen.

(145) Das Webportal MUSS die Möglichkeit bieten, Berichte für die Mitigationszeiträume mit den o.a. Statistiken im PDF-Format für mindestens 12 Monate nach der Mitigation herunterzuladen.

(146) Das Zeitintervall für Berichte SOLL sich an die jeweiligen Mitigationszeiträume automatisch anpassen, um die Informationen möglichst detailliert darstellen zu können.

(147) Das Webportal MUSS ein Audit-Log führen, welches alle Änderungen und Aktionen im System unveränderlich ablegt und damit protokolliert.

(148) Das Webportal MUSS eine umfangreiche Dokumentation und Hilfefunktion bieten.

5.4. Proaktives Monitoring und Benachrichtigung

(149) Der AN MUSS eine proaktive Überwachung wichtiger Leistungsbestandteile einrichten, welche Störungen zeitnah erkennt.

(150) Bei einer Störung MUSS der AN nach spätestens 15 Minuten eine Störungsmeldung in Form eines Störungstickets zum AG absetzen. Eine Reaktion seitens des AN MUSS in den im Kapitel 5.2.1 Service-Level genannten Zeiten erfolgen.

(151) Der DDoS-Protection Service MUSS bei Start und Beendigung einer DDoS-Mitigation automatisiert eine Alarmierung per SMS versenden. Die Alarmierung MUSS innerhalb von maximal fünf Minuten nach Erkennung des jeweiligen Ereignisses erfolgen und an einen vom AG definierten Empfängerkreis gerichtet sein.

(152) Der DDoS-Protection Service MUSS im Rahmen der Störungsbehebung eine Unterstützung des Security Operation Center (SOC) des AG bei länger anhaltenden Angriffen zur Eindämmung und Optimierung von Gegenmaßnahmen beinhalten.

5.5. Netzwerksicherheit

(153) Die Vertraulichkeit der Daten, die Datenintegrität und die Authentizität der Kommunikationsendpunkte sowie die Verfügbarkeit sind die obersten Ziele beim Aufbau und Betrieb der Mutli-ISP Connect inkl. DDoS-Protection.

(154) Der AN stellt sicher, dass von unberechtigter Seite kein Zugriff auf die dem AG zur Verfügung gestellten Transportwege, beteiligte Komponenten sowie Systeme möglich ist. Dies gilt insbesondere auch für andere Kunden des AN (Mandantentrennung).

(155) Der AN hält während der gesamten Vertragslaufzeit die jeweils aktuell gültige ISO/IEC 27001 Zertifizierung auf der Basis des BSI IT-Grundschutz aufrecht und weist dies dem AG auf Anforderung nach.

5.6. Mitwirkungsleistungen des AG

(156) Der AG ist verpflichtet, die für die erfolgreiche Leistungserbringung in seiner Sphäre erforderlichen Mitwirkungsleistungen zu erbringen.

(157) **Informationsbereitstellung**: Der AG stellt dem AN Dokumentationen der bestehenden Netzwerkinfrastruktur und IT-Systemlandschaft sowie Informationen zu IP-Adressbereichen, VLAN-Strukturen und Netzwerktopologie bereit.

(158) **Ansprechpartner**: Der AG benennt fachlich qualifizierte und entscheidungsbefugte Ansprechpartner für Netzwerk- und Sicherheitsfragen sowie administrative Belange. Auch nennt der AG dem AN Ansprechpartner für Support-Eskalationsprozesse (vgl. Kapitel 5.8.2).

(159) **Zutritt**: Der AG gewährt physischen Zutritt zu Räumlichkeiten für Installation und Wartung von entsprechenden Komponenten, z.B. CPE-Router. Für den Zugang ist eine vorhergehende (in der Regel mit 5 Tagen Vorlauf) Anmeldung beim AG erforderlich.

(160) **Technische Infrastruktur:** Der AG stellt dem AN entgeltfrei geeignete Räumlichkeiten bzw. Rack-Einbauplätze in ausreichender Anzahl mit Klimatisierung, Stromversorgung (Redundante Stromversorgung (230V/400V) mit USV-Anbindung) und Brandschutz für den Einbau seiner Komponenten zur Verfügung. Der AG macht exakte Standortangaben und deren Übergabepunkten für die Leitungsabschlüsse in den Gebäuden (Etage, Raumbezeichnung, Racknummer etc.).

(161) **Projektorganisation**: Der AG sorgt für den Aufbau einer gemeinsamen Projektorganisation mit dem AN und gewährleistet die Teilnahme an gemeinsamen Meetings und Arbeitsterminen.

5.7. Dokumentation

(162) Im Rahmen des Aufbaus der Multi-ISP Internet-Connect-Kommunikationsinfrastruktur inkl. DDoS-Protection MUSS der AN eine detaillierte Dokumentation anfertigen und dem AG in elektronischer Form spätestens innerhalb von 4 Wochen nach erfolgreicher Inbetriebnahme der Anbindung zur Verfügung stellen. Diese MUSS insbesondere folgende Bestandteile umfassen:

- Darstellung der eingesetzten Komponenten und Wegeführung auf der letzten Meile zu den beiden RZ des AG
- Detaillierte Darstellung der Netzwerkarchitektur und Topologie-Diagramme
- Router-Konfigurationsparameter inkl. Darlegung der BGP-Konfiguration
- Standard Operating Procedures (SOPs) für alle Betriebsprozesse
- Disaster Recovery und Business Continuity Pläne
- Sicherheitskonzepte und Incident Response Abläufe

(163) Die Dokumentation ist während der gesamten Vertragslaufzeit vom AN aktuell zu halten und dem AG in aktualisierter Form zur Verfügung zu stellen.

5.8. Support

(164) Der AN erbringt Supportleistungen gemäß den nachfolgenden Vorgaben und Service-Level. Ziel ist die Sicherstellung des stabilen Betriebs der Multi-ISP-Anbindung inkl. DDoS-Protection und Managed Router mit definierten Reaktions- und Lösungszeiten. Der AN als Hauptvertragspartner ist immer gegenüber dem AG für die Einhaltung des Service-Level verantwortlich und somit auch für die Trouble Ticketing System (TTS)-Kopplung. Selbst wenn der AN mehre Unterauftragnehmer hat bleit der AN an erster Stelle für die Supportleistungen.

5.8.1. Störungsannahme

(165) Im Standardverfahren MÜSSEN die Störungen auf Seiten des AN über ein TTS verwaltet werden. Die Ticketnummer MUSS dem AG mitgeteilt werden. Die gesamte Störfall-Bearbeitung ist mit dem TTS zu handhaben.

(166) Das TTS des AN MUSS eine Kopplung über eine Dataclearing Instanz, z.B. Lomnido (s. Anlage L2 Kopplung Ticketsystem) für die Anbindung an das Service-

Tool des AG "SMAX" zur Verfügung stellen. Die AN-seitigen Kosten für die Einrichtung und Nutzung dieser Schnittstelle trägt der AN.

(167) Grundsätzliche Anforderungen an das TTS sind im Folgenden:

- die Eröffnung eines neuen Support-Tickets
- das Hinzufügen von Anmerkungen an bereits bestehende Supporttickets
- das Ändern von Support-Ansprechpartnern in bestehenden Tickets
- das Eskalieren eines Tickets (Heraufstufen der Priorisierung)
- das Schließen von abgeschlossenen Tickets

(168) Der AG hat auch die Möglichkeit, Störungen telefonisch beim AN aufzugeben und erste Informationen über den Status aus Sicht des AN zur Störung zu erhalten. Die Aufnahme einer Störung wird vom AN durch die Benennung einer Störungsnummer quittiert. Der Störungsverlauf wird vom AN fortlaufend schriftlich dokumentiert und ist für den AG jederzeit einsehbar.

(169) Eine Übermittlung von Störungsmeldungen per Mail ist jederzeit möglich. Der AN stellt sicher, dass der Eingang per Mail (siehe Kapitel 5.2) mit einer ersten Stellungnahme zum Problem bestätigt wird.

5.8.2. Eskalationsprozesse und Ansprechpartner

(170) Der AN hat sein internes Support-Eskalationskonzept dem AG zum Kickoff-Termin vorzulegen. Der AN MUSS durch entsprechende organisatorische Maßnahmen sicherstellen, dass er die vertraglich vereinbarten Servicezeiten einhalten kann. Der Prozess wird gegenüber dem AG offengelegt und während der Vertragslaufzeit bei Bedarf aufgrund der gesammelten Erfahrungen verbessert. Der AN übergibt dem AG spätestens zwei Wochen vor Produktivsetzung der Netzwerkanbindung eine Eskalationsmatrix mit zuständigen Ansprechpartnern und Kontaktdaten (Telefonnummer und E-Mail-Adresse). Der AG nennt dem AN ebenfalls die zuständigen Ansprechpartner für den Eskalationsprozess.

(171) Der AN ist verpflichtet, den AG über selbst erkannte und von dem AG noch nicht gemeldete Störungen per Mail (Verteilerliste wird durch den AG bereitgestellt) zu informieren.

(172) Bei Ausfällen, die eine Vergütungsminderung gem. § 7 des Vertrags auslösen, ist für den AG jederzeit ein koordinierender Ansprechpartner einer angemessenen Eskalationsstufe des AN verfügbar.

(173) Sollten Ausfälle auftreten, werden die jeweils Verantwortlichen des AN offen und transparent über die Hintergründe und ihre Erkenntnisse berichten, um so dem Ziel einer schnellen und effizienten Fehlersuche zu dienen.

(174) Alle Ausfälle, die zu einer Einschränkung der vereinbarten Servicequalität geführt haben, MÜSSEN vom AN in Bezug auf die Ursachen genau untersucht werden. Die Ergebnisse sowie Maßnahmen zur Prävention werden dem AG erläutert bzw. mit dem AG abgestimmt.

(175) Für alle Ausfälle, die eine Vergütungsminderung gem. § 7 des Vertrags auslösen, ist eine abschließende schriftliche Stellungnahme in deutscher Sprache (per E-Mail) über Ursache, Präventionsmöglichkeiten sowie beabsichtigte Präventionsmaßnahmen erforderlich.

5.9. Anpassung an zukünftige Anforderungen

(176) Planung und Weiter-/Entwicklung sind wesentlicher Bestandteil einer partnerschaftlichen Geschäftsbeziehung. Es ist daher auch Aufgabe des AN, den AG regelmäßig hinsichtlich Möglichkeiten zur Verbesserung der Tele- und Datenkommunikation zu beraten. Insbesondere Hinweise auf technische Alternativen bzw. auf Möglichkeiten zur Kostenersparnis sind Bestandteil der Kundenbetreuung des AN.

(177) Die Vertragspartner sind sich darüber einig, dass im Verlauf der Entwicklung technologische Weiterentwicklungen, Anpassungen an veränderte Marktanforderungen oder neue gesetzliche Vorgaben berücksichtigt werden sollten. Notwendige Änderungen und Erweiterungen der gesamten Lösung sind in einem abgestimmten Änderungsprozess umzusetzen.

(178) Der AN MUSS bei der DDoS-Protection seine Angriffserkennung stets an die sich laufend verändernden Angriffsmuster anpassen und erweitern.

(179) Der AN MUSS die Abwehrbandbreite der DDoS-Protection ausreichend dimensionieren und regelmäßig anpassen, um einen ausreichenden Schutz gegen volumenbasierte Angriffe zu bieten.

(180) Während der Vertragslaufzeit wird es mit Blick auf die technischen Veränderungen in dem betreffenden Marktumfeld voraussichtlich erforderlich sein, das Preisblatt anzupassen.

(181) Für solche Veränderungen gelten folgende Vereinbarungen:

(182) - Eine Änderung/Erweiterung kann von beiden Seiten (AG oder AN) vorgeschlagen werden.

(183) - Die Aufnahme der Änderung/Erweiterung in das Leistungsverzeichnis MUSS von beiden Seiten (AN und AG) freigegeben werden.

(184) - Die Herausnahme einer Position bedarf der Zustimmung beider Seiten (AN und AG)

(185) Das Leistungsverzeichnis wurde vom AG mit großer Sorgfalt erstellt, gleichwohl ist es möglich, dass Leistungen versehentlich nicht aufgenommen wurden oder durch technische Entwicklungen nicht vorhersehbar waren. Unabhängig hiervon darf der Preis für diese Leistungen die Marktpreise im Sinne vom § 4 PreisVO 30/53 nicht übersteigen.

5.10. Überlassung von Geräten

(186) Der AN überlässt dem AG alle für die Nutzung der Leistungen – in den Räumlichkeiten des AG bzw. der q.beyond – erforderlichen Geräte (Netzabschluss, Router, Switch, Appliance etc.). Diese Geräte bleiben im Eigentum des AN. Die Geräte werden in speziellen, räumlichen Abschnitten der beiden Rechenzentren (sog. „Carrier-Räumen“) betrieben.

(187) Der AG stellt sicher, dass die überlassenen Geräte nur bestimmungsgemäß und nicht von unbefugten Personen benutzt werden.

(188) Nach Beendigung des Vertragsverhältnisses (einschließlich einer etwaigen Fortleistung gemäß § 9 des Vertrages) holt der AN alle überlassenen Geräte vom

betroffenen Aufstellungsort unverzüglich ab. Die Abholung erfolgt maximal 30 Kalendertage nach der Außerbetriebnahme am Installationsort.

(189) Projektorganisation und Servicemeetings

(190) Die Leistungen des AN zur Erreichung des vertraglichen Gesamtzwecks „Einführung und Betrieb einer Multi-ISP Internet Connect inkl. DDoS-Protection“ gemäß dieser Leistungsbeschreibung durchlaufen mehrere Phasen, um eine reibungslose Migration der bisherigen Lösungen auf die neue Lösung zu gewährleisten. Die nachfolgend beschriebenen Phasen sind bindend für die Umsetzung. Die detaillierte Zeitplanung stimmen die Vertragsparteien in der Vertragsdurchführung ab. Diese wird nach Freigabe der TK verbindliche Grundlage für die weitere Vertragsdurchführung.

(191) Bei der Erbringung der Leistungen hängt der Erfolg maßgeblich von einer sehr guten technischen und zeitlichen Abstimmung zwischen AN und AG ab. Daher werden im folgenden Kapitel Regelungen getroffen, wie diese Abstimmungen ablaufen MÜSSEN.

(192) Die Arbeitssprache zwischen dem AG und dem AN ist Deutsch. Die Dokumentationen und Berichte für den AG werden nur in deutscher Sprache verfasst.

(193) Unmittelbar nach Zuschlagserteilung bestimmen der AN und der AG jeweils einen Projektleiter sowie Vertreter, welcher allein und hauptverantwortlich Ansprechpartner während aller Phasen bis hin zur finalen Inbetriebnahme ist. Das Projektmanagement-Team des AN liefert dem AG während aller Projektphasen übersichtliche Tabellen und Dokumente zum jeweiligen Stand der Auftragsumsetzung und führt ggf. die Aufgaben zur Mitwirkung auf und teilt diese regelmäßig den Ansprechpartnern des AG mit.

5.11. Projektphasen für die Inbetriebnahme der Leistungen

5.11.1. Einmaliger Kickoff

(194) Der AG wird den AN unmittelbar nach der Zuschlagserteilung zu einem halbtägigen Abstimmungstermin (Kickoff) einladen, welcher spätestens 2 Wochen nach Zuschlagserteilung stattfinden wird. Zur Vorbereitung werden dem AN auf Nachfrage alle notwendigen Informationen und Details (z.B. Raumbezeichnung Carrierräume, Racknummer etc.) für die zu erbringende Leistung zur Verfügung gestellt, welche sich nicht aus der vorliegenden Leistungsbeschreibung ergeben.

(195) Der Termin (Inhalt und Ablauf) wird einvernehmlich zwischen AG und AN vereinbart und findet in den Geschäftsräumen des AG (Unternehmenszentrale TK), Bramfelder Straße 140, 22305 Hamburg statt.

(196) Am Termin werden seitens des AG technische sowie kaufmännische Mitarbeitende teilnehmen. Seitens des AN werden ebenfalls alle technischen und kaufmännisch-vertraglichen Projektbeteiligten teilnehmen.

(197) Im Rahmen des Kickoffs werden Details für die Umsetzung des Auftrages, inklusive Vorgehen und Terminplanung, einvernehmlich zwischen dem AG und dem AN festgelegt. Auf Anforderung durch den AG dokumentiert der AN die Ergebnisse der Abstimmung in Form eines Protokolls und stellt dieses dem AG zur Abstimmung zur Verfügung. Der AG prüft das Protokoll und stimmt dieses mit dem

AN ab. Danach gibt der AG das Protokoll frei. Mit Freigabe wird das Protokoll verbindlich für die weitere Leistungserbringung.

5.11.2. Fein-Konzeption

(198) Anhand der vorliegenden Leistungsbeschreibung und basierend auf dem Realisierungskonzept (vgl. Anlage A3) wird in dieser Phase das Fein-Konzept für die Projektdurchführung erstellt. Dies beinhaltet insbesondere die Festlegung wichtiger technischer Parameter für den Aufbau und Betrieb der Leistungen.

5.11.3. Parallelaufbau

(199) Der AN hat die Multi-ISP Internet Connect -Anbindung an den bestehenden RZ-Standorten des AG bereitzustellen. Diese neuen Anbindungen MÜSSEN unabhängig von der derzeit bestehenden Internetverbindung des AG betrieben werden.

(200) Im Einzelnen umfasst die Leistung mindestens folgende Arbeitsschritte:

- Erschließung der Rechenzentrumsstandorte des AG mit den für die Anbindung erforderlichen Leitungen und Übergabepunkten, sofern diese noch nicht vorhanden sind.
- Installation, Konfiguration und betriebsfertige Übergabe des projektbezogenen CPEs gemäß den technischen Vorgaben des AG.
- Der AG stellt für den Parallelaufbau einen öffentlichen IPv4-Adressbereich der Größe /24 aus seinem /22er IPv4-Adressbereich zur Verfügung. Der AN sorgt in Abstimmung mit dem AG für sonstige Voraussetzungen, damit der AG den IPv4-Adressbereich routen kann.
- Die Arbeiten erfolgen unabhängig vom laufenden Betrieb der bestehenden Internetanbindung des AG. Eine Beeinträchtigung des Produktivbetriebs ist auszuschließen.
- Nach erfolgreichem Abschluss des Parallelaufbaus erfolgt die Übergabe in den produktionsnahen Parallelbetrieb.

5.11.4. Tests Parallelaufbau

(201) Nach erfolgreicher Installation und Konfiguration MUSS der AN Funktions- und Performancetests zur Überprüfung der ordnungsgemäßen Bereitstellung, Erreichbarkeit, Stabilität sowie Leistungsfähigkeit der neuen Anbindung durchführen.

(202) Ziel ist der Nachweis, dass die neue Anbindung ordnungsgemäß, stabil und unabhängig von der bestehenden Internetverbindung des AG betrieben werden kann.

(203) Die Tests umfassen mindestens folgende Punkte:

- Überprüfung der physischen und logischen Erreichbarkeit der angeschlossenen Rechenzentrumsstandorte über die neue Anbindung.
- Messung und Dokumentation der Übertragungsparameter und Performancekriterien Round Trip Time, Jitter, Frameverlustrate und Bandbreiten-Durchsatz.
- Nachweis des gewünschten Failover-Verhalten bei Ausfall einzelner Komponenten durch strukturierte Ausfalltests.

- Überprüfung des ordnungsgemäßen Zusammenspiels mit der Netzwerkinfrastruktur des AG (Routing, Firewalls, Monitoring-Schnittstellen).

(204) Alle Testergebnisse sind durch den AN in einem schriftlichen Testprotokoll zu dokumentieren und dem AG vorzulegen. Erst nach erfolgreicher Abnahme durch den AG gilt die Parallelverbindung als abnahmefähig.

5.11.5. Migration der operativen Umgebung (Schwenk)

(205) Nach erfolgreichem Abschluss der Funktions- und Leistungstests erfolgt die kontrollierte Migration der neuen Internetanbindung in die produktive Umgebung des AG. Der AN hat den Schwenkablauf detailliert zu planen, mit dem AG abzustimmen und nach Freigabe des AG außerhalb der Regelarbeitszeit durchzuführen.

(206) Der Schwenk umfasst insbesondere folgende Maßnahmen:

- Erstellung eines abgestimmten Migrationsplans einschließlich Zeitfenster, technischer Schritte, Rückfallplan (Rollback-Konzept) und Kommunikationswege.
- Umsetzung des Plans im vereinbarten Zeitfenster, außerhalb der Regelarbeitszeit des AG.
- Umschaltung des produktiven Internetverkehrs von der bisherigen Anbindung auf die neue Multi-Provider-Internetverbindung unter Wahrung der Netzstabilität und Dienstverfügbarkeit.
- Überwachung sämtlicher System- und Netzparameter während und nach der Umschaltung zur Sicherstellung des ordnungsgemäßen Betriebs.
- Dokumentation der Migration einschließlich durchgeführter Prüfungen, Messergebnisse und etwaiger Abweichungen.

(207) Nach erfolgreicher Migration bestätigt der AN die dauerhafte Betriebsfähigkeit der Multi-ISP Internet Connect inkl. DDoS-Protection.

5.11.6. Gesamtabnahme und Inbetriebnahme

(208) Nach erfolgreicher Durchführung der Migration in die produktive Umgebung erfolgt die Gesamtabnahme der erbrachten Leistungen durch den AG. Der AN ist verpflichtet, sämtliche für die Abnahme erforderlichen Nachweise, Protokolle und Dokumentationen vollständig vorzulegen und die Betriebsbereitschaft der Lösung nachzuweisen.

(209) Die Gesamtabnahme umfasst insbesondere folgende Punkte:

- Prüfung der vollständigen Umsetzung aller vertraglich vereinbarten Leistungen einschließlich Leitungsbereitstellung, technischer Installationen, DDoS-Schutzmaßnahmen und Monitoring-Funktionen.
- Nachweis der erfolgreichen Durchführung aller Funktions-, Last- und Failover-Tests sowie der stabilen Betriebsaufnahme der neuen Anbindung.
- Kontrolle der korrekten Dokumentation der Netzarchitektur, Konfigurationen und Übergabepunkte.
- Überprüfung der Betriebs-, Wartungs- und Supportunterlagen sowie der definierten Kommunikations- und Eskalationswege.
- Durchführung eines gemeinsamen Abnahmetermins zwischen AG und AN mit protokollarischer Feststellung des funktionalen und betriebsfähigen Zustands.

(210) Die Abnahme der ordnungsgemäß in Betrieb genommenen Leistungen erfolgt per E-Mail durch den AG.

5.11.7. Regelmäßige Service Meetings während des Betriebs

(211) Die Parteien stimmen sich während des Betriebs regelmäßig im Rahmen von Service-Meetings ab. Diese Meetings finden regelmäßig vierteljährlich und zusätzlich aus konkretem Anlass auf Anforderung des AG remote statt und haben eine Dauer von ca. einer Stunde. Die notwendige Terminserie wird nach erfolgreicher Inbetriebnahme aufgesetzt.

(212) Der AN benennt einen verantwortlichen Service-Manager sowie Vertreter, welcher als zentraler Ansprechpartner für den AG dient.

(213) In den Service-Meetings werden Themen wie die aktuelle technische Auslastung, vergangene Ausfälle, zukünftige Wartungen oder Änderungen an den Leistungen des AN besprochen.

(214) Der AN protokolliert die Inhalte der Service-Meetings schriftlich. Nach Fertigstellung der Protokolle sendet der Ansprechpartner des AN das Protokoll unverzüglich per Mail an die Ansprechpartner des AG. Das Protokoll enthält je nach Einzelfall Details zu Auftragsinhalten (z.B. Bandbreitenanpassung oder Rechenzentrumsumzug) und zur Ressourcenplanung sowie Termine. Der AG hat das Recht, das Protokoll zu prüfen und Änderungen zu verlangen.

6. Schulungen für Betrieb und Administration

(215) Der AN bietet dem AG strukturierte Schulungen zu den Themen Betrieb und Administration der bereitgestellten Multi-ISP Internet Connect inkl. DDoS-Protection Leistungen anhand der nachfolgenden Anforderungen an. Die Schulungen erfolgen in deutscher Sprache und werden nach einem gemeinsam zwischen AG und AN festgelegten Ablaufplan durchgeführt.

6.1. Schulungsdauer und -kosten

(216) Die Schulungen umfassen jeweils 8 Stunden im Zeitraum von 9:00 Uhr bis 17:00 Uhr inkl. einer Stunde Pause. Sie kann von dem AG mit einem Vorlauf von 3 Wochen In Textform abgerufen werden. Die Schulungen werden separat vergütet (vgl. Pos 5.1 in Preisblatt). Voraussichtlich werden während der ersten 48 Monate ab Vertragsbeginn 1 bis 5 Schulungen abgerufen.

6.2. Teilnehmeranzahl

(217) Pro Schulung nehmen maximal zehn (10) Mitarbeitende des AG teil, um einen hohen individuellen Lerneffekt der Teilnehmenden zu gewährleisten.

6.3. Schulungsumgebung

(218) Die Schulungen finden in den Räumlichkeiten des AG in Hamburg statt. Nach Abstimmung können die Schulungen auch in den Räumlichkeiten des AN stattfinden. Eine gesonderte Vergütung von Reisekosten für den AN findet nicht statt.

(219) Der AN ist für die Bereitstellung der Schulungsunterlagen und die Durchführung der Schulungen verantwortlich.

(220) Der AN MUSS die die Schulungen sinnvolle und strukturierte Informations- und Begleitmaterialien vorbereiten und diese spätestens eine Woche vor Schulungstermin dem AG vorlegen. Die Unterlagen können in deutscher oder in englischer Sprache verfasst sein.

6.4. Schulungsinhalte und Ziele

(221) Ziel der Schulungen ist es, die Administratoren und IT-Experten des AN in allen technischen und organisatorischen Belangen der Multi-ISP Internet Connect inkl. DDoS-Protection Lösung zu schulen.

(222) Ein Teil der Schulung orientiert sich am konkreten Projektablauf und der Dokumentation der Schnittstellen zwischen AG und AN.

(223) Ein weiterer Teil der Schulungen ist die praxisorientierte Einführung in die Monitoring- und Managementtools durch Live-Demos und praxisnahe Übungen für die Teilnehmenden.

(224) Dies beinhaltet insbesondere:

- die Architektur und Funktionsweise der eingesetzten Multi-ISP Internet Connect inkl. DDoS-Protection zu erläutern. Dabei MUSS mindestens auf die Routing-Mechanismen und das Redundanzkonzepte eingegangen werden.
- die Performance- und Betriebsparameter der Multi-ISP Internet Lösung anhand der entsprechenden Web-Portale zu erläutern.
- die eingesetzten DDoS-Schutzmechanismen (Erkennung, Abwehr, Monitoring) zu erläutern, sodass eine qualifizierte Überwachung mithilfe des entsprechenden Web-Portals möglich ist.
- Meldungen und Reports des DDoS-Protection-Systems zu erläutern.

- die Erläuterung, wie im Störungsfall eine strukturierte Eskalation an den technischen Support des AN durchzuführen ist gemäß Kapitel 5.8.2 Eskalationsprozesse und Ansprechpartner.
- Die Schnittstellen, Abläufe und Ansprechpartner beim Auftragnehmer sind zu nennen, um eine reibungslose Zusammenarbeit sicherzustellen.

6.5. Zeitpunkt der Durchführungen

(225) Die erste Schulung wird in Abstimmung zwischen AN und AG frühestens in Projektphase 5.11.3 Parallelaufbau durchgeführt.

(226) Die Schulungsleistung kann erneut während des Vertragslebens erneut mehrfach abgerufen werden, um beispielsweise neue Mitarbeitende des AG zu schulen oder Wissen aufzufrischen.

(227) Die Frist zwischen Eingang des Abrufs und Durchführungszeitpunkt der Schulung beträgt maximal 2 Monate.

7. Migration und Vertragsende

(228) Zum Vertragsende verpflichtet sich der AN den AG bei einer unterbrechungsfreien Migration zu einer Nachfolgelösung zu unterstützen. Der AN reagiert fristgerecht auf Anfragen und stellt qualifizierte Ansprechpartner bereit.

(229) Der AN verpflichtet sich dabei auch, alle für die Migration notwendigen technischen Informationen bereitzustellen (z.B. Dokumentation, Betriebsparameter etc.)

(230) Er verpflichtet sich weiterhin während des Übergangs zu einer anderen Lösung Konfigurationen in Kooperation mit dem AG durchzuführen (z.B. Unterstützung bei BGP-/Routing-Anpassungen) und einen Parallelbetrieb zu ermöglichen, bis die Migration erfolgreich abgeschlossen ist.

(231) Nach erfolgreicher Migration führt der AN einen geordneten Rückbau seiner bereitgestellten Hard- und Software durch.

Glossar

Abkürzung	Begriff	Beschreibung
AG	Auftraggeber	Die Techniker Krankenkasse, die die Ausschreibung für die Multi-ISP Internet Connect inkl. DDoS-Protection durchführt. Die Techniker Krankenkasse
AMX-IX	Amsterdam Internet Exchange	Einer der größten Internetknotenpunkte weltweit, der sich in Amsterdam befindet.
AN	Auftragnehmer	Der Generalunternehmer, der die Planung, den Aufbau, die Bereitstellung und den Betrieb der Multi-ISP Internet Connect inkl. DDoS-Protection übernimmt.
AS, ASN	Autonomes System	Ein autonomes System ist eine Gruppe von IP-Netzen und Routern, die unter der Kontrolle einer einzigen Organisation stehen und eine einheitliche Routing-Richtlinie haben. Jedes AS wird durch eine eindeutige Nummer, die Autonomes System Number (ASN), identifiziert.
BGP	Border Gateway Protocol, Routingprotokoll	BGP ist ein Routing-Protokoll, das den Austausch von Routing-Informationen zwischen autonomen Systemen ermöglicht und für die effiziente und zuverlässige Weiterleitung von Datenpaketen sorgt. Im Rahmen von Express Route wird BGP für die Konfiguration von Routing-Regeln und die Verwaltung des Datenverkehrs zwischen lokalen Netzwerken und Azure verwendet.
BSI	Bundesamt für Sicherheit in der Informationstechnik	
CPE	Customer Premises Equipment	Geräte, die beim AG installiert werden, um eine Verbindung zum Netzwerk des ISPs herzustellen.
DE-CIX	Deutscher Commercial Internet Exchange	Einer der größten Internetknotenpunkte weltweit, der sich in Frankfurt am Main befindet.
DWDM	Dense Wavelength Division Multiplexing	DWDM ist eine optische Multiplexing-Technologie. Sie ermöglicht die Übertragung mehrerer Datenströme über verschiedene Lichtwellenlängen durch eine einzelne Glasfaser.
EOS	End Of Support	Der Zeitpunkt, an dem ein Hersteller die Unterstützung für ein Produkt oder eine Technologie einstellt.
GA	General Availability	GA steht für General Availability (deutsch: Allgemeine Verfügbarkeit). Im Kontext von

		Azure Express Route bezieht sich GA auf die allgemeine Verfügbarkeit von Express Route-Features oder -Diensten durch den CSP Microsoft Azure, die nach einer erfolgreichen Test- und Vorschau-Phase für alle Kunden (z.B. der AG) verfügbar sind.
HSRP	Hot Standby Router Protocol	Ein Cisco-proprietäres Protokoll, das die Redundanz von Routern in einem Netzwerk sicherstellt und bei Ausfall eines Routers automatisch umschaltet.
IPS	Intrusion Prevention System	Ein IPS ist ein Sicherheitssystem, das Netzwerke und Computersysteme vor Angriffen schützt, indem es den Datenverkehr überwacht und automatische Abwehrmaßnahmen ergreift. Es kann verdächtige Pakete verwerfen, Verkehr von bestimmten Quellen oder zu bestimmten Zielen blockieren und Verbindungen unterbrechen oder zurücksetzen.
Looking Glass	Engl. für Spiegel	Ein Looking Glass ist ein Software-Werkzeug, um Informationen über Übertragungswege (Routen) von Routern im Internet zu erhalten. Ein Looking Glass besteht meistens aus einer Sammlung von Skripten, die auf einem Rechner mit Web-Frontend laufen, über die Befehle (z. B. Ping, Traceroute, BGP-Befehle etc.) mit entsprechenden Parametern an die CPE-Router gesendet werden können. Die Ergebnisse werden ebenfalls in dem Web-Frontend dargestellt und dienen zum Beispiel der Fehlersuche bei Routing-Problemen.
PCAP	Packet Capture	Eine Methode zur Erfassung und Analyse von Netzwerkverkehrsdaten für Diagnose- und Sicherheitszwecke.
PI	Provider Independent	IP-Adressbereich, der nicht an einen bestimmten ISP gebunden ist und frei zwischen verschiedenen ISPs geroutet werden kann.
POP	Point of Presence	Ein Zugangspunkt oder Standort, an dem ISP-Netzwerkausrüstung untergebracht ist und Kunden Zugang zum Internet erhalten.
PP	Private Peering	Direkte, dedizierte Verbindung zwischen zwei AS zum bilateralen IP-Verkehrsaustausch ohne Transit und ohne öffentliche SwitchingInfrastruktur-.
RIPE	Réseaux IP Européens	Die Organisation, welche die Verwaltung und Zuweisung von IP-Adressen und AS-Nummern in Europa koordiniert.
RPKI ROA	Resource Public Key	RPKI: Kryptografisches Framework zur Bindung von IP-Präfixen/AS-Nummern an

	Infrastructure Route Origin Authorization	Inhaber per Zertifikat, schützt BGP vor Hijacking. ROA: Signiertes Objekt, das autorisierte AS für ein IP-Präfix definiert; ermöglicht Route Origin Validation.
RTT	Round Trip Time	Der RTT-Wert ist die Zeit in Millisekunden (ms), die benötigt wird, um Ethernet-Frames von einem Ausgangsstandort zu einem Zielstandort und zurück zu übertragen. RTTs werden als Durchschnittswerte über einen Monat berechnet.
RZ	Rechenzentrum	
SIEM	Security Information and Event Management	Systeme zur Aggregation und Analyse von sicherheitsrelevanten Informationen und Ereignissen aus verschiedenen Quellen.
SLS	Second Level Support	Technischer Support, der bei komplexeren Problemen aktiv wird, die vom First Level Support nicht gelöst werden können.
SNMP	Simple Network Management Protokol	Ein Protokoll zur Verwaltung und Überwachung von Netzwerkgeräten und deren Funktionen.
SSO	Single Sign-On	Eine Authentifizierungsmethode, die es Benutzern ermöglicht, sich mit einer einzigen Anmeldung Zugang zu mehreren Systemen oder Anwendungen zu verschaffen.
TK	Techniker Krankenkasse	
TOTP	Time-based One-Time Password	Ein zeitabhängiger Einmalpasswort-Algorithmus, der für die Zwei-Faktor-Authentifizierung verwendet wird.
TTS	Trouble Ticketing System	Software zur Erfassung, Verwaltung, Priorisierung und Nachverfolgung von Störungen und Serviceanfragen über den gesamten Lebenszyklus, inklusive Dokumentation und Reporting.
VRRP	Virtual Router Redundancy Protocol	Ein offenes Standardprotokoll, das die Redundanz von Routern in einem Netzwerk sicherstellt und bei Ausfall eines Routers automatisch umschaltet.