Whitepaper Voice-Cloud Deutsche Telekom

November 2022

ERLEBEN, WAS VERBINDET.

Impressum

Herausgeber

Deutsche Telekom AG

Version	Stand	Status
1.0	10.12.2021	Final
1.1	22.11.2022	Final

ERLEBEN, WAS VERBINDET.

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

In diesem Dokument wird der IP-Telefoniedienst (Festnetz) der Deutschen Telekom hinsichtlich seiner Einordnung im Kontext „Cloud“ beschrieben. Es wird dargelegt, inwieweit dieser Dienst hinsichtlich Architektur und betrieblichen Aspekten den Kriterien entspricht, die mit dem Begriff „Cloud“ verbunden werden.

Der Begriff „Cloud“ wird oft unspezifisch verwendet; es gibt jedoch vielfältige Ausprägungen der Anwendung von „Cloud“-Architektur und -Technologien bei der Realisierung und dem Betrieb von IP-Diensten, die auf den Strukturen des Internets aufbauen.

Insbesondere muss zwischen „Public Cloud“ und „Private Cloud“ unterschieden werden:

Eine „Public Cloud“ ist vor allem gekennzeichnet durch Multimandantenfähigkeit. Dies bedeutet insbesondere die gemeinsame Nutzung derselben physischen Infrastruktur/Server durch verschiedene Kunden/Unternehmen („Mandanten“ oder „Tenants“) sowie die Möglichkeit der Administration einzelner Cloud-Funktionen durch diese verschiedenen Mandanten. Dieser Ansatz erfordert entsprechende Mechanismen zur Beschränkung des Zugriffs auf Ressourcen und Daten für die jeweiligen Mandanten.

Oft wird der Begriff „Cloud“ automatisch mit einer solchen „Public Cloud“ gleichgesetzt. Aus dieser Einordnung resultieren bei der Bewertung von IP-Diensten oft pauschale Sicherheitsbedenken.

Die IP-Telefonie der Deutschen Telekom ist jedoch in Form einer „Private Cloud“ realisiert, die sich grundlegend von einer „Public Cloud“ dadurch unterscheidet, dass die Cloud-Infrastruktur ausschließlich für einen Kunden (hier die Deutsche Telekom) genutzt wird und nur für diesen Kunden zugänglich ist. Host, Administrator und Nutzer dieser „Private Cloud“ sind identisch.

Details zu den unterschiedlichen Ausprägungen einer „Cloud“ finden Sie im vorliegenden Dokument.

2 Übersicht über die aktuellen Sprachplattformen

Die Produktion von Sprachdiensten innerhalb der Deutschen Telekom Technik erfolgt über mehrere unterschiedliche Plattformen. Die Gemeinsamkeit dieser Plattformen ist aktuell, dass diese auf dedizierten physikalischen Knoten produziert werden. Die Anwendungen können in denselben Betriebsstellen, aber auch in unterschiedlichen Betriebsstellen laufen. Zukünftig wird moderne Cloud-Technik in den Betriebsstellen bzw. den Data Centern der Deutschen Telekom Technik zum Einsatz kommen und dedizierte physikalische Knoten ersetzen, sodass die Anwendungen virtualisiert auf unterschiedlichen Servern verteilt laufen können.
Diese Verfahren kommen heute schon in der IT zum Einsatz und haben sich dort bereits bewährt. Neu ist, dass diese Verfahren jetzt auch für Telekommunikationsanwendungen zum Einsatz kommen. Die Transformation in die Cloud ist vergleichbar mit der bereits durchgeführten Transformation auf IP-Technologie und dem (baldigen) Verschwinden des ISDN/PSTN[1] Netzes. Abbildung 1 zeigt eine grobe Übersicht der einzelnen Sprachplattformen.

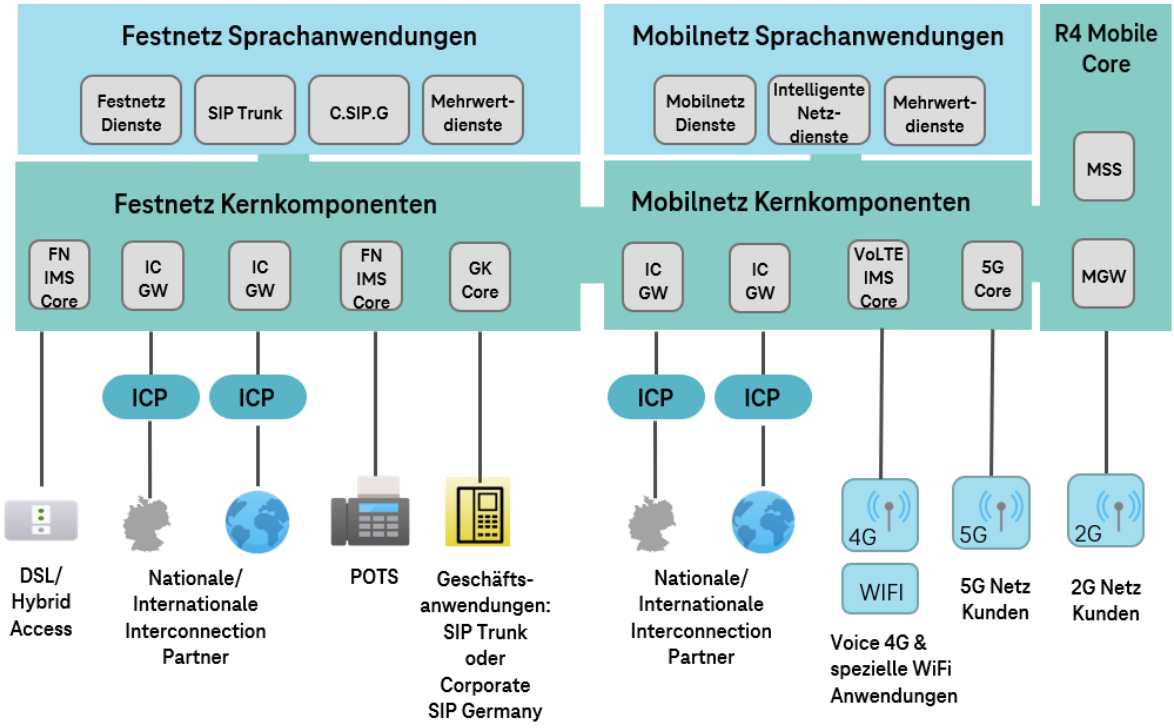

Abbildung 1 Übersicht der Sprachplattformen der Deutschen Telekom Technik ohne ISDN/PSTN

Hauptkomponenten sind jeweils ein IMS (IP-Multimedia Subsystem)-Netz für Festnetz und ein IMS-Netz für Mobilfunk sowie die zugehörigen Applikationsserver (AS). Letzteres wirkt für Mobilnetze ab der vierten Generation (4G). Für 2G (Mobilnetz der zweiten Generation bzw. GSM) steht weiter ein R4 (Release 4 Netz nach 3 GPP Standard)-Netz bereit. Spezielle Geschäftskundenprodukte werden über spezielle Plattformen bereitgestellt. Über ICP (Interconnetion Partner) wird die Kommunikation zu anderen Telekommunikationsgesellschaften weltweit sichergestellt. Bei den grauen Kästen handelt es sich um Komponenten zur Erbringung des Sprachdienstes, die – wie oben beschrieben – heute auf dedizierter Hardware implementiert sind.

[1] Klassische Vermittlungstechnik: Integrated Services Digital Network/ Public Switched Telephone Network

3 Definition einer Cloud

Hinter dem Begriff „Cloud“ verbirgt sich nach allgemeinem Verständnis eine Ansammlung von Servern, auf die über ein Netzwerk wie beispielsweise das Internet zugegriffen werden kann. Auf diesen Servern läuft unterschiedliche Software auf Standardhardware (x86 Prozessoren). Zudem findet mit Nutzung von Cloud-Technologie eine Trennung von Software- und Hardware-Lebenszyklus statt. Die Software läuft auf virtuellen Maschinen (VNF) oder in Containern (CNF) verteilt über viele Server. Die Cloud zeichnet sich durch einen hohen Automatisierungsgrad aus und erlaubt die automatische Skalierung von Software (Größenveränderung) für den Fall, dass zusätzliche Kapazitäten benötigt oder frei werden. Ebenso wird durch eine Continuous Integration & Continuous Delivery bzw. Continuous Deployment (CI/CD) sichergestellt, dass die Softwarezyklen und Softwareupdates – auch inkrementelle – schneller ausgerollt werden können.

Weiterhin wird mit dem Begriff „Cloud“ in der allgemeinen Begriffswelt assoziiert, dass ein Cloud-Anbieter unterschiedlichen Kunden Rechenkapazität anbietet, die ihre Software in den Rechenzentren dieses Anbieters laufen lassen. Das erfordert die Einhaltung von Datenschutz- und Sicherheitsrichtlinien. Zudem ist die Gerichtsbarkeit nicht immer eindeutig geklärt – für den Fall, dass die Rechenzentren außerhalb Deutschlands oder der Europäischen Union (EU) liegen.

Bei einer verfeinerten Definition von „Cloud“ gilt es, unterschiedliche Typen von „Cloud“ zu unterscheiden. Eine Verwendung von Cloud-Technologie bedeutet nicht automatisch, dass es sich um eine öffentliche Cloud handelt, auf die unterschiedliche Teilnehmer Zugriff haben. Es gibt auch die Möglichkeit, eine Cloud privat zu betreiben, das heißt, ein Netzbetreiber baut eine eigene Cloud auf, in der nur seine eigene oder durch ihn installierte Software läuft und für die sonst kein anderer Zugriffsrechte hat. Diese sogenannte „private Cloud“ erfüllt insbesondere die deutsche bzw. europäische Datenschutzrichtline für Datenschutz und deutsche Gerichtsbarkeit. Im Fall der Deutschen Telekom kommt noch die Einhaltung des Telekommunikationsgesetzes (TKG) hinzu.
Bei den von der Deutschen Telekom AG (DTAG) eingesetzten Instanzen für Sprachdienste (Voice) kommen entweder rein private Clouds oder dedizierte Hard- und Software-Komponenten zum Einsatz. Diese werden ausschließlich in Rechenzentren der Deutschen Telekom betrieben. Die Verwendung des Begriffs „Cloud“ für Sprachprodukte bei der Deutschen Telekom gibt nur den Hinweis darauf, dass die Deutsche Telekom auch Cloud-Technik einsetzt, um die oben geschilderten Vorteile der Produktion in einer Cloud nutzen zu können.

Die Einführung von Cloud-Technologie bei Netzbetreibern wie der Deutschen Telekom beschreibt also den Weg in die Softwareisierung und ist ein Schritt in Richtung der Digitalisierung der Telekomunikationsindustrie. Für die Deutsche Telekom ist die Nutzung von Cloud-Technologie ein fester Bestandteil auf ihrem Weg zu einer „Software gesteuerten“ Firma. Die Nutzung von Cloud-Technologie oder die Verwendung von Produktbegriffen wie „cloud PBX“ bedeutet dabei nicht, dass die Software, welche die Telekom verwendet, in einer öffentlichen Cloud frei zugänglich läuft, sondern, dass spezielle Software-Technologien zum Einsatz kommen bzw. dass die Telekom eine Dienstleistung für einen Kunden bereitstellt.

Eine allgemeine Definition einer öffentlichen oder privaten Cloud findet sich zum Beispiel unter [1] und lautet:

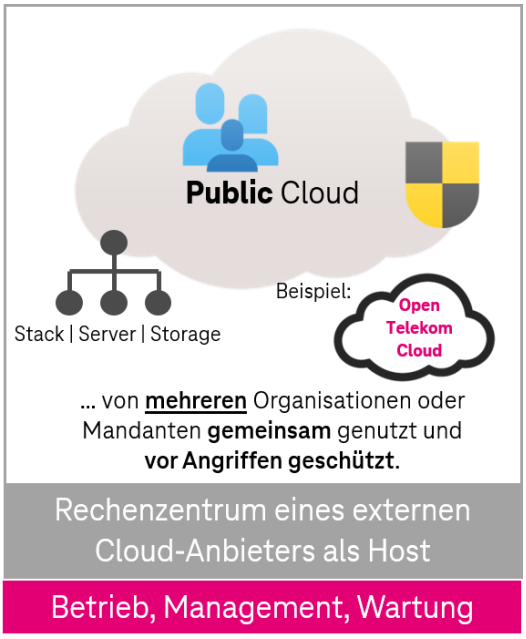

Abbildung 2: Öffentliche Cloud oder auch Public Cloud [1]

Öffentliche Cloud [1]: Eine öffentliche Cloud – auch als „Public Cloud“ bezeichnet – ist ein Dienst, der von einem externen Anbieter ausgeführt wird und zu dem Server in einem oder mehreren Rechenzentren gehören können. Öffentliche Clouds werden von mehreren Organisationen oder Mandanten gemeinsam genutzt. Mithilfe von virtuellen Maschinen können einzelne Server von verschiedenen Unternehmen gemeinsam genutzt werden. Dies wird als „Mehrmandantenfähigkeit“ bezeichnet, weil mehrere Mandanten Serverkapazität desselben physischen Servers mieten. Diese Mandanten haben die Möglichkeit, gewisse Funktionen in der Cloud selbst zu steuern. Die Public Cloud wird von einem externen Cloud-Anbieter als Host (Recheninfrastruktur mit permanenter Zugriffsmöglichkeit) zur Verfügung gestellt und ist offen für mehrere Mandanten oder Mieter, die auch – aus dem Englischen übersetzt – als „Tenants“ bezeichnet werden.

Lokale private Cloud [1]: Eine private Cloud – auch als „Private Cloud“ bezeichnet – ist ein Rechenzentrum, das vollständig einem einzigen Unternehmen gewidmet ist, so dass die Funktionen innerhalb dieser Cloud nur von diesem Unternehmen gesteuert werden können. Die Server in einer privaten Cloud werden nicht von Software, Dateien oder Daten anderer Nutzer oder Mandanten geteilt. Lokale private Clouds werden von den Unternehmen, die sie betreiben, selbst verwaltet und gesichert – nicht von einem externen Anbieter. Für den Fall, dass unterschiedliche Software in der privaten Cloud läuft, besitzt ausschließlich der Betreiber der Cloud die Möglichkeit zur Verwaltung der Ressourcen. Die Infrastruktur gehört ausschließlich dem Betreiber dieser privaten Cloud. Die Sicherheitskontrolle obliegt ausschließlich dem Besitzer der privaten Cloud sowie die Kontrolle, welche Software auf der Serverinfrastruktur installiert ist.

Abbildung 3: Private Cloud [1]

Sprachprodukte der Deutschen Telekom AG bzw. der Deutschen Telekom Technik GmbH werden ausschließlich in privaten Clouds produziert. Die Deutsche Telekom und ihre Mitarbeiterinnen und Mitarbeiter unterliegen der nationalen Gerichtsbarkeit und folgen den nationalen Sicherheits- und Datenschutzrichtlinien.

Unabhängig davon bietet die Deutsche Telekom auch öffentliche Clouds wie die Open Telekom Cloud (OTC) an. In diesen laufen aber keine Telekommunikationsdienste der Deutschen Telekom. Private und öffentliche Cloud-Rechenzentren der Deutschen Telekom sind auch betrieblich strikt voneinander getrennt.

4 Funktionsweise der privaten Cloud für Sprachprodukte der Telekom

Die Deutsche Telekom verwendet für eigene Sprachprodukte in Deutschland entweder dedizierte Plattformen oder eine eigene private Cloud. Dieses Kapitel beschreibt weitere Details zur Funktionsweise, insbesondere dazu, wie das standardisierte IMS (IP-Multimedia Subsystem), das die Deutsche Telekom für ihre Sprachprodukte verwendet, in einer privaten Cloud implementiert und betrieben wird.

Bei der Deutschen Telekom kommen Hardware- und Software-Systeme unterschiedlicher Lieferanten zum Einsatz, die in geschlossenen Rechenzentren laufen, die der Deutschen Telekom gehören. Sicherheitsbestimmungen und Datenschutz für die Systeme und Funktionen folgen den gesetzlichen Regeln. Unabhängige Sachverständige der Telekom und Fachexpertinnen und -experten für diese Fragestellungen stellen sicher, dass die Technik der Telekom die gesetzlichen und regulatorischen Anforderungen erfüllt. Audits unabhängiger Expertinnen und Experten stellen die Sicherheit und Robustheit der Plattform sicher oder zertifizieren sie. Zudem besitzt das IP-Multimedia Subsystem (IMS), welches die Deutsche Telekom für ihre Sprachprodukte als wesentliche Komponente benutzt, eine TÜV-Zertifizierung.

Die nachfolgende Abbildung 4 zeigt den Technologiewandel innerhalb der Technik, welche die Digitalisierung auch für Netz- und Systemkomponenten ermöglicht, die bei der Sprachproduktion zum Einsatz kommen.

In einem ersten Schritt wird das Festnetz der Deutschen Telekom virtualisiert; die Produktion erfolgt zukünftig entsprechend der innovativen technologischen Möglichkeiten. Virtualisierung wird bereits heute schon auch auf dedizierten Komponenten eingesetzt. Eine vollständige Trennung von Hardware und Software inklusive hohem Automatisierungsgrad und flexibler Nutzung der Server, Rechenleistung und Speicher erfolgt jedoch mit dem Schritt der Transformation in eine echte Cloud-Umgebung.

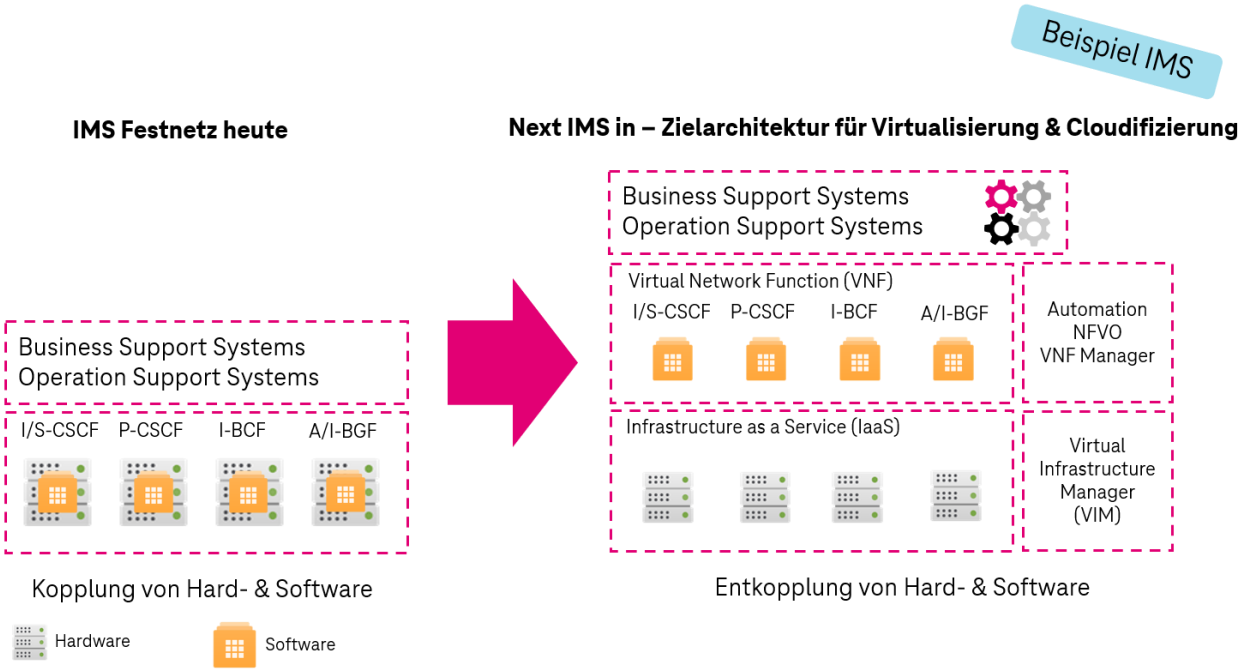

Abbildung 4: IMS Transformation

Ziel der Transformation in die Cloud ist ein hoher Grad an Prozessautomatisierung und Automatisierung mit geschlossenem Regelkreis. Die kontinuierliche Integration und Bereitstellung leitet sich aus dem Englischen „Continuous Integration / Continuous Delivery /Deployment (CI/CD)“ ab und wird auch als „DevOps-Schleife“ bezeichnet, siehe Abbildung 5.

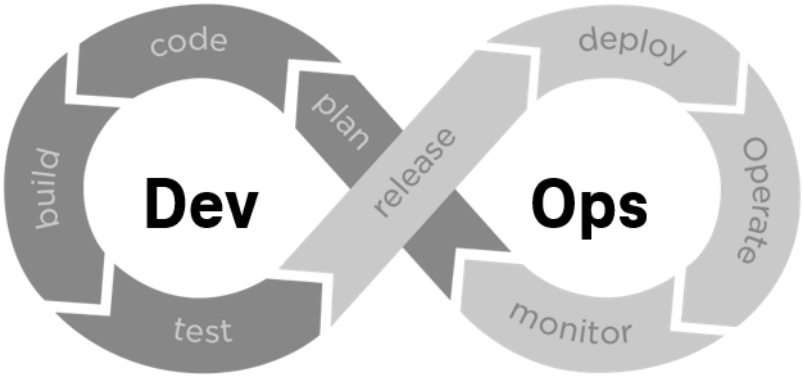

Abbildung 5: DevOps-Schleife

Durch die Transformation in die Cloud wird das Rechenzentrum zu einem großen „Computer“, auf dem unterschiedliche Arten von Software aufgespielt und betrieben werden können.
Das funktioniert dann auch für Software, mit der Telekom-Sprachprodukte realisiert sind.

5 Sicherheitsaspekte

Die Cloud folgt notwendigen Sicherheitsrichtlinien und ist heute in drei Sicherheitszonen aufgeteilt. Damit wird erreicht, dass ein Zugriff von außerhalb auf interne, für die Service-Erbringung relevante Komponenten unterbunden wird. Die Zonen sind über Security Groups und Zugriffsrechtemanagement gegeneinander abgesichert. Eine Security Group, auch Netzwerksicherheitsgruppe oder Cloud-basierte Zugriffsgruppe genannt, ist somit eine Zusammenfassung von Netzwerkknoten, für die eine gemeinsame Sicherheitsrichtlinie (Policy) gilt. Zudem ist sichergestellt, dass die Software-Komponenten unterschiedlicher Hersteller gegeneinander isoliert laufen. Gleiches gilt für die Nutzung der Cloud-Ressourcen an sich. Nachfolgend sind die Eigenschaften der Sicherheitszonen beschrieben. Dieses Konzept wurde bei der privaten Cloud der Telekom von den klassischen Rechenzentren für dedizierte Komponenten übernommen.

5.1 Sicherheit der Cloud-Infrastruktur

In Hinblick auf die Sicherheit sind Netzressourcen und Rechenleistung gegeneinander logisch segmentiert. In der Vergangenheit war die Separierung bei anderen Services auch physikalisch im Rechenzentrum umgesetzt, was allerdings dem Prinzip einer heutigen Cloud widerspricht. Aus dem Grund wurde von den Cloud Security Experten ein Konzept entwickelt, um das Sicherheitsniveau einer physikalischen Trennung beizubehalten. Da eine Telefonieplattform kritische Daten beinhaltet, wurde die Separierung beibehalten und um weitere Sicherheitsmaßnahmen ergänzt. Als Beispiel kann hierfür ein sehr regelmäßiges Patchmanagement in kurzer Abständen oder auch ein cloudspezifisches Logging und Monitoring der Security Events genannt werden. Mithilfe dieser und vieler weiteren Maßnahmen ist das Sicherheitsniveau in der Cloud vergleichbar zum Niveau bei Services, die nicht in einer Cloud gehostet sind. Infolgedessen ist auch die Cloud Infrastruktur vor typischen Hyper Visor Breaches oder auch Ressourcenüberlastung geschützt.

Abbildung 6 verdeutlicht das anhand einer Data Center-Anschaltung.

Die External Zone (EXT) ist die Grenze zwischen dem Rechenzentrum außerhalb und den internen Komponenten, die sich in der sogenannten „Internal Zone“ (INT) befinden. In dieser Zone befinden sich Komponenten, auf die der Kundenverkehr auftrifft, beispielsweise Proxy-Funktionen. Diese Proxy-Funktion weist eine erhöhte Robustheit bezüglich Sicherheit auf.

Die INT ist eine Zone mit hohen Sicherheitsanforderungen. Diese Zone enthält Systeme, die dauerhaft kritische Daten speichern müssen und Systeme, die vollständig von der Außenwelt getrennt sein müssen. Beispiele für Systeme in der INT-Zone sind Applikationsserver, Kundendatenbanken und Teile der Anrufsteuerung.

Die Management-Zone (MGMT) enthält Systeme zur Verwaltung von virtuellen Netzwerkfunktionen, die in der privaten Cloud „gehostet“ werden. Zu den Verwaltungssystemen, die sich in der Management-Zone befinden, gehören u.a. interne Jump-Server, Überwachungssysteme und Elementverwaltungssysteme. Die in der Management-Zone (MGMT) „gehosteten“ Managementsysteme werden von Telekommitarbeiterinnen und -mitarbeitern gesteuert bzw. betrieben. Cloud-Infrastruktur-Verwaltungssysteme sind nicht Teil der Verwaltungszone der Management-Zone. Sie befinden sich in einem physikalisch getrennten Management-Netzwerk.

Zentrale Managementfunktionen werden in einem separaten Management-Rechenzentrum betrieben. Sie sind über ein separates Netzwerk an die Produktionsrechenzentren angeschlossen. Grundsätzlich ist die Kommunikation zwischen den Rechenzentren verschlüsselt.

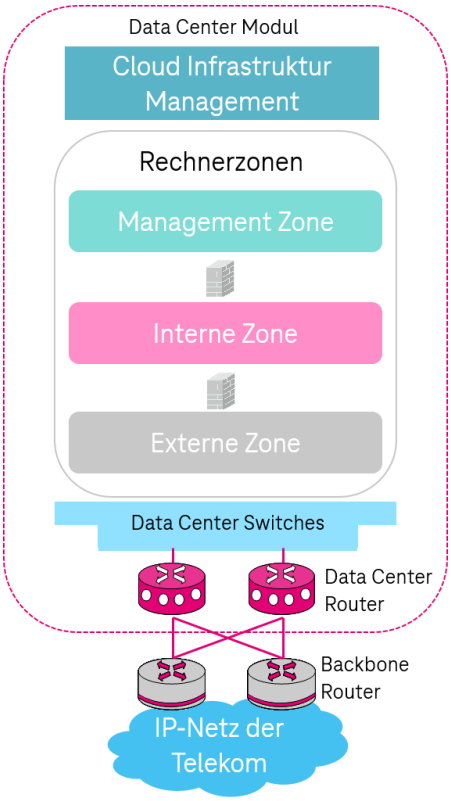

Abbildung 6: Sicherheitszonen in einem Data Center

Sicherheitstechnisch sind die Data Center untereinander durch verschlüsselte IPSec Tunnel (VPN) miteinander verbunden, so dass Verkehr zwischen den Data Centern ausschließlich verschlüsselt und von anderem Verkehr getrennt übertragen wird. Abbildung 7 verdeutlicht diesen Sachverhalt. Weiterhin sind die Betriebsstellen bzw. die Data Center gegen Angriffe von außen durch spezielle Sicherheitskomponenten geschützt. Diese schützen vor unerwünschtem Verkehr und verhindern DoS oder DDoS (Distributed Denial of Service) Attacken, siehe Abbildung 8.

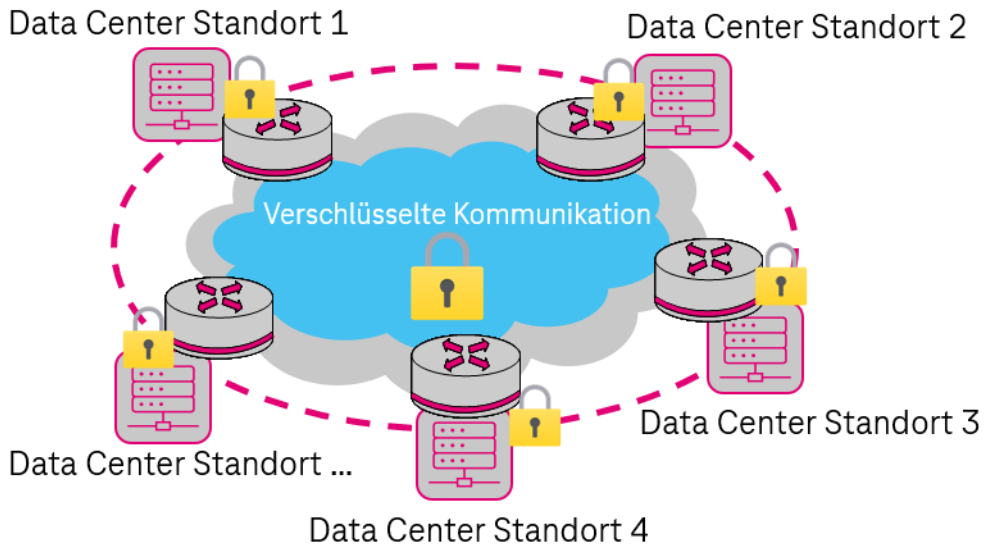

Abbildung 7: Verschlüsselte Verbindungen zwischen den Data Centern

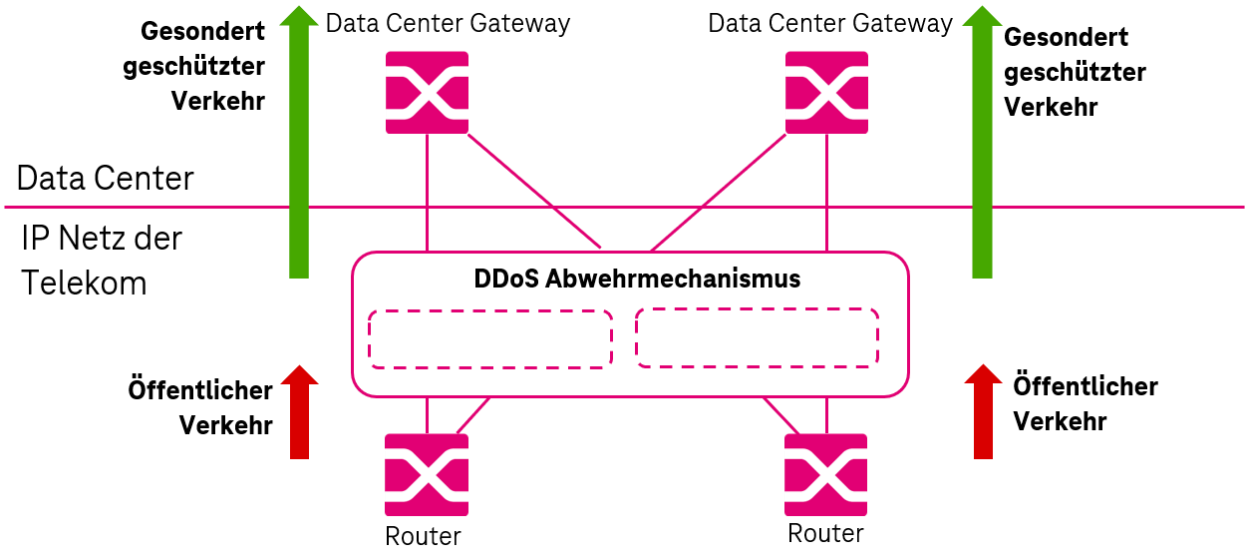

Abbildung 8: Schutz des Data Centers vor DoS- und DDoS-Attacken

6 Netzanschaltung

Ein weiterer wichtiger Aspekt bei der Betrachtung der Cloud ist die Netzanschaltung. Insbesondere ist hierbei wichtig zu betrachten, ob die private Cloud über das Internet erreichbar ist und wie sie vor externem Zugriff geschützt wird. Bei der Deutschen Telekom wird nach Telekom-Zugang (Telekom Access - TA) und Fremdzugang (Foreign Access - FA) unterschieden. Damit ist der Zugang zu den im Rechenzentrum laufenden Komponenten gemeint, aus dem der Kunde seine Sprachverbindung heraus aufbaut, so dass diese vermittelt werden kann. Kunden aus dem Ausland können die Sprachplattform der Deutschen Telekom nur über einen speziellen Zugangspunkt (FA) erreichen. Das gilt beispielsweise, wenn sie sich im Ausland in einem Hotel befinden.

Über Peering bzw. aus dem Internet ist ausschließlich der Fremd-Access (FA) routingtechnisch (Streckenführung) erreichbar. Im Fremd-Access werden weitere Sicherheitsmechanismen, sogenannte Verschlüsselungs- oder Tunnelverfahren angewandt, die das IMS der Telekom schützen. Die Externe-, Interne- und die Management-Zone sind jeweils über Firewalls geschützt. Die Interne- und die Management-Zone können nicht direkt aus dem Internet angesprochen werden. In der aktuellen Cloud-Architektur sind die Hardware- und Ressourcen-Pools der jeweiligen Zone gegeneinander isoliert. Die Telekom-Access (TA)-Komponenten, wie P-CSCF oder I-BCF, sind robust für den Betrieb als Eingangstor ausgelegt und haben weitere Schutzmechanismen, die sie vor Angriffen schützen.

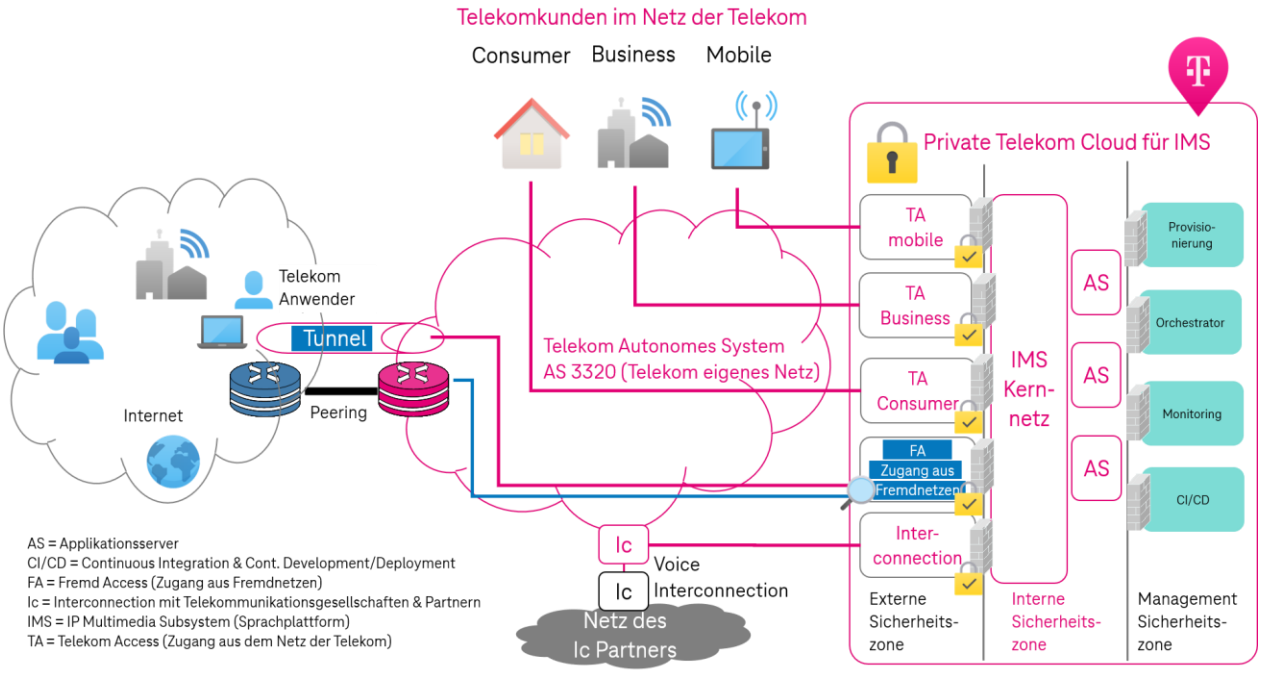

Abbildung 9: Aufbau einer privaten Telekom Telko Cloud und deren Netzanschaltung

Die Deutsche Telekom nutzt die Funktion der Virtualisierung, bei der die Software verteilt in der Cloud bezogen auf die jeweilige Sicherheitszone läuft. Das hat den Vorteil, dass für den Fall eines Serverausfalls die Funktion auf einem anderen Server hochgefahren und der Kunde nahtlos auf diesen migriert werden kann. Das erhöht die Robustheit des Dienstes vor Kunde. In der klassischen Welt hingegen ist die Funktion an die Hardware gebunden und kann nur auf einen gleichartigen Hardwaretyp migriert werden. Die oben genannten Vorteile der Automatisierung unterstützen diese Redundanzszenarien ebenfalls.

Für den Fall, dass ein Telekom Kunde sein Produkt nomadisch nutzt oder einen Netzanschluss über einen Fremdanbieter besitzt, stellt Abbildung 10 dar, wie die Verbindung zur Telekommunikations-Cloud – auch als Telko-Cloud bezeichnet – der Deutschen Telekom erfolgt.

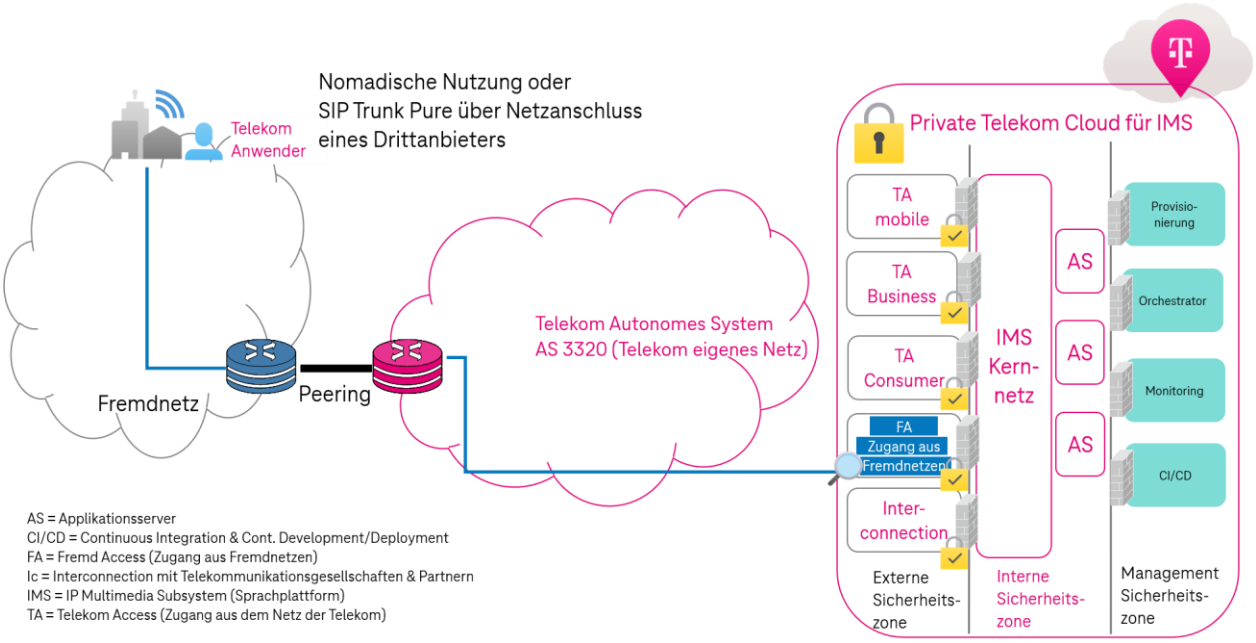

Abbildung 10: Nomadische Nutzung oder Zugang über das Netz eines Drittanbieters

Solange nicht alle Dienste der Deutschen Telekom in die private Telekom Cloud migriert sind und Dienste sowohl klassisch als auch virtuell produziert werden, sind die Betriebsstellen über verschlüsselte VPNs miteinander verbunden.

Mehrere Produkte der Deutschen Telekom ermöglichen einen Zugang aus einem Fremdnetz. Allen ist gemein, dass sie speziell autorisiert sind und die Kommunikation verschlüsselt mittels TLS erfolgt. Durch die Absicherung über verschlüsselte Kommunikation ist sichergestellt, dass die Verbindung nicht abgehört und gegen andere Kommunikationsverbindungen getrennt erfolgt. In Abbildung 10 handelt es sich bei der Verbindung aus dem Fremdnetz um eine verschlüsselte TLS-Kommunikation.

Zugang über Fremdnetze kann zum Zeitpunkt der Erstellung dieses Dokuments mit folgenden Produkten (inkl. Tarifvarianten) genutzt werden:

- DeutschlandLAN SIP-Trunk
- CompanyFlex
- Corporate SIP-Trunk
- Corporate CompanyFlex
- Corporate SIP Germany
- Corporate SIP International

7 Zusammenfassung

Die Deutsche Telekom wird im Rahmen der Digitalisierung und Automatisierung ihrer Netze Cloud-Techniken einsetzen. Software für Sprachanwendungen der Deutschen Telekom werden ausschließlich in Rechenzentren der Deutschen Telekom betrieben, die der nationalen Gerichtsbarkeit unterliegen. Die bewährten Sicherheitsstandards klassischer Rechenzentren werden erweitert. Ausschließlich der Deutschen Telekom obliegt die Möglichkeit, die Rechenzentren zu steuern. Die Deutsche Telekom ist davon überzeugt, dass die Tranformation in die Cloud – ähnlich wie die Transformation auf IP (Internet Protokoll)-Technik – zum Wohl ihrer Kunden ist und den Technologieinnovationsgrad verbessert.

Quellenverzeichnis

[1] https://www.cloudflare.com/
[2] https://www.wirtschaftswissen.de/
[3] https://cloudacademy.com

ERLEBEN, WAS VERBINDET.