ComConsult GmbH
Beratung + Planung + Schulung

Der Netzwerk Insider

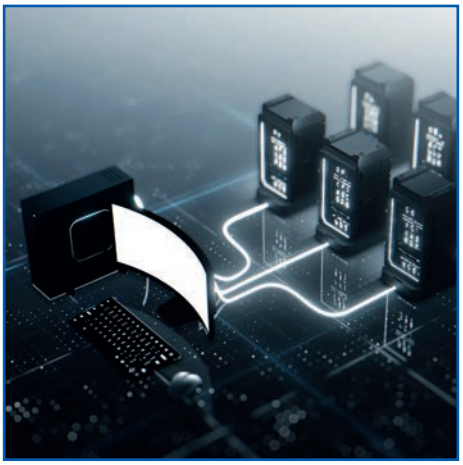
November 2021

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Virtual Desktop Infrastructure – Möglichkeiten, Technologie, Sicherheit

von Dr. Markus Ermes

Der moderne Büroarbeitsplatz kommt heute nicht mehr ohne einen Arbeitsplatz-PC aus. Doch der Rechner des Mitarbeiters, egal ob Desktop-PC oder Notebook, bringt einen erheblichen Aufwand mit sich. Das gilt auch für die Sicherheit dieser Systeme. Daher wünscht sich mancher Administrator die Möglichkeit, die Clients nicht nur zentral zu verwalten, sondern auch zentral bereitzustellen und möglichst einfache Endgeräte bei den Mitarbeitern zu platzieren. Hier bietet sich eine „Virtual Desktop Infrastructure“ (VDI) an.



VDI erlaubt genau diese zentralisierte Bereitstellung von (virtuellen) Clients für die Mitarbeiter. Hersteller preisen ihre jeweilige Lösung als besonders sicher, einfach und kostengünstig an. Was wirklich dahinter steckt, wird in diesem Artikel genauer beleuchtet.

Gerade die verschiedenen (alten und neuen) Client-Varianten, die für eine VDI erforderlich sind, können etwas verwirrend sein.

weiter auf Seite 7

5G-Mobilfunk im Gebäude

von Dr. Joachim Wetzlar

ab Seite 20

Geleit

Die wichtigsten Netztrends 2022

ab Seite 2

Standpunkt

Exchange Emergency Mitigation Service – Microsofts Fernsteuerung für Exchange

ab Seite 30

Kostenloses Webinar der Woche

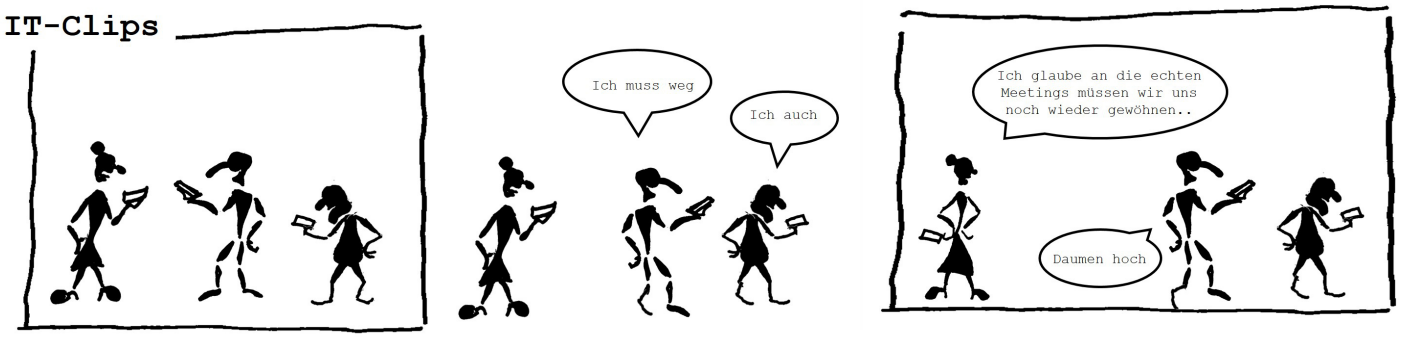
Zertifizierungen in der Informationssicherheit – Wo fange ich an?

auf Seite 18

Aktuelle Sonderveranstaltung

Sonderveranstaltung Netze Beginn der Frühbucherphase

ab Seite 26



Geleit

Die wichtigsten Netztrends 2022

Nachdem ich im Oktober 2021 mit Blick auf die ComConsult-Leistungen für unsere Kunden die Top-Themen der IT-Basisprojekte zusammengefasst habe, möchte ich im Folgenden wieder anhand aktueller Projekte von den wichtigsten aktuellen Netztrends berichten. Wir haben die Erfahrung gemacht, dass die Aufträge, die uns jährlich in dreistelliger Anzahl von unseren Kunden erteilt werden, für den Markt durchaus repräsentativ sind. In der Regel dauert es eine Weile, bis ein brandneuer, starker Trend den Weg von der Produkt- oder Service-Idee bis zum Rollout hinter sich hat. Wenn dieser einen signifikanten Teil unserer Kunden erfasst hat, kann man davon ausgehen, dass es sich auch um einen Trend handelt. Texte wie folgender werden unter anderem deshalb gelesen, weil man wissen will, womit sich andere IT-Organisationen befassen. Der Blick über den Tellerrand hinaus dient dazu, sich gedanklich darauf vorzubereiten, was einen in absehbarer Zeit wahrscheinlich erwartet.

In diesem Sinne also die Frage: Was sind die wichtigsten Netztrends 2022?

WAN – Internet – Cloud-Zugang

Einer der Trends mit einem sehr langen „Hype Cycle“ heißt Cloud. Die ersten Prognosen, dass, wenn nicht alles, aber doch fast alles von den unternehmensinternen Rechenzentren (RZ) in externe Clouds verlagert werde, liegen mehrere Jahre zurück. Solche Prognosen haben sich für mittelgroße bis große Organisationen als übertrieben erwiesen. Die privaten RZ haben sich bei unseren Kunden behauptet. Dabei ist jedoch zu berücksichtigen, dass die ComConsult-Kunden meistens mittlere bis große Unternehmen sind. Daneben zählen wir öffentliche bzw. nicht privatwirtschaftlich geführte Organisationen jeglicher Größe, von der Kommune über das Bundesland bis zu großen Unikliniken, zu unseren Kunden. In allen diesen Fällen gibt es für viele Applikationen gute Gründe, sie weiterhin in eigenen RZ zu betreiben.

Die Propheten der RZ-Ablösung durch Clouds sagten also Unzutreffendes, jedoch nicht nur. Fakt ist, dass für viele Unternehmen, vor allem für kleine Firmen, externe Clouds alles bieten, was an zentraler IT benötigt wird. Für die IT in solchen Firmen geht es somit hauptsächlich darum, welche Endgeräte man nutzt, wie man sie vernetzt, auf welchem Weg diese mit Clouds verbunden sind und – vor allem – wie die IT-Sicherheit im Cloud-Zeitalter aussieht.

Die Erfahrungen seit ca. 50 Jahren zeigen: Viele IT-Trends zeichnen sich zunächst im Consumer-Bereich ab, dann erfassen sie kleine Firmen und „wachsen“ in große Organisationen hinein. So war das mit kleinen Computern und vielen anderen IT-Erfindungen der letzten fünf Jahrzehnte. So ist es auch mit Cloud Computing. Unternehmen wurden in dem Maße „Cloud-ready“, wie die Clouds „Business-ready“ wurden. Letzteres geschah tatsächlich. Beispiel: Nachdem US-Hyperscaler wie Amazon, Google und Microsoft erkannt haben, dass sie bei vielen potenziellen Kunden in der EU gar nicht anzuklopfen brauchen, solange sie Europa von den USA aus bedienen, schossen Cloud-Rechenzentren im EU-Gebiet wie die Pilze aus dem Boden. Wenn es keinen Markt dafür gäbe, würden die Hyperscaler nicht Milliarden in diese Einrichtungen investieren.

Der Cloud-Markt entwickelt also weiter seine Dynamik. Es gibt immer mehr Cloud-Nutzer, auch bei unseren Kunden. Und hier kommen wir zu einem wichtigen Netztrend: Aus dem klassischen Wide Area Network (WAN), das die Firmenstandorte miteinander verbindet, wird ein komplexeres Gebilde. Zum einen müssen die Standorte einer Organisation miteinander und in vielen Fällen mit dem eigenen RZ verbunden sein. Zum anderen muss das „externe“ Netz den Cloud-Zugriff ermöglichen. Der Internet-Zugang als Hauptzubringer vieler Cloud-Dienste wird immer wichtiger. WAN- und Internet-Service-Provider sind meistens dieselben Anbieter. So gibt es viele gute Gründe, das klassische WAN, den Internet- und den Cloud-Zugang immer zusammen zu betrachten, zusammen zu planen und in vielen Fällen zusammen auszuschreiben. Die standortübergreifende Kommunikation, wenn man diesen verallgemeinernden Begriff verwenden möchte, bedarf in vielen Organisationen eines Neudesigns. Man kann diesen starken Trend WAN-Internet-Konvergenz nennen.

RZ-Netze

Wie schon erwähnt haben sich viele RZ als Totgesagte herausgestellt, die länger leben. Wenn ein RZ zu betreiben ist, wird auch ein RZ-Netz benötigt. Bekanntlich wird RZ-intern intensiver kommuniziert als über die RZ-Grenzen hinaus (das bekannte Bild von mehr Ost-West- als Nord-Süd-Verkehr). Für immer schnellere Prozessoren und Speicher sind immer schnellere Netze notwendig. 100Gigabit Ethernet hat also durchaus seine Daseinsberechtigung. Gleiches wird für höhere Übertragungsraten gelten.

Doch Speed ist nicht alles. Ein RZ-Netz braucht mehr als nur schelle Leitungen und Switches. Angesichts der anhaltenden Sicherheitsrisiken müssen RZ-Netze in Zonen aufgeteilt werden. Sowohl die Zonenbildung als auch die Regeln für die Kommunikation zwischen den Zonen werden aufgrund wechselnder Anforderungen der Applikationen immer dynamischer. Generell entfernen sich die RZ-Netze von den ehemals statischen Konstrukten zu ständig anzupassenden Strukturen. Daher wünschen sich viele RZ-Betreiber mehr Automatismen im Netzbetrieb, eine Art Fabric mit dynamischer Konfiguration. Dazu haben Standardgremien und Hersteller in den letzten acht Jahren verschiedene Verfahren entwickelt: IEEE Shortest Path Bridging (SPB), IETF Ethernet Virtual Private Network (EVPN), Cisco ACI, VMware NSX sind die wichtigsten. Keines dieser Verfahren dominiert RZ-Netze ganz für sich, und keines davon ist vom Markt verschwunden bzw. ein Kandidat für den Untergang. Diese vier Verfahren sind nicht kompatibel zueinander. Man wählt meistens eine Fabric aus und lässt sie implementieren. Die meisten RZ-Betreiber entscheiden sich vorrangig für einen Hersteller und folgen der Fabric-Empfehlung desselben.

Können wir also von automatischen Fabrics als DEM Trend in RZ-Netzen sprechen? Ja und nein. Ja, weil sich immer mehr Betreiber für eine solche Fabric entscheiden. Nein, weil RZ-Netze auf Fabric-Basis nach unserer Wahrnehmung immer noch die Minderheit sind. In den meisten RZ-Netzen, vor allem in kleinen Netzen, reicht die Kombination von einfachen ro-

Virtual Desktop Infrastructure – Möglichkeiten, Technologie, Sicherheit

Fortsetzung von Seite 1

Dr. Markus Ermes hat im Bereich der optischen Simulationen promoviert und Artikel in verschiedenen Fachzeitschriften veröffentlicht. Teil seiner Promotion waren Planung, Aufbau und Nutzung von verteilten und Höchstleistungs-Rechenclustern (HPC). Bei der ComConsult GmbH berät er Kunden im Bereich Rechenzentren, wobei seine Hauptaufgaben bei Netzwerken, Storage und Cloud-basierten Diensten liegen. Seine Kenntnisse im HPC-Bereich geben zusätzlich Einblicke in modernste Hochleistungstechnologien (CPU, Storage, Netzwerke), die in Zukunft auch im Rechenzentrum Einzug erhalten können.

Der moderne Büroarbeitsplatz kommt heute nicht mehr ohne einen Arbeitsplatz-PC aus. Doch der Rechner des Mitarbeiters, egal ob Desktop-PC oder Notebook, bringt einen erheblichen Aufwand mit sich. Das gilt auch für die Sicherheit dieser Systeme. Daher wünscht sich mancher Administrator die Möglichkeit, die Clients nicht nur zentral zu verwalten, sondern auch zentral bereitzustellen und möglichst einfache Endgeräte bei den Mitarbeitern zu platzieren. Hier bietet sich eine „Virtual Desktop Infrastructure“ (VDI) an.

VDI erlaubt genau diese zentralisierte Bereitstellung von (virtuellen) Clients für die Mitarbeiter. Hersteller preisen ihre jeweilige Lösung als besonders sicher, einfach und kostengünstig an. Was wirklich dahinter steckt, wird in diesem Artikel genauer beleuchtet.

Gerade die verschiedenen (alten und neuen) Client-Varianten, die für eine VDI erforderlich sind, können etwas verwirrend sein. In diesem Artikel werden dafür die folgenden Begriffe genutzt, wie auch in Abbildung 1 dargestellt:

- Der **(physische) Client** bezeichnet den „klassischen“ Arbeitsplatzrechner eines Mitarbeiters.
- Der **virtuelle Client** ist der per Virtualisierungstechnik zentral bereitgestellte Client.
- Als **Endgerät** bzw. der **zugreifende Client** wird der physische PC oder das physische Notebook am Arbeitsplatz des Benutzers bezeichnet. In einer VDI-Umgebung wird von hier aus der virtuelle Client bedient. Der Begriff Endgerät betrifft stärker das physische Gerät, während der zugreifende Client mehr Fokus auf die Software für die Verbindung zum virtuellen Client legt.
- Der **Benutzer** bedient mithilfe des zugreifenden Clients den virtuellen Client.
- Der Begriff **VDI** umfasst die notwendigen Komponenten für die Verwaltung der virtuellen Clients und den Zugriff auf diese.

Ausgehend von einer typischen Umgebung werden die üblichen Argumente für den Einsatz von VDI und danach die technischen Grundlagen für eine solche Lösung dargestellt. Aber unabhängig von der Technik will eine solche Lösung auch vernünftig geplant und betrieben werden. Zusätzlich werden Sicherheitsaspekte beleuchtet und die Kosten betrachtet.

Ausgangslage – Warum möchte ein Administrator VDI einsetzen?

Nur noch wenige Branchen können vollständig auf IT-Systeme verzichten. Jedes Handwerksunternehmen setzt Computer ein und sei es nur zur Rechnungserstellung und Buchhaltung.

Doch ist die Anzahl der genutzten Arbeitsplatzrechner üblicherweise deutlich größer. In international tätigen Unternehmen wird die Zahl schnell fünf- oder gar sechsstellig. Und man kommt auch schon lange nicht mehr mit einem „One-size-fits-all“-Ansatz aus. In einer CAD-Abteilung wird beispielsweise eine ganz andere Leistung von den Clients erwartet als in der Buchhaltung. Software-Entwickler benötigen andere Umgebungen als der Empfang. Dadurch ergeben sich nicht nur viele Endgeräte, sondern auch viele verschiedene Client-Typen. Will man all diese Systeme zuverlässig verwalten und die Nutzer im Fehlerfall unterstützen, braucht man entsprechend ausgestattete Support-Abteilungen. Zwar lässt sich durch eine zentrale Software-Verwaltung der Aufwand reduzieren, aber spätestens wenn der Benutzer „nichts gemacht hat“ und der Client trotzdem nicht funktioniert, ist häufig doch ein Vor-Ort-Besuch notwendig.

Hier wäre eine zentrale Umgebung wünschenswert, in der man die Clients vollständig ausstatten und die Leistung flexibel festlegen kann. Wir kennen das aus dem Server-Bereich: Wenn ein neuer Server für eine vorgegebene Aufgabe benötigt wird, kann die IT diesen in wenigen Mi-

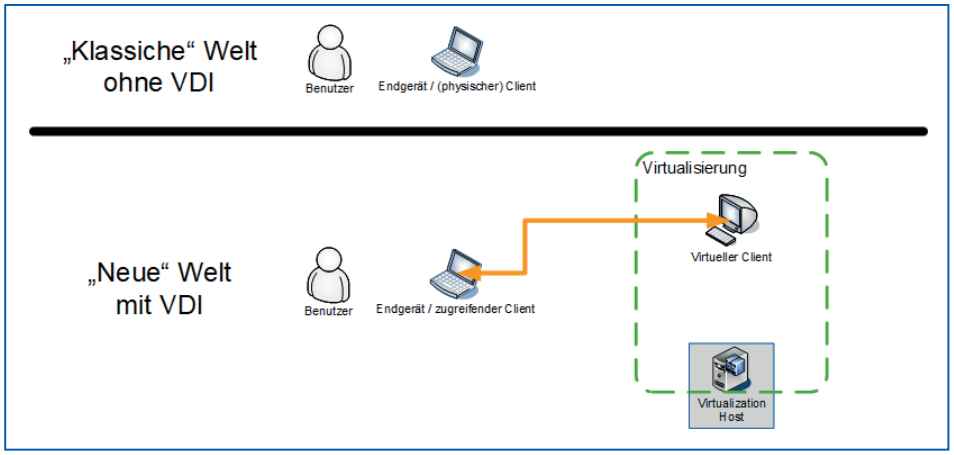


Abbildung 1: Client-Typen ohne (oben) und mit (unten) VDI

nuten bis Stunden zur Verfügung stellen. Und wenn etwas schiefgeht, kann man den Server auch wieder zurücksetzen.

Hier setzt Virtual Desktop Infrastructure an: Man verwendet diese Server-Technologien auch für Clients und gibt dem Benutzer nur noch ein möglichst einfaches Endgerät (engl. Desktop), mit dem er sich mit einem virtuellen Client über ein Firmennetz oder das Internet verbindet. Im optimalen Fall ist dies sogar so transparent und leistungsfähig, dass der User den Unterschied zu einem vollausgestatteten eigenen Endgerät gar nicht bemerkt. Aber ergibt eine solche Lösung wirklich immer Sinn? Natürlich nicht und im folgenden Abschnitt beschäftigen wir uns mit genau dieser Fragestellung.

Wo ergeben virtuelle Clients einen Sinn?

Bevor wir uns mit den technischen Grundlagen von VDI beschäftigen, soll kurz erläutert werden, in welchen Bereichen VDI sinnvoll sein kann und wo nicht. Dabei spielt ein Aspekt eine zentrale Rolle: Ich benötige eine Netzverbindung zur VDI, um auf „mein“ System zugreifen zu können.

Damit fallen einige Einsatzmöglichkeiten sofort weg:

- Bei Mitarbeitern, die viel unterwegs sind, ist VDI häufig nicht das Mittel der Wahl. Abgesehen von der eventuell suboptimalen Netzverbindung am jeweiligen Einsatzort spielt auch die geografische Entfernung der VDI eine Rolle. Je weiter weg, desto schlechter lässt sich ein virtueller Client bedienen.

- Wenn spezielle Hardware verbaut ist, zum Beispiel für die Entwicklung von IoT-Geräten, kann diese in einer VDI ebenfalls nicht einwandfrei reproduziert werden. Zwar kann man USB-Geräte wie USB-Sticks oder Kameras an den virtuellen Client weiterreichen, aber sobald man spezielle Zusatzkarten einsetzt, ist eine Nutzung von VDI ausgeschlossen.

- Wenn der Zugriff über das Internet erfolgen soll, muss auch die Internetleitung, über die zugegriffen werden soll, ausreichend dimensioniert sein. Das gilt sowohl für das Endgerät als auch für die Internetanbindung der VDI.

- Außerdem macht VDI erst ab einer bestimmten Größe der Umgebung wirklich Sinn. Wenn Sie alle Ihre Clients auf einem Server virtualisieren können und dieser immer noch zu viel Leistung hat, ist es gegebenenfalls nicht wirtschaftlich, die Clients zu virtualisieren.

Demgegenüber steht eine ganze Reihe von Szenarien, in denen eine VDI den Betrieb extrem vereinfachen kann:

- Es existieren nur wenige verschiedene Client-Typen? Dann kann eine VDI mit wenigen Vorlagen und Gruppen den Bereitstellungsprozess von dann virtuellen Clients extrem vereinfachen.

- Ein Unternehmen arbeitet mit vielen externen Partnern zusammen, die gelegentlich Zugriff auf interne Ressourcen benötigen? Eine VDI kann schnell virtuelle Clients bereitstellen, die nur auf genau diese Ressourcen zugreifen können, ohne dass Notebooks verschickt oder größere Anpassungen an der Firewall gemacht werden müssen.

- Es gibt Systeme und Netze, in denen besonders schützenswerte Daten verarbeitet werden und auf die Clients typischerweise nicht zugreifen sollen, z. B. eine Management-Umgebung? Eine VDI ermöglicht es, solche Sprungsysteme einfach und einheitlich zu verwalten. Die zugreifenden Clients bekommen dann nur Zugang zur VDI und nicht zu den eigentlichen Systemen.

- Ein Mitarbeiter arbeitet immer wieder in verschiedenen Bereichen mit unterschiedlichen, vielleicht sogar gegenläufigen Anforderungen an die Clients? In einer VDI können einem Benutzer mehrere virtuelle Clients zur Verfügung gestellt werden.

Das klingt alles vielversprechend und es wurde schon die Nähe zur Server-Virtualisierung erwähnt. Aber wie funktioniert die Technik genau?

Technische Grundlagen einer Virtual Desktop Infrastructure

Das Kernstück der Virtual Desktop Infrastructure (VDI) ist eine Virtualisierungsumgebung, in der Clients virtualisiert werden. Dem jeweiligen Benutzer können sowohl komplette virtuelle Clients als auch einzelne Anwendungen bereitgestellt werden. Letzteres überträgt dann nur das oder die Fenster der jeweiligen Anwendung an den zugreifenden Client.

Virtualisierung ist als Technik mittlerweile über 20 Jahre alt und kann als beherrschbar gelten, daher ist dieser Ansatz naheliegend und in den oben genannten Fällen auch sinnvoll.

Es ergeben sich jedoch einige Unterschiede zur klassischen Server-Virtualisierung:

- Ein zentraler Unterschied ist, dass die virtuellen Clients nicht nur einzelne Dienste bereitstellen wie DNS oder einen Webserver, sondern dass – der Name sagt es schon – Client-Anwendungen ausgeführt werden, mit denen ein Benutzer in Echtzeit interagieren kann. Wo ein Server einen, vielleicht zwei Dienste bereitstellt, laufen auf einem virtuellen Client Dutzende von Applikationen, von einem Browser über Office-Programme bis hin zu CAD-Tools und sonstigen Spezialanwendungen. Dabei wird entweder der vollständige Desktop des virtuellen Clients oder nur eine bestimmte Anwendung auf dem zugreifenden Client sichtbar und kann so genutzt werden, als ob man direkt „vor“ dem virtuellen Client sitzt.

- Im Gegensatz zu einem virtuellen Server handelt es sich um einen Client. Dieser muss auch auf Netzebene so behandelt werden − inklusive aller Zugriffsbeschränkungen auf andere Systeme.

- Zwar gibt es je nach Branche auch bei virtuellen Servern immer wieder Lastspitzen, bei virtuellen Clients sind diese aber klarer ersichtlich: Morgens zu Beginn der Arbeitszeit werden alle Nutzer nahezu gleichzeitig versuchen, sich anzumelden und die VDI mit der zugrunde liegenden Infrastruktur aus Virtualisierungsservern und Speichern stark belasten. Ob diese Anmeldeversuche funktionieren und wie angenehm das Erlebnis für die Benutzer ist, hängt von der Dimensionierung der Umgebung ab.

- Und ein letzter Punkt, der trotz der Verbreitung von Virtualisierung eine Rolle spielen kann: Nicht jede Client-Software ist für den Einsatz in einer virtuellen Umgebung geeignet. Dies kann einerseits an besonderer Hardware liegen. Andererseits gibt es durchaus Softwarehersteller, die den Einsatz ihrer Software in einer VDI explizit untersagen oder eine andere, häufig kostenintensivere Lizenzierung verlangen.

Sind all diese Unterschiede berücksichtigt, lohnt sich ein Blick auf den Aufbau einer typischen VDI-Umgebung, inklusive des Zugriffs durch den Benutzer, wie es in Abbildung 2 dargestellt ist. Dabei sind die VDI-spezifischen Systeme rot eingefärbt, die für die Verwaltung und den Zugriff notwendig sind.

Die eigentliche Arbeit, insbesondere das Ausführen der virtuellen Clients, übernimmt eine Virtualisierungsinfrastruktur, die auf den gleichen Technologien und Prinzipien aufbaut wie eine Server-Virtualisierung.

Die eigentliche VDI wird durch zusätzliche Komponenten umgesetzt, die ggf. auch

5G-Mobilfunk im Gebäude

Fortsetzung von Seite 1

Dr. Joachim Wetzlar ist seit mehr als 25 Jahren Senior Consultant der ComConsult GmbH und leitet dort das Competence Center „Tests und Analysen“. Er verfügt über einen erheblichen Erfahrungsschatz im praktischen Umgang mit Netzkomponenten und Serversystemen. Seine tiefen Detailkenntnisse der Kommunikations-Protokolle und entsprechender Messtechnik haben ihn in den zurückliegenden Jahren zahlreiche komplexe Fehlersituationen erfolgreich lösen lassen. Weiterhin führt er als Projektleiter und Senior Consultant regelmäßig Netzwerk- WLAN- und RZ-Redesigns durch.

Der 5G-Mobilfunk scheint die Welt zu verändern. Ging es beim Mobilfunk jahrelang im Wesentlichen darum, zu telefonieren und das Internet ein wenig nutzen zu können, wird es nun offensichtlich zu einer Basis für unternehmenskritische Anwendungen. Die technischen Konzepte, die eine solche Aufwertung des Mobilfunks ermöglichen, haben wir an dieser Stelle im Rahmen verschiedener Artikel erläutert.

Nun soll es darum gehen, wie der Mobilfunk in unsere Gebäude kommt. Viele Kunden haben uns dazu in den vergangenen Monaten angesprochen; Projekterfahrungen liegen diesbezüglich vor. Darüber möchten wir in diesem Artikel berichten. Und wir möchten noch einmal die Begriffe klären: Sind es wirklich die neuen Features von 5G, die im Gebäude benötigt werden? Falls ja, was bedeutet das technisch? Was ist eigentlich ein privates 5G-Campusnetz?

Wie kommt der Mobilfunk ins Gebäude? Klar, durchs Fenster!? Dass das in der Regel nicht funktionieren wird, ist eine Binsenweisheit. Moderne Gebäude zeichnen sich durch thermische Isolierung aus. Fenster sind oft mit Metall bedampft, damit Sonnenstrahlung nicht ungehindert hineindringt. Funkstrahlung kommt dort ebenso wenig durch. Aus optischen Gründen werden überdies gern Fassaden aus metallischen Materialien angebracht, beispielsweise aus Aluminium. Sie können sich vorstellen, dass derlei Gebäude hervorragend gegen alle Funkwellen von außen abgeschirmt sind − zum Leidwesen aller Mobilfunknutzer.

Die grundsätzlichen technischen Möglichkeiten der Abhilfe haben wir in den letzten Jahren bereits an dieser Stelle diskutiert. Mein Kollege David Feuser stellte im Netzwerk Insider 11/2020 typische Varianten der Inhouse-Mobilfunk-Versorgung vor und wie man die entsprechende Ausleuchtung plant. Ich selbst habe im Januar 2017 erläutert, wie Mobilfunk über WLAN funktioniert, das in modernen Bürogebäuden üblicherweise von jedermann genutzt werden kann.

Auf diese Techniken werde ich in der Folge noch einmal eingehen, jedoch in geringerer Tiefe als in den beiden erwähnten Artikeln. Viel wichtiger erscheint mir jedoch die praktische Vorgehensweise bei derlei Projekten. Wie wählt man die passende Lösung aus? Wie kommt man zu aussagekräftigen Angeboten? Wie nimmt man die Leistung eines Mobilfunkproviders am Ende ab? Beginnen wir zunächst mit der Technik.

Wi-Fi Calling

Das 3rd Generation Partnership Project (3GPP) ist bekanntlich für die Standardisierung des Mobilfunks zuständig. 3GPP hat unter der Bezeichnung „Un-trusted Non-3GPP IP Access“ (u.a. in TS 23.402) ein Verfahren spezifiziert, bei dem sich das mobile Endgerät mit einer IP-Adresse in einem beliebigen IP-Netz befindet, also insbesondere in einem WLAN. Es baut einen mit IPsec geschützten Tunnel zum Mobilfunk-Kernnetz auf und kann darüber alle Dienste so nutzen, als wäre es im Mobilfunknetz eingebucht. Die Provider nennen diese Verbindungsart „Wi-Fi Calling“ oder auch „WLAN Call“.

Die meisten modernen Smartphones unterstützen Wi-Fi Calling. Darüber hinaus muss die Nutzung im Mobilfunkvertrag freigeschaltet sein. Ich selber nutze Wi-Fi Calling mit Erfolg im Homeoffice, da ich in der Nähe der niederländischen Grenze wohne und weder zu deutschen noch zu niederländischen Providern eine brauchbare Mobilfunkverbindung habe. Einige meiner Kunden haben versucht, Wi-Fi Calling für die Nutzung im Unternehmen einzuführen. Die Erfahrungen damit waren eher gemischt, wie zwei Beispiele zeigen:

- Es scheint vom Provider abzuhängen, wie gut Wi-Fi Calling funktioniert. Mein „dienstlicher“ Provider (Deutsche Telekom) schaltet auf WLAN um, sobald es mit guter Qualität verfügbar ist. Mein „privater“ Provider schaltet dagegen auf Mobilfunk um, sobald das Telefon auch nur schwachen Mobilfunkempfang hat. Sie können sich vorstellen, dass dies in meiner Wohnsituation eher unbrauchbar ist. Ich muss also zunächst den Flugmodus wählen und dann WLAN aktivieren, damit Wi-Fi Calling funktioniert. Ähnliches berichteten mir Kunden.
- Des Weiteren wurde ebenfalls berichtet, dass Mitarbeiter über Wi-Fi Calling

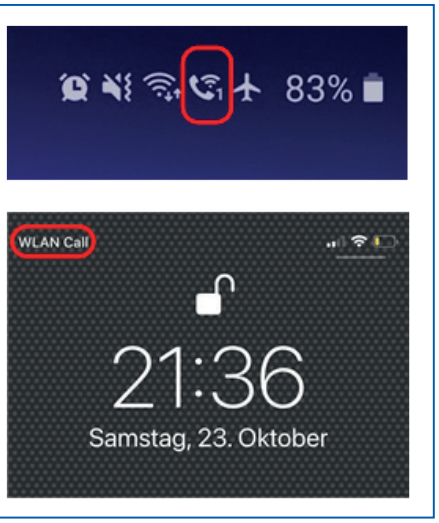


Abbildung 1: Hinweise auf Wi-Fi Calling am Smartphone

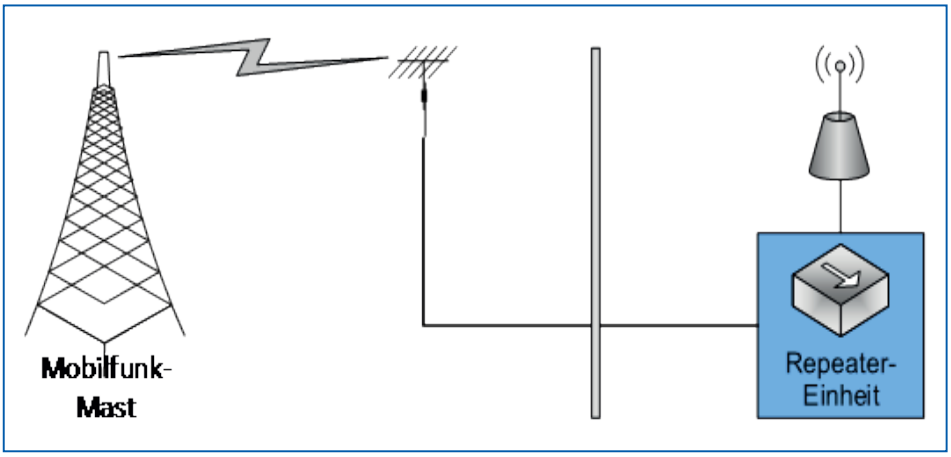


Abbildung 2: Zur Funktionsweise eines Repeaters

erkennbar (siehe Symbole typischer Smartphones in Abbildung 1) eingebucht und dennoch nicht erreichbar waren. Anrufer erzählten, der Teilnehmer sei nicht erreichbar gewesen, und es habe lediglich die Mailbox geantwortet. Der Teilnehmer erhielt jedoch die Kurznachricht (SMS) mit der Rückrufbitte.

Darüber hinaus stellt sich die Frage, wie man bei Wi-Fi Calling Quality of Service im WLAN umsetzt. Einerseits muss man sich darauf verlassen, dass die Smartphones entsprechende Datenpakete mit erhöhter Priorität, z.B. in der Access Category „Voice“, ausstrahlen und auch im IP Header entsprechend markieren. Andererseits kann man erwarten, dass Pakete, die aus dem Providernetz über das Internet eintreffen, keine QoS-Markierungen aufweisen. Hier muss man also selber tätig werden.

Fazit: Wi-Fi Calling funktioniert grundsätzlich, scheint jedoch keine verlässliche Lösung für die flächendeckende Versorgung von Gebäuden mit Mobilfunk zu sein.

Mobilfunk-Repeater

Wenn Sie im Internet nach diesem Begriff suchen, werden Ihnen zahlreiche Seiten angeboten, auf denen Sie derlei Repeater für wenig Geld kaufen können. Mobilfunk-Repeater bestehen aus mehreren Teilen (Abbildung 2):

- Eine Außenantenne, die auf den nächsten Mobilfunkmast ausgerichtet wird. Sie stellt den Kontakt zum Mobilfunknetz her.
- Eine Repeater-Einheit, die indoor angebracht wird und die Signale des Mobilfunknetzes verstärkt.
- Eine Indoor-Antenne, die Ihrem Smartphone eine Verbindung ermöglicht. Es werden auch Repeater angeboten, an die sich mittels Splitter mehrere Indoor-Antennen anschließen lassen.

Außenantenne und Indoor-Antennen dürfen sich nicht „sehen“, was in Abbildung 2 durch eine Wand angedeutet ist. Andernfalls gäbe es eine Rückkopplung. Außerdem dürfen Sie in Deutschland solche Geräte keinesfalls selber betreiben! Die von den Repeatern verstärkten Frequenzen gehören nämlich den Mobilfunk-Providern, die der Bundesnetzagentur viel Geld für die Nutzungsrechte bezahlt haben. Auf Wunsch installieren Ihnen die Provider jedoch Repeater.

Fazit: Mobilfunk-Repeater sind in begrenztem Umfang eine einfache Lösung zur Verbesserung des Mobilfunkempfangs. Installation und Betrieb müssen durch Mobilfunk-Provider erfolgen.

Distributed Antenna Systems

Die Idee des verteilten Antennensystems (Distributed Antenna System, DAS) ist so simpel wie naheliegend: Man nehme eine herkömmliche Mobilfunk-Basisstation und verteile deren Signale mittels Hochfrequenzkabel gleichmäßig auf zahlreiche Antennen im Gebäude. DAS ist im Grunde vergleichbar mit der Verteilung von Fernsehen in einem großen Wohnhaus. Auch dort gibt es einen zentralen Antennenverstärker, der das Signal soweit anhebt, dass es über Koaxialkabel im Gebäude verteilt werden kann. Fernseher werden an Antennensteckdosen angeschlossen, die einen kleinen Teil des auf dem Koaxialkabel anliegenden Signals zum Fernseher auskoppeln und den Rest an die nächste Dose weiterleiten.

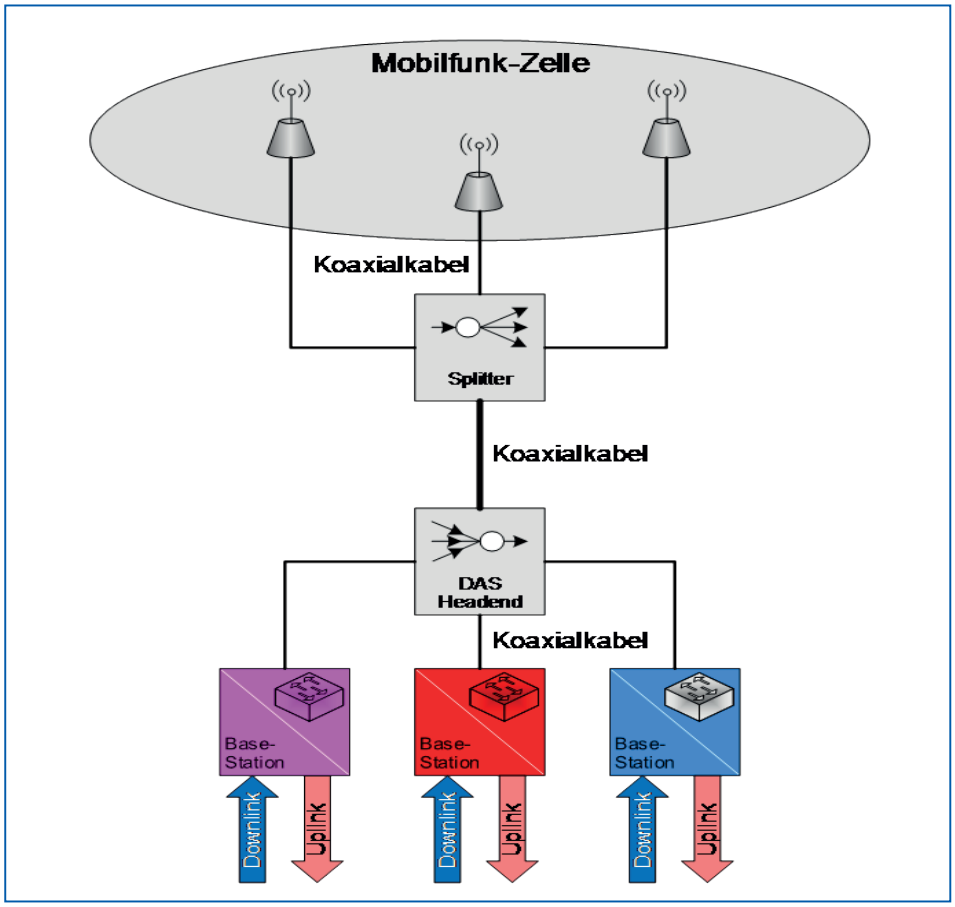


Abbildung 3: Distributed Antenna System