ComConsult Research

Der Netzwerk Insider

Mai 2017

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

„UCaaS Lite“: Können die Cloud-Anbieter mit ihren On-Premises Kollegen konkurrieren?

von Timo Schmitz, B.Sc. und Dipl.-Ing. Dominik Zöller

Cloud-Dienstleistungen der unterschiedlichsten Art sind mittlerweile sowohl im Alltag als auch im beruflichen Umfeld als Alternative zu On-Premises Lösungen angekommen. Die Nutzung von Everything as a Service (XaaS) ist heute kein Wunschdenken mehr, sondern in vielen Fällen bereits gelebte Realität. Warum sollte ein Unternehmen also im Bereich der Kommunikation und Kollaboration, zwei der essentiellen Grundsteine im Businessalltag, auf den Luxus, den ein Full-Managed-Cloud-Service mit sich bringt, verzichten? Dieser Frage folgend, etablierten sich bereits einige der großen Anbieter mit „Unified Communications as a Service“ (UCaaS) Leistungen am Markt (z.B. Microsoft, Cisco, Avaya).

Mit *Amazon Chime* möchte nun auch Amazon einen Teil vom UCaaS-Kuchen abhaben und startete vor kurzem seine eigene Cloud-Kommunikationsplattform. Mit Features wie „crystal clear audio and high definition video [conferencing]“ , gestützt durch die geballte AWS Rechenleistung, versucht der Anbieter seine potentielle Kundschaft zu umgarnen. Wir stellen uns dabei jedoch die Frage: Kann eine solche Lösung aus der Cloud effektiv mit einer On-Premises UC Plattform der Enterprise-Klasse mithalten? Ist der Funktionsumfang vergleichbar, lohnen sich die Kostenunterschiede und welche Vor- oder Nachteile bieten die Varianten?

weiter auf Seite 6

Zweitthema

Abwehr zielgerichteter Angriffe - die Paradedisziplin der Informationssicherheit

von Dr. Simon Hoff und Dipl.-Math. Simon Oberem

Zielgerichtete Angriffe, im Englischen Advanced Persistent Threats (APTs), zur Spionage und Sabotage der IT von Unternehmen, Behörden, politischen Institutionen und insbesondere auch kritischer Infrastrukturen (KRITIS) haben seit mehreren Jahren eine kontinuierliche Präsenz in den Statistiken zu Informationssicherheitsvorfällen.

Von APTs geht ein erhebliches Gefährdungspotential aus, und es ist sogar schon vorgekommen, dass am Ende einer Abwehrschlacht eine Komplettsanierung der IT anstand, wie der Angriff auf den Deutschen Bundestag vom Juni 2015 eindrucksvoll gezeigt hat.

weiter auf Seite 17

Geleit

Verdrängt BGP OSPF? Stehen wir vor einem signifikanten Design-Wandel in unseren Netzwerken?

auf Seite 2

Standpunkt

Ist Windows für Produktionsumgebungen geeignet?

auf Seite 14

Sonderveranstaltung

Das PSTN stirbt: Die neue Kommunikation mit SIP/IP

auf Seite 15

Aktuelle Seminare

Betriebsvereinbarungen und Mitarbeiterdatenschutz bei IT- und TK-Systemen

Sommerschule 2017 – Intensiv-Update auf den neuesten Stand der Netzwerktechnik

auf Seite 13 und Seite 4

Geleit

Verdrängt BGP OSPF? Stehen wir vor einem signifikanten Design-Wandel in unseren Netzwerken?

Diese Frage hat explosiven Charakter. Sie beinhaltet nicht weniger als eine Abkehr von einem Netzwerk-Design, das nun seit mehr als 15 Jahren unsere Unternehmen und Behörden prägt. Und nicht nur das. Die Frage ist gleichzeitig verbunden mit einer komplett anderen Produktauswahl: es geht also nicht um den Austausch von Software. OSPF kommt noch aus der Zeit der großen (und teuren) Modularen Switches im Kern unserer Netzwerke. BGP kommt einher mit einem Parallel-Design aus Nicht-Modularen, relativ einfachen und preiswerten Switches, dafür dann aber in größerer Zahl. Dies geht automatisch einher mit einem deutlich höheren Verkabelungs-Aufwand. BGP liegt voll auf der Linie eines Trends hin zu Switches, die mehr Hersteller-neutral sind, auf Third-Party ASICs basieren (Broadcom und Mellanox dominieren diesen Mark) und die gleichzeitig eine Basis für ein komplett offenes Netzwerk legen könnten (keine Sorge, davon sind wir noch weit entfernt, und natürlich sind Cisco und Konkurrenten fleißig dabei mit Analytics und ähnlichen Anwendungen wieder Hersteller-spezifische Elemente im Markt zu platzieren). Und dies ist keine Hersteller-abhängige Diskussion, auch Cisco ist dabei.

Wir haben die offene Diskussion dieser Frage vor dem ComConsult Netzwerk Forum 2017 begonnen und seitdem hat sie weiter an Fahrt aufgenommen. Tatsächlich hat sie gerade in den letzten Wochen einen neuen Höhepunkt erreicht. Und natürlich ist die Frage auf den ersten Blick absurd. BGP wurde nie für den Einsatz im Rechenzentrum oder im Campus geschaffen (wenn man einmal von den Hyperscalern absieht, deren Design fast immer auf BGP basiert. Dies betrifft nicht nur Facebook und Co., auch Betreiber sehr großer Rechenzentren wie Microsoft sind den Weg nach BGP gegangen). Was bedeutet das, wenn ein Protokoll nicht für einen bestimmten Einsatzzweck geschaffen wurde? Nun, ganz einfach, es erfüllt nicht alle Anforderungen dieses Bereiches. Im Falle von BGP sind das mindestens einmal die notwendigen Umschaltzeiten im Fehlerfall. Hinzu kommt, dass es mehrere Varianten von BGP gibt. So gibt es im Markt ein verwirrendes Produktangebot. Nicht alle Hersteller unterstützen alle Varianten und dies wird ergänzt um Hersteller-spezifische Erweiterungen, um die Mängel an BGP auszugleichen. Ein akzeptierter offener Standard sieht definitiv anders aus. Aber man arbeitet daran. Microsoft hat eine Liste von BGP-Erweiterungen in die Normierung eingebracht, die im Prinzip alle Mängel des Verfahrens beseitigen würden.

Wieso haben wir diese Diskussion überhaupt? Und mit welchen anderen Annahmen oder Fragen geht sie einher?

Der Hauptauslöser dieser Diskussion ist die Unterstützung von Tunnelverfahren im Layer 3-Bereich von Netzwerken. Tunnelverfahren wie VXlan oder Geneve sind für virtuelle Umgebungen unverzichtbar. Der Handlungsdruck ist dabei direkt abhängig von der Größe des virtuellen Bereiches, sprich der Anzahl der virtuellen Maschinen oder Container, und der Anzahl der physikalisch durch Layer 3 getrennten Layer-2-Bereiche. In der reinen Theorie können solche Tunnel-Verfahren in jedem IP-basierten Layer-3-Netzwerk ablaufen ohne dort irgend eine Änderung zu erfordern. In der Praxis gilt dies nur für kleinere und sehr lokale Umgebungen. Für diese ist ein Design mit OSPF und eventuell MC-LAG in der Regel die beste Wahl. Dabei ist die Lokalität wichtiger als die Größe.

Gleichzeitig ist die Prognose von ComConsult Research, die wir exklusiv zu den Technologietagen 2016 im November vorgestellt haben, dass wir eine deutlich Zunahme der Anzahl von virtuellen Maschinen in den nächsten Jahren bekommen werden, die untereinander auf Layer 2 kommunizieren wollen.

Warum ist das so und wieso beeinflusst das das Netzwerk?

Analysiert man die Megatrends in den IT- und Anwendungs-Architekturen so gibt es einen Trend, der sich wie ein roter Faden durch alle Diskussionen zieht: der Zwang zur Agilität. Unter Agilität verstehen wir die Fähigkeit eines Unternehmens innerhalb von Stunden (Minuten oder Tagen, je nach Situation) seine Kapazitäten an Servern, Speicher und Netzwerk um mehrere Hundert Prozent erweitern zu können.

Wo kommt diese scheinbar absurde Forderung her? Wir haben eine ganze Reihe von Industrie-Bereichen, die vor großen Umbrüchen stehen. Beispiele wären Medien, Banken, Versicherungen, Produktionsunternehmen. Ein populäres Beispiel ist der Trend zum autonomen Auto, auch wenn dies eher im Sinne dieser Diskussion ein Randgebiet ist. Auch innerhalb der IT erleben wir große Verschiebungen: angefangen von der Ablösung der traditionellen TK-Anlagen durch UC und nun zum Beispiel im Speicher-Bereich. Generell geht es innerhalb der IT um die Ablösung von Spezial-Hardware durch Standard-Hardware und Software. Auch im Netzwerk-Bereich drohen solche Tendenzen zum Beispiel im Access-Bereich.

Was bedeutet das Wort Umbrüche und mit welchen Forderungen geht es einher?

Nehmen wir als Beispiel den Bankenbereich. Änderungen der Software im Internet-Banking erforderten in der Vergangenheit nicht selten Laufzeiten von 2 Jahren. Die neue Forderung ist: 2 Wochen. Von 2 Jahren auf 2 Wochen: dies ist der rote Faden, der sich durch unsere Untersuchung zieht, ich erspare Ihnen die anderen mehr oder weniger gleich lautenden Beispiele. Wenn es in Ihrer Branche zu einem Umbruch kommt, muss Ihr Unternehmen reagieren können. Und zwar sofort.

Na und, werden Sie denken. Was hat das mit meinem Netzwerk zu tun? Unternehmen können nur agil sein, wenn dies die Anwendungen sind. Agile Anwendungen sind grundsätzlich anders von ihrer Architektur her. Dies ist erforderlich, um zum Beispiel schnelle Änderungen in 2 Wochen in einer Banking-Applikation durchsetzen zu können ohne dabei den Super-Gau zu riskieren. Das Schlüsselwort heißt hier Mikroservice-Architekturen. Große monolithische Anwendungen werden zerlegt in viele kleine Einzel-Services. Diese skalieren besser, zum Beispiel kann ich dann von einem

Verdrängt BGP OSPF? Stehen wir vor einem signifikanten Design-Wandel in unseren Netzwerken?

stark nachgefragten Service schnell einmal 10 oder 100 oder mehr Instanzen nachlegen (wenn dies im Datenbank-Modell möglich ist). Und es ist viel leichter einen kleinen und überschaubaren Service upzugraden als ein großes monolithisches Programm (Anbieter wie Amazon AWS bieten dafür sogar Automatismen). Naturgemäß sprechen wir hier über mittel- bis langfristige Entwicklungen, da Kern-Anwendungen bei Banken und Versicherungen nicht mal eben so abgelöst werden können.

Was ist aber ein Service? In der Regel eine virtuelle Maschine (oder ein Container, diese Diskussion lasse ich hier mal aus). Dies bedeutet: ein Service hat eine MAC-Adresse und kommuniziert mit den anderen Services einer Applikation über Layer 2.

Services der Zukunft liegen immer in virtuellen Umgebungen, die die Eigenschaften der Cloud nachbilden (ich will das hier nicht vertiefen). Damit haben wir in diesen Umgebungen eine starke Zunahme der Layer-2-Teilnehmer zu erwarten. Naturgemäß findet das dann erst einmal nicht im physikalischen Netzwerk statt. Im Gegenteil beobachten wir einen Trend zu einer internen Strukturierung solcher Netzwerke mit NFV innerhalb der virtuellen Welt. Dummerweise müssen aber auch virtuelle Welten irgendwie mit der Realität kommunizieren oder auch mit anderen virtuellen Umgebungen verbunden werden. Hier kommen jetzt die Tunnel-Verfahren wie VXlan zum Einsatz. Und damit kommen wir zum guten alten Hardware-Netzwerk.

Um die Diskussion in diesem Geleit abzukürzen gibt es eine zentrale Forderung für das Design der Netzwerke der Zukunft:

- das Layer-3-Netzwerk der Zukunft muss aber einer bestimmten Größe oder Verteiltheit die Existenz von Tunnel-Verfahren kennen und diese auch unterstützen.

Diese Frage ist zentral und kann nicht genug herausgehoben werden. OSPF kann das nicht und müsste dementsprechend in den Netzwerk-Bereichen, in denen das benötigt wird, abgelöst werden. Wir wollen defakto Broadcast-Flutungen in unseren Layer-3-Bereichen vermeiden und wir wollen aktiv zwischen Tunnel-Endpunkten routen. OSP fehlt die Fähigkeit die notwendigen Informationen dazu zu übertragen. Und hier ist BGP natürlich prädestiniert. Die Vermittlung von Informationen zwischen autonomen Systemen ist ja der Design-Kern von BGP. Nur wurde BGP eben nicht für lokale Umgebungen geschaffen. So sind seine Umschaltzeiten deutlich zu lang und auch ECMP, also die Schaffung paralleler gleichwertiger Wege, die zum Kern des neuen Designs gehören, ist keine Standard-Eigenschaft von BGP (kann aber konfiguriert werden). Und damit sind wir bei einem anderen theoretischen Nachteil von BGP: es wurde für Provider entwickelt. Dies bedeutet, dass es aufwendig zu konfigurieren ist (das ist so, aber wieso eigentlich?). Es ist in keinem Fall selbst-lernend wie OSPF. Hier kommen natürlich wieder die Hersteller mit ihren Hersteller-spezifischen Management-Lösungen ins Spiel. Auf der Basis einer Layer-2-Discovery ist es zum Beispiel möglich den Konfigurations-Aufwand deutlich zu senken (siehe Extreme als Beispiel).

Ist BGP die einzige Alternative in dieser Situation? Nein, ist es nicht. IS-IS wäre eine andere und vielleicht näher liegende Variante gewesen, die in Kombination mit SPB zum Einsatz kommt und die Übertragung von Service-Informationen unterstützt. Aber diese Variante ist im Markt nicht angenommen worden (warum eigentlich nicht, das wäre die nahe liegendere Lösung gewesen?).

Damit sind wir natürlich noch nicht am Ende der Diskussion. Tatsächlich ist die Diskussion umfassend und betrifft fast das ganze Netzwerk.

Und wir greifen auch die anderen Elemente der Diskussion auf der Sommerschule auf:

- wo sollte die Grenze zwischen Layer-2 und Layer-3 in Zukunft sein? Virtualisierungs-Hersteller wie VMware sehen Layer 2 komplett in der virtuellen Welt. Die einzige Aufgabe des Hardware-Netzwerkes aus der Sicht von VMware besteht in der Verbindung der virtuellen Systeme. Auch VMware empfiehlt zu diesem Zweck BGP (zumindest in den USA).

- wo ist die Control-Plane für die Tunnel-Verfahren? Innerhalb der virtuellen Welt, NSX sei das typische Beispiel? Oder im Hardware-Netzwerk, E-VPN ist hier der Trend? Ist dies der Kampf zwischen Netzwerkern und Server-Betreibern oder den Virtualisierungs-Herstellern und müssen wir das ausbaden? Aus meiner Sicht ist für die Control-Plane nur eines entscheidend: sie muss offen und Hersteller-übergreifend sein. Tatsächlich würde ich hier einen Einsatzbereich für SDN sehen. BGP mit E-VPN wird mit seiner Komplexität leben oder sterben. Wird keine halbwegs automatische Form der Konfiguration gefunden, werden die Hersteller-spezifischen Verfahren den Markt übernehmen.

- gilt diese Diskussion nur für das Rechenzentrum oder auch für den Campus?

- was passiert im Access-Bereich? Die Zukunft ist hier aus heutiger Sicht Wireless. Die weltweiten Zahlen im Verkauf sprechen hier eine deutliche Sprache. Aber wir stoßen klar an die Grenze der aktuellen WLAN-Technologien, was nun?

Gerade der letzte Punkt ist entscheidend. Wir sehen klar die Limitierung der aktuellen WLAN-Technologien für den Fall, dass sie weiter deutlich ausgebaut werden sollen. Gleichzeitig entsteht mit 5G ein Monster, das zwar noch 4 bis 5 Jahre auf sich warten lässt, das wir aber im Design von neuen Gebäuden in keinem Fall ignorieren dürfen.

Lange Rede kurzer Sinn: Netzwerk-Design ist auf dem Prüfstand. Und dabei bleibt kein Stein auf dem anderen. Je nach Branche kann es sein, dass Sie Zeit haben, oder auch nicht. Aus unserer Sicht ist der Trend zumindest im Rechenzentrum klar: BGP wird OSPF ablösen. Ob und in welchem Umfang das Auswirkungen auf den Campus haben wird, kann man zum jetzigen Zeitpunkt wohl nicht pauschal sagen. Aber natürlich wird es die Umgebungen geben, in denen man dieses Design nach Lösung einiger offener Fragen (Stichwort: Konfigurationsaufwand, Umschaltzeiten) bis zu den Gebäuden ausdehnen will. Dabei spielt es auch eine große Rolle, dass die bisherige Trennung zwischen Layer-2 und Layer-3 eine künstliche ist. In vielen Fällen wurde sie durch die höheren Kosten eines Layer-3-Designs ausgelöst. Aber für moderne Switches mit Standard-ASICs gibt es keinen technischen Grund warum ein Layer-3 Switch teurer sein sollte als ein Layer-2 Switch (bei einem einfachen Standard-Verfahren wie BGP, natürlich gibt es Abhängigkeiten bezogen auf den Ausbau mit schnellem und teurem Puffer-Speicher oder ähnlichen Merkmalen). Dies ist auch eine Marketing-Entscheidung des Herstellers. Der Trend dürfte aber bei den hier angesprochenen Produkten zu einer starken Reduzierung der Preise von Layer 3 gehen.

Mehr dazu auf der Sommerschule. Hier bieten wir Ihnen unsere Analysen und den Raum für Diskussionen zu diesem für alle entscheidenden Thema.

Zum Thema Mikrosegmentierung und Ablösung großer monolithischer Anwendungen haben wir vor einigen Monaten einen Selbstversuch gestartet. Wir lösen ComConsult Study.tv durch eine Cloud-Installation ab und vergleichen dabei gleichzeitig Amazon AWS mit Microsoft Azure. Unsere Erfahrungen bisher liegen voll auf der Linie unserer Analyse für das Technologieforum 2016. Der funktionale Mehrwert der Cloud-Umgebungen ist deutlich wichtiger als ihr Preis. Wir kombinieren diese Tests mit dem Vergleich der Netzwerk-Designs in der Cloud und in der Anbindung der Cloud. Wir berichten über den aktuellen Stand auf der Sommerschule.

Ihr
Dr. Jürgen Suppan

Aktuelles Seminar

Sommerschule – Intensiv-Update auf den neuesten Stand der Netzwerktechnik

03.07. - 07.07.2017 in Aachen

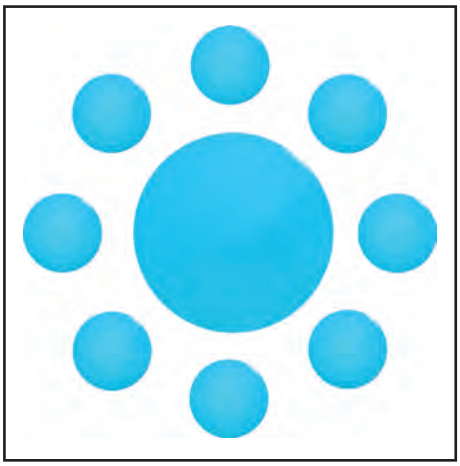
Die ComConsult Akademie veranstaltet vom 03.07. bis 07.07.2017 ihr Seminar "Sommerschule – Intensiv-Update auf den neuesten Stand der Netzwerktechnik" in Aachen.

Die Sommerschule 2017 bringt Sie in 5 Intensiv-Tagen auf den letzten Stand der Netzwerk- und Kommunikations-Technik. Ausgehend von einer aktuellen Bedarfsanalyse bewerten wir neue Technologien, zeigen deren Potenziale auf und geben umsetzbare Empfehlungen für die Zukunft Ihrer Netzwerke und Infrastrukturen.

Die IT-Zukunft und ihr Bedarf für Netzwerke
- welche konkreten Anforderungen an Netzwerke und IT-Infrastrukturen gibt es für die nächsten Jahre?
- wie kann Zukunfts-sicher investiert werden?

Agilität und Skalierbarkeit
- mit welchen Verfahren und Architekturen kann schnell auf einen sich ändernden Bedarf reagiert werden?
- wie können Skalierbarkeit und Routing erfolgreich kombiniert werden?

Die Zukunft der Netzwerke, das Ende der Hardware, die Rolle der Software
- welche Rolle spielt der Hardware-Switch in Zukunft?
- auf welche ASIC-Eigenschaften muss beim Kauf geachtet werden?
- wo suchen die Hersteller in Zukunft Alleinstellungsmerkmale?



- gibt es wieder eine Chance für ein rein Standard-basiertes Netzwerk?

Was bedeuten VXLan und Geneve für die Architektur von Netzwerken
- warum werden sie gebraucht?
- müssen diese Verfahren im Switch unterstützt werden?
- wie geht man damit um?
- wer plant die Nutzung und wer hat die Betriebshoheit?

Das neue Layer 2 und seine Herausforderungen
- Layer 2 nur noch mit Software-Switches im Hypervisor?
- Layer 3 in Hardware?
- wer gestaltet das Gesamtkonzept?

Kampf um das "neue" Layer 3
- wieso auf einmal BGP, gehört ihm die Zukunft?
- was ist mit IS-IS und OSPF?
- welche Kriterien sind unverzichtbar?
- was bedeutet VXLan-/Geneve-Unterstützung im Layer 3?

Netzwerk-Sicherheit und die Cloud
- warum gewinnt Netzwerk-Sicherheit so an Bedeutung?
- welche neuen Ansatzpunkte gibt es?
- Sicherheit mit, durch oder in der Cloud?

Positionierung der Cloud
- müssen wir die Cloud einbeziehen?
- wie sieht die Verbindung aus?
- wie werden Netzwerke in der Cloud gestaltet?

Das WLAN der Zukunft und die Abgrenzung zum Mobilfunk
- WLAN kommt an seine Grenzen, warum ist das so?
- wie sehen Lösungen zur besseren Skalierung aus?
- Mobilfunk wächst in eine neue Dimension: was ist die Perspektive und was bedeutet das für das WLAN?

Die Zukunft von Telefon und Video
- was bedeutet Ende von ISDN?
- wie sieht die Kommunikation der Zukunft funktional aus?
- wie kann das zu Cloud-Angeboten abgegrenzt werden?

Anmeldung an kundenservice@comonsult-research.de

Sommerschule 2017

Ich buche das Intensiv-Seminar
Sommerschule 2017
03.07. - 07.07.2017 in Aachen

☐ zum Preis von € 2.290,-- netto*

☐ Bitte buchen Sie mir ein Hotelzimmer

*gültig bis zum 31.05.2017

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

_____ Vorname	_____ Nachname
_____ Firma	_____ Telefon/Fax
_____ Straße	_____ PLZ,Ort
_____ eMail	_____ Unterschrift

Programmübersicht Sommerschule

Montag, der 03.07.17 - IT-Architekturen und ihre Auswirkung auf Netzwerke

10:00 - 12:30 Uhr
Aktuelle Technologie-Trends und ihre Bedeutung für die IT
- Wie ändert sich die IT und welche Auswirkungen hat das auf Infrastrukturen?
- Was passiert auf der Netzwerkseite, um diesen Anforderungen zu entsprechen?
  - Welche Architektur-Eigenschaften müssen Netzwerke für die IT der Zukunft haben?
- Welche neuen Technologien müssen speziell bei den Planungen für die nächsten Jahre beachtet werden?

Dr. Franz-Joachim Kauffels, Technologie-Analyst

14:00 - 15:15 Uhr
Cloud Computing – Einsatz im Unternehmen
- Infrastructure as a Service: Server und Speicher aus der Cloud
- Software as a Service
- Warum Cloud-Anwendungen anders sind
  - Anforderungen / Hybrid-Clouds/ Single-Sign-On
- Office 365
  - Überblick
  - Assessment: Anforderungen an die Netzanbindung

Dipl.-Math. Cornelius Höchel-Winter, ComConsult Research GmbH

15:15 - 17:00 Uhr
Netzwerk-Gestaltung in und mit der Cloud
- Was sind typische Cloud-Dienste und wie wirken sie zusammen?
- Welche Netzwerk-Komponenten gibt es in der Cloud?
- Worauf ist beim Design einer Lösung zu achten?
- Welche nativen Sicherheitsmechanismen bieten Cloudprovider?
- Welche Verbindungsvarianten für Hybrid-Cloud-Lösungen existieren?
- Was lässt sich seriös über die Kosten einer Cloud-Lösung sagen?
- Umzug von ComConsult-Study.tv in die Cloud: Projekterfahrung?

Markus Schaub, ComConsult-Study.tv

11:00 - 11:15 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
15:00 - 15:15 Uhr Kaffeepause
ab 19:00 Uhr Happy Hour

Dienstag, der 04.07.17 - RZ-Netzdesign

9:00 - 15:45 Uhr
Das RZ-Netzdesign der Zukunft: Overlays und Tunnel prägen die Protokollauswahl
- Motivation: Warum Overlays?
  Wo liegen die Vorteile solcher Strukturen?
- Welche Tunnelprotokolle stehen zur Verfügung, wo liegen die Unterschiede und wie sieht deren Zukunft aus: SPB / TRILL / VXLAN / NVGRE / Geneve
- Welche Möglichkeiten gibt es, diese Strukturen zu steuern? Wie sieht die jeweilige Control Plane aus? Die Rolle von BGP und EVPN: Kann es die eine Control Plane geben?
- Wie werden virtuelle Server integriert? Hypervisor vs. Netzwerkkomponente: Wo enden die Overlays? NFV und das Software-Defined Datacenter: Was leistet die Control Plane im Hypervisor? Produktüberblick: VMware NSX, Cisco ACI, Anwendungsfälle

Konsequenzen für das Underlay:
- Ist BGP das neue Routing-Protokoll im LAN?
  - Was unterscheidet das bisherige OSPF Layer 3 Design vom BGP Ansatz?
  - Was steckt hinter der Idee von BGP im RZ, Core & Campus?

  Welche Auswirkungen hat der Einsatz von iBG bzw. eBGP auf das Netzdesign?
  Welcher Ansatz eignet sich für die Anwendungsfälle im RZ?
  Wie werden die Nachteile von BGP gegenüber OSPF kompensiert:
  - Konvergenz Beschleunigung
  - Automatisierter Aufbau von BGP Peers
  - Equal Cost Multipathing (ECMP)
- Switch Fabrics
  BGP im Hyperscaler DC:
  - Das Netzdesign von DCs mit mehr als 1 Million Server
  - Die Adaption für das Unternehmens RZ

  Warum kommen Layer 2 Fabrics aus der Mode:
  - IS-IS Fabric mit Cisco, Juniper, Brocade
  - Was spricht gegen diese Ansätze
- Spine Leaf vs. klassischer DC Aufbau:
  Warum Spine Leaf oder die Dominanz von Ost-West Verkehr im RZ
  Vorteile des Scale Out Ansatzes
- Campus LAN:
  Layer 3 Fabric bis in den Edge Bereich
  Layer 2 mit MC-LAG vs TRILL/SPB & Spanningtree
  - Was der Standard zulässt

Markus Geller, Dipl.-Math. Cornelius Höchel-Winter, ComConsult Research GmbH

10:30 - 10:45 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
15:30 - 15:45 Uhr Kaffeepause

Mittwoch, der 05.07.17 - Sicherheit im Netzwerk und aus der Cloud

9:00 - 17:00 Uhr
Informationssicherheit in und aus der Cloud
- Neue Netzwerkkonzepte durch Cloud-Computing
- Integration Private Cloud und Provider Cloud
- Herausforderung sicheres Cloud Computing
- Standardisierte und zertifizierte Cloud-Sicherheit
- Virtuelle Sicherheits-Gateways und virtuelle Internet DMZ in der Cloud: Mehr als ein Trend!
- Management von WLAN und LAN-Komponenten aus der Cloud
- Rolle der Cloud bei der Abwehr von Distributed Denial of Service (DDoS)
- Rolle von Data Loss Prevention für die Nutzung von Cloud-Diensten

Abwehr zielgerichteter Angriffe
- Angriffsmethoden und Werkzeugkasten
- Erkennung von Symptomen
- Sandboxing
- Protokollierung, 2nd Generation SIEM und Big Data
- Bedeutung eines Information Security System für die Abwehr zielgerichteter Angriffe
- Abwehr zielgerichteter Angriffe durch Cloud-Dienste
- Systematisches Schwachstellenmanagement, Behandlung von Sicherheitsvorfällen
- Vulnerability Scanning: Techniken und Werkzeuge
- Demonstration

NAC in der Praxis
- Warum IEEE 802.1X immer noch ein Alptraum sein kann
- Best Practice NAC: Wie NAC erfolgreich umgesetzt und betrieben werden kann
- Der Teufel steckt im Detail: Wo sich die Hersteller unterscheiden
- Projektbeispiele und typische Fehler in der Praxis
- Evolution von NAC: MACsec, Advanced Monitoring und Profiling

Zonenkonzepte als Standardinstrument zur Absicherung der IT
- Warum Zonenkonzepte zu einem Standard-instrument geworden sind
- Zonen im Campusbereich und die Rolle von NAC
- Zonen im Rechenzentrum, zwischen Rechenzentren und über WAN
- Zonen in der Cloud, zwischen Private Cloud und Provider Cloud
- Zonen in der virtualisierten Welt: Wie sehen Zonenkonzepte für Network Overlays aus?
- Virtualisierte Firewalls, Hypervisor-Integration von Firewalls
- Staging-Umgebungen: Trennung von Entwicklung/ Test und produktiver Umgebung
- Zonenkonzepte in der Industrial IT
- Prozesse für den Betrieb einer Zonenarchitektur
- Storage und Datensicherung in einem zonierten Netz
- Projektbeispiele

Dr. Simon Hoff, Dipl.-Math. Simon Oberem, Dipl.-Inform. Daniel Prinzen, Sebastian Wefers, ComConsult Beratung und Planung GmbH

10:30 - 10:45 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
15:00 - 15:15 Uhr Kaffeepause

Donnerstag, der 06.07.17 - Die Zukunft des Access ist Wireless

9:00 - 12:30 Uhr
WLAN als produktionskritische Infrastruktur?!
- Weiterentwicklung des WLAN mit 10 Gbit/s und für hohe Client-Dichten
- Neues Band, neues Glück: Kommt jetzt endlich 60-GHz-WLAN, und was bringt es uns?
- Anwendungen in Office und Shop Floor, was sind die Anforderungen?
- Maßnahmen zur Skalierung von WLAN
- Beispiele aus einem Projekt im Industrie-Umfeld

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

14:00 - 17:00 Uhr
Analyse der neuesten Entwicklungen
- Explosives Wachstum in allen Anforderungsbereichen
- Echte Multi-Gigabit WLANs mit IEEE 802.11ad
- Die nächsten WiFi-Generationen 11ax und 11ay
- Die Entwicklung von LTE
- Problematik von LTE in lizenzfreien Bereichen
- Kommt schneller als man denkt: 5G Mobilfunk
- Anforderungen an unterstützende Infrastrukturen

Dr. Franz-Joachim Kauffels, Technologie-Analyst

Diskussion
- Welche Rolle wird WLAN in der Zukunft haben?
- Müssen wir seine Nutzung einschränken und bestimmten Anwendungen vorbehalten?
- Wie sollten neue Gebäude vorbereitet werden?
- Wird der Access-Bereich in Zukunft ganz Wireless?
- Wird 5G Teile des heutigen WLAN übernehmen?
- Wie kann das umgesetzt werden? Provider-Installationen im Haus, elektromagnetische Abschirmung von Gebäuden?

10:30 - 10:45 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
15:00 - 15:15 Uhr Kaffeepause

Freitag, der 07.07.17 - Die Welt nach ISDN

9:00 - 15:30 Uhr
Die Welt nach ISDN: Funktionalität, System-Alternativen und Herausforderungen
- All-IP – und jetzt? (Einleitung, Motivation)
- Wo ist das Call-Routing? Und weitere Fragen zu All-IP (On-Premises vs. Hosting vs. Cloud-Ansätze)
- UC aus der Cloud? Ein Überblick
- UCaaS – einfach via Internet? Das Zusammenspiel von Netz und Cloud
- Garanten der Netzqualität? Assessment und Monitoring von VoIP und UC

SIP vs PSTN
- Kanalvermittlung vs. Paketvermittlung
- Rufaufbau und Echtzeit-Datenstrom
- Bandbreitenbedarf

Was geschieht bei einer Überbuchung der Datenleitung?

Warum ist CAC so wichtig?
- SIP Response Codes und ihre Bedeutung
- Gebührenabrechnung

Advice of Charge Varianten
- Woher kommt die Zeit?

NTP
- Layer 2/3 Multipath Probleme • QoS Grundlagen

VoIP Access
- Trunk Produkte
- T-Systems/Telekom; BT; Vodafone; O2/Telefonica; Colt
- Netzanschaltung (DSL, Cable, Fiber)
- Allgemeine Leistungsmerkmale
- Design Beispiele für Standorte und Niederlassungen

Der Weg zu All-IP
- NNI Standards

ETSI TISPAN für Deutschland
- SIP URI vs. Tel URI (DNS, ENUM,…) • TR Notruf 1.0

TR Notruf 2.0 Entwurf 2017

Markus Geller, ComConsult Research GmbH, Dipl.-Ing. Dominik Zöller, ComConsult Beratung und Planung GmbH

10:30 - 10:45 Uhr Kaffeepause
13:00 - 14:00 Uhr Mittagspause
15:30 Uhr Ende der Veranstaltung

Der Veranstalter behält sich Änderungen im Programm vor.

Schwerpunktthema

„UCaaS Lite“: Können die Cloud-Anbieter mit ihren On-Premises Kollegen konkurrieren?

Fortsetzung von Seite 1

Timo Schmitz, B.Sc. ist bei der ComConsult Beratung und Planung GmbH in den Bereichen „Kommunikationslösungen“ und „IT-Sicherheit“ tätig. Im Projektgeschäft befasst er sich u.a. mit der Erstellung von Konzepten und der Erarbeitung von Seminarinhalten.“

Dipl.-Ing. Dominik Zöller ist seit 2006 Berater bei der ComConsult Beratung und Planung GmbH und fungiert hier als Leiter des Competence-Center „Kommunikationslösungen“. Gemeinsam mit seinem Team berät er eine Vielzahl von Kunden in Privatwirtschaft und öffentlichem Sektor. Die thematische Spannbreite umfasst insbesondere die Themenfelder Unified Communications, Sprachkommunikation, Kollaborationswerkzeuge, integrierte Geschäftsprozesse und sichere Kommunikationslösungen. Herr Zöller ist regelmäßig als Referent für die ComConsult Akademie tätig und als Autor und Co-Autor an einer Vielzahl von Veröffentlichungen beteiligt. Unter anderem ist er Co-Autor der „Technischen Leitlinie für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf“ (TLSTK II) des BSI.

Um diesen Fragen nachzugehen schauen wir uns zwei Anbieter einer solchen Cloud-Dienstleistung einmal genauer an: Zum einen Amazon Chime, als Neuankömmling in der Branche, sowie *Zoom*, einem erfolgreichen und mittlerweile etablierten Anbieter, mit über die Jahre aufgebauter Expertise im Bereich der Multi-Tenancy Unified Communications.

Amazon Chime

Mit den Amazon Web Services (AWS) entwickelte sich Amazon zu einem der populärsten und erfolgreichsten Anbieter im Segment des Cloud Computings. Die Angebote entwickelten sich im Laufe der Jahre kontinuierlich hin zu einem breit aufgestellten Leistungsportfolio. Im Februar 2017 entschied sich Amazon nun dazu, einige der Kapazitäten für eine eigene Kommunikationsplattform zur Verfügung zu stellen: *Amazon Chime* (siehe Abbildung 1).

Amazons Versuch in den Cloud-basierten UC Markt einzudringen, kann als Angriff gegen Mitbewerber wie Microsoft mit *Office 365* oder Google mit seinen als *G Suite* vermarkteten Unternehmensapplikationen gewertet werden. Bern Elliot, ein Analyst von Gartner, schätzt den Umsatz im entsprechenden Marktsektor auf 12 Milliarden Dollar im Jahr 2016 ein. Dieser soll seinen Einschätzungen zufolge, um 15 % wachsen und damit ein Umsatzhoch von 22 Milliarden Dollar im Jahr 2020 erreichen [2] (Anm. d. Autors: ein Wachstum von 12 auf 22 Mrd. Dollar binnen vier Jahren entspricht einem CAGR von durchschnittlich 16,3%). Im Unterschied zu Microsoft oder Google kann Amazon jedoch wenig Erfahrung im UC Bereich vorweisen. Um diese Wissenslücke zu schließen, erwarb Amazon im Jahr 2015 das Unternehmen *Elemental*, welches sich laut eigenen Angaben mit „Software-Defined Video Processing Solutions“ auseinandersetzt. Im darauffolgenden Jahr eignete das Unternehmen sich zusätzlich *Biba* an – ein Anbieter für Chat, Video und Audio Conferencing. Die dadurch gewonnen technologischen Erkenntnisse stellen die Basis für die nun erschienene Amazon Chime Dienstleistung dar.

Chime bietet seinen Nutzern, laut Produktkatalog [3], die gängigen UC Funktionalitäten, wie beispielsweise Online Meetings, Videokonferenzen, Chaträume, Smart Presence sowie Datenaustausch. Gegenüber seinen Konkurrenten möchte sich Chime u.a. durch herausragende Audio- sowie Videoqualität hervorheben. Eine zentrale Applikation soll als Einstiegshub für die verschiedenen Kommunikationsdienste dienen, die von stationären und mobilen Geräten angesteuert werden können. Hierbei verspricht Amazon einen „nahtlosen Übergang“ (auch während Meetings) zwischen den verschiedenen Gerätetypen, inklusive automatischer Synchronisation zwischen diesen.

Für die Nutzung von Amazon Chime werden Applikationen für die Plattformen iOS, Android, Windows sowie Mac bereitgestellt. Raumsysteme, die H.323 mit G.711/G.722 unterstützen, können eben-

„UCaaS Lite“: Können die Cloud-Anbieter mit ihren On-Premises Kollegen konkurrieren?

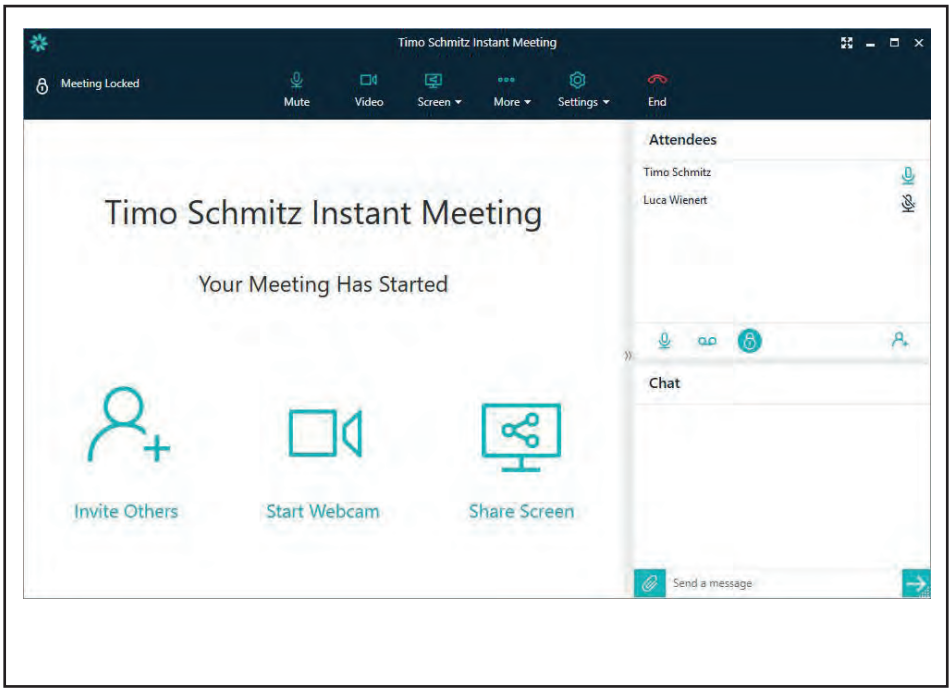


Abbildung 1: Amazon Chime Meeting User Interface

falls (ohne zusätzliche Kosten) in Meetings eingebunden werden. Damit werden die gängigsten Systeme im Enterprise-Umfeld unterstützt; einem nicht zu unterschätzenden Teil des Marktes (Linux, Windows Phones, …) wird jedoch – wie marktüblich – zunächst der Zugang verwehrt.

Dies wäre verschmerzbar, wenn die UC Plattform einen Zugriff über den Browser ermöglichen würde. Leider scheitert der Dienst in diesem Bereich jedoch kläglich: In Zeiten von HTML5 und WebRTC mit einem Produkt an den Markt heranzutreten, welches lediglich massiv eingeschränkte Funktionalitäten im Browser bietet (einzige Browser-Funktionalität: Beobachtung der Bildschirmfreigabe – ohne Audiofeed; siehe Abbildung 2), ist nicht mehr zeitgemäß. Gerade bei Cloud-Dienstleistungen sollte eine vollständige Plugin-lose Browser Lösung, auf Basis moderner, mittlerweile weit verbreiteter Protokolle, eine Selbstverständlichkeit darstellen. Interessant ist dabei, dass die Amazon Chime Software laut ersten Meldungen wohl WebRTC als technologische Basis einsetzt [4] – ohne die Möglichkeit zur Nutzung im Browser, geht der größte Mehrwert dieser Technologie für den Kunden jedoch verloren.

Insbesondere externe Teilnehmer sind dadurch gezwungen, eine proprietäre Software herunterzuladen, sofern sie am Videochat teilhaben wollen. Immerhin: Ein externer Teilnehmer muss hierfür keinen Account anlegen (anonyme Teilnahme). Für interne Teilnehmer ist außerdem eine SAML-basierte SSO Anmeldung möglich – sofern ein Chime Plus Account vorliegt.

Um externen Teilnehmern die Installation der Applikation zu ersparen, bietet Chime jedoch die Möglichkeit des Dial-In auf Kostenbasis einer Per-Minute-Rate. Auf sämtliche weitere UC Features fernab der Audiokommunikation muss der Teilnehmer dann natürlich verzichten. Die Kosten belaufen sich bei Anrufen aus Deutschland derzeit auf $0,004/Min. bzw. ca. 0,4 Euro-Cent/Min. [5]

In Punkto Sicherheit kann Amazon Chime eine AES 256-Bit Verschlüsselung vorweisen. Grundsätzlich gibt sich Amazon etwas wortkarg in der Beschreibung der Sicherheitsumstände, unter denen die (ggf. streng vertraulichen) Gesprächsdaten gesichert werden: „Amazon Chime is an AWS service, which means you benefit from a data center and network architecture built to meet the requirements of the most security-sensitive organizations“. [3]

Wie der Titel bereits andeutet: Man sollte Amazon Chime nicht ohne weiteres als vollwertige UCaaS Lösung bezeichnen. Die Telefonie über SIP-Nebenstellen kann nicht durch die Applikation übernommen bzw. aufgefangen werden. Eine Ergänzung der Lösung im Sinne einer Hybrid Cloud oder einer Kombination von Cloud-Lösungen wird daher vonnöten sein, wodurch die ursprünglich eingesparten Investitionskosten u.U. wieder hinfällig sein werden.

Beim Zahlungsmodell setzt Amazon auf ein gestaffeltes Abonnement-Modell und die „Pay-As-You-Go“ Zahlungsvariante. Basisfunktionalitäten, wie die 1:1 Kommunikation, stehen Nutzern dabei kostenlos zur Verfügung. Für $2,50/User/Monat stehen Funktionalitäten zur Bildschirmfreigabe sowie Anbindung an das Active Directory zur Verfügung. Um Meetings selbst leiten und erstellen zu können, wird jedoch eine Pro Lizenz notwendig, welche mit $15/User/Monat zu Buche schlägt. Diese ermöglicht die Erstellung von Video Meetings für bis zu 100 Teilnehmer. Abbildung 3 stellt die Funktionalitäten, die durch die jeweilige Lizenz freigeschaltet werden können, noch einmal explizit vor. Zunächst erscheint das Zahlungsmodell mit der Basic und Plus Variante preislich sehr fair gestaltet. Der drastische Preisunterschied zwischen der Plus und Pro Lizenz stößt dabei jedoch sauer auf. Bei

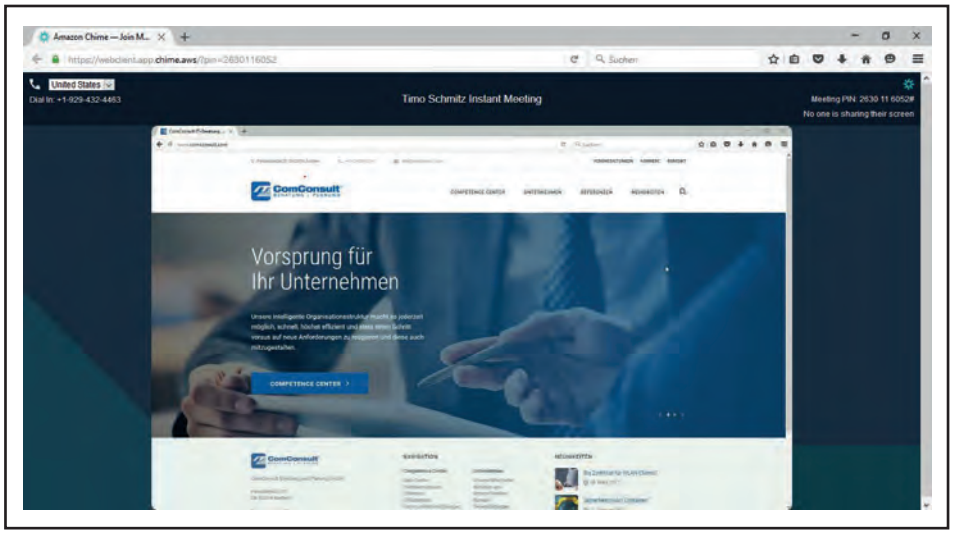


Abbildung 2: Amazon Chime Ansicht einer Bildschirmfreigabe im Browser

der praktischen Nutzung des Angebots werden potentielle Kunden dadurch nicht umhin kommen, ihre Power-User mit den teuersten Lizenzen auszustatten, obwohl die Teilnehmergröße eines Meetings die Grenze von 10 Personen möglicherweise nie übersteigen würde. Hier wäre eine weitere, kundenfreundlichere Preisstaffelung wünschenswert.

Insgesamt wirkt Amazon Chime im Vergleich zu konkurrierenden Angeboten eher wie ein hastig auf den Markt gebrachtes Produkt. Es wirkt wie der Versuch den Anschluss an Konkurrenzprodukte zu gewinnen, welche mittlerweile jedoch von jahrelanger Erfahrung und Detailverbesserung profitierten. Oberflächlich betrachtet kann die Software zwar die grundsätzlichen UCaaS Leistungsmerkmale liefern – der Teufel steckt jedoch im Detail. Im direkten Vergleich zeigt sich, dass einzelne Funktionalitäten an vielerlei Stellen unausgereift wirken und durchaus Potential nach oben vorhanden ist: Im Praxistest konnte die Bildschirmfreigabe häufig nicht aufgebaut werden, Chats sind nicht durchsuchbar, Kontakte können nicht gruppiert werden, die Performanz insgesamt wirkt verbesserungswürdig, der Installationspfad der Applikation kann nicht angepasst werden, etc.. Amazon Chime ist darüber hinaus zum jetzigen Zeitpunkt ausschließlich in einer englischsprachigen Fassung verfügbar.

Hinsichtlich der notwendigen Hochverfügbarkeit des Dienstes, hätte es bei Amazon Chime bis vor kurzem wahrscheinlich deutlich weniger Bedenken gegeben. Die medial hohe Wellen schlagenden Störungen von Amazon S3 Ende Februar 2017 [6], zeigen hier jedoch eindrücklich, welches Risiko mit der Nutzung von Diensten „in der Cloud“ eingegangen wird. Die technische Realisierung der Verfügbarkeit ist also ein wichtiges Kriterium für Cloud Services, das vor einer Entscheidung für einen Dienst sorgfältig geprüft werden muss. Bei On-Premises Lösungen ist man vor derartigen Ausfällen natürlich ebenfalls nicht geschützt, kann jedoch gegebenenfalls Eigeninitiative ergreifen, um dem Problem präventiv entgegenzuwirken und aktiv zur Beseitigung des Problems beitragen.

Zoom

Gegenüber dem Newcomer Amazon Chime wirkt Zoom, eine Dienstleistung des 2011 gegründeten Unternehmens *Zoom Video Communications, Inc.*, wie ein reiferer großer Bruder. Zoom bietet eine ähnliche UCaaS Dienstleistung wie Chime an, welche sich in ihrem Funktionsumfang jedoch vom Konkurrenten unterscheidet.

Edition	Basic	Plus	Pro
Calls & meetings			
1:1 Video calls	•	•	•
1:1 Voice calls	•	•	•
Outlook plugin	•	•	•
Screen sharing		•	•
Remote Desktop Control		•	•
Schedule and host meetings (attendees are always free)			•
Record meetings			•
Personalized meeting URLs			•
Conference room video systems			•
Join meetings using a standard phone line*			•
Maximum attendees	2	2	100
Chat			
1:1 Chat	•	•	•
Chat rooms	•	•	•
IT Administration			
User management		•	•
Active Directory integration		•	•
Message history	30 days	Up to 1GB/user	Up to 1GB/user

Abbildung 3: Amazon Chime Preismodell Quelle: Amazon Chime; Zugriff am 20.03.2017

Zoom Video Communications (im Folgenden „Zoom“ benannt) wurde von ehemaligen Ingenieuren des Cisco bzw. WebEx Entwicklungsteams gegründet. Eric S. Yuan, einer der Gründer und derzeitiger CEO von Zoom, war vorher bspw. „Vice President of Engineering“ beim jetzigen Konkurrenten WebEx. [7] Daher scheint es nicht verwunderlich, dass die gewonnene Expertise aus dem Bereich in das UCaaS Angebot von Zoom eingeflossen ist. Laut eigener Angaben nutzten im Jahr 2015 40 Millionen Einzelpersonen sowie 65.000 Unternehmen den Service Zoom. [8]

Zoom möchte, ähnlich wie Amazon Chime, eine konsistente Oberfläche und Bedienung über sämtliche Produktfunktionalitäten anbieten. Dazu bietet Zoom Applikationen für die Plattformen Windows, Mac, Linux, Chrome OS, iOS, Android und Black Berry an. H.323 bzw. SIP Raumsysteme können ebenfalls in Verbindung mit Zoom genutzt werden – dies kostet jedoch extra. Hier überrascht der Anbieter zwar durch eine große Plattformvielfalt – eine WebRTC Unterstützung im Browser suchen wir jedoch auch hier vergebens. Im Gegenteil: Hier enttäuscht Zoom sogar mehr als sein Konkurrent, da zwar eine Meeting-Einladung per URL versendet werden kann, die Webseite den Nutzer jedoch sofort zum Herunterladen der plattformspezifischen Zoom Applikation auffordert. Beim Praxistest stieß uns außerdem die Tatsache sauer auf, dass Zoom sich beim Öffnen der heruntergeladenen Windows Applikation ungefragt selbst installiert.

Neben der grundlegenden Video-/Audio-Conferencing Funktionalität (inkl. Chat) für bis zu 500 Teilnehmer, geht Zoom auch den nächsten Schritt und möchte sich als Webinar Plattform für Schulungen und Fernlehre etablieren. Zoom verspricht dabei Kapazitäten, um „bis zu 50 interaktive Teilnehmer [und] bis zu 10.000 Zuhörer“ in einem Webinar zu unterstützen. [9] Die Bereitstellung von technischem Support über Zoom soll ebenso möglich sein. Passend dazu erlaubt Zoom eine simultane Bildschirmfreigabe, jeweils inklusive der Möglichkeit zur Remote Steuerung und Bildschirmannotation, welche im Praxistest tadellos ihren Dienst verrichteten.

Weiterhin wirbt Zoom mit „softwarebasierte[r] Kollaboration für den Konferenzraum“: den sogenannten *Zoom Rooms* (siehe Abbildung 4). Diese sollen einen modernen, preisgünstigen Ersatz für herkömmliche Raumsysteme bieten und auf Basis verschiedener einzelner Hardwarekomponenten und einer passenden Software (Windows/Mac/iOs/Android) gemeinsam nutzbar sein.

Im Praxistest stechen insbesondere die über viele Jahre verbesserten und erprobten Detailfunktionalitäten ins Auge: Eine Gruppierungsmöglichkeit der Kontakte, Annotationsmöglichkeiten bei der Bildschirmfreigabe, Live-Broadcast Funktionalitäten zu Facebook oder YouTube, Moderationssteuerungen, Live Q&A Funktionalitäten, Untertitel, usw. . Trotz des relativ mächtigen Funktionsumfangs erschließt sich die Bedienung erfreulich schnell, da Benutzerfreundlichkeit und das erwähnte konsistente Bedienungsmuster konsequent verfolgt werden.

Zoom verschlüsselt die Kommunikation standardmäßig über TLS, gestützt

durch eine AES-256-Bit Punkt-zu-Punkt-Verschlüsselung – optional (nach expliziter Aktivierung) sogar über eine Ende-zu-Ende Verschlüsselung, die allerdings nicht auf einzelne User beschränkt werden kann. Zoom bietet außerdem eine rollenbasierte Zugriffssteuerung sowie eine individuelle Funktionssteuerung auf Administratorebene um den Funktionalitätsumfang gezielt einschränken zu können. Zur Anmeldung am Service stehen verschiedene Möglichkeiten zur Verfügung: SAML-basierte SSO Authentifizierung oder Direktregistrierung/-login über Google oder eine beliebige E-Mail Adresse.

Zoom fehlt ebenfalls ein essentielles Merkmal, das eine vollwertige UCaaS Lösung auszeichnet: Telefonie über SIP-Nebenstellen. Grundsätzlich ist nur die zentrale Erreichbarkeit über den Zoom Identifier gegeben – Teilnehmer können sich lediglich telefonisch in Meetings einwählen. Dabei werden Optionen zur nutzungsbasierten Bezahlung oder gegen pauschales monatliches Nutzungsentgelt angeboten. Zoom bietet weiterhin ein sogenanntes „Call Out“ Feature an, mit dem sich potentielle Teilnehmer anrufen und somit zu einem Meeting einladen lassen. Dies fällt jedoch ebenfalls unter das beschriebene, als „Premium Audio“ betitelte, Bezahlangebot, unter welches die Dial-In Option fällt. Ob dies als alltagstauglicher Ersatz für herkömmliche Telefonie herhalten kann erscheint fraglich.

Bezüglich einer Interoperabilität kann Zoom eine Integration in Lync bzw. Skype for Business vorweisen. Externe Teilnehmer sind ansonsten auch hier auf die Installation der entsprechenden Zoom Software für ihr jeweiliges Betriebssystem oder eine telefonische Einwahl angewiesen.

Im Vergleich zu Amazon Chime verfolgt Zoom ein etwas abgewandeltes Preismodell, das in Abbildung 5 dargestellt wird. Viele Funktionalitäten wie bspw. Webinare, Zoom Rooms oder die Anbindung von Raumsystemen erzeugen zusätzliche monatliche Kosten. In der „Basic“ Variante ihres Preismodells stehen dem potentiellen Kunden jedoch kostenfrei unlimitierte 1:1 Meetings sowie 40-minütige Gruppenmeetings mit bis zu 50 Teilnehmern zur freien Verfügung. Ab 15$ im Monat pro Moderator steht dann auch das Bereitstellen von Meetings ohne Zeitlimitierung zur Verfügung. SSO Integration folgt für 20$/Monat/Moderator. Die maximale Teilnehmergröße lässt sich über das von Zoom angebotene Preismodell flexibel erweitern und wird ggf. mit einem Preisaufschlag/-nachlass bedacht.

Interessanterweise brachten die bereits erwähnten AWS Probleme aus dem Februar 2017 [6] auch Zoom ins Straucheln: Diverse Zoom-Dienste nutzen die Cloud Computing Dienste von Amazon. [10] Die Frage der Verfügbarkeit muss also auch bei diesem Anbieter genauestens bedacht werden.

Abbildung 4: Komponenten eines Zoom Room Quelle: Zoom

Amazon Chime vs. Zoom

Beschränkt man sich im direkten Vergleich auf die elementaren UC Funktionalitäten für Teilnehmerzahlen im Bereich von kleinen und mittelständischen Unternehmen, so hebt sich keiner der Anbieter außerordentlich gegenüber dem anderen hervor. Die konkreten Anforderungen, die aus der jeweiligen Unternehmensstruktur resultieren, sowie individuelle Vorlieben spielen daher die maßgebliche Rolle bei der Auswahl eines solchen „UCaaS Lite“. Wenn Videokonferenzen mit mehr als 100 Teilnehmern oder gar Webinare notwendig sein sollten, spielt Amazon Chime beispielsweise bereits keine Rolle mehr.

Nutzt ihr Unternehmen bereits eigene Legacy-Raumsysteme, die in die UC Landschaft integriert werden sollen, so könnte hingegen Amazon Chime der passendere Kandidat für Sie sein, da Zoom einen Aufpreis für entsprechende cloud-basierte oder lokale H.323/SIP-Konnektoren ver-

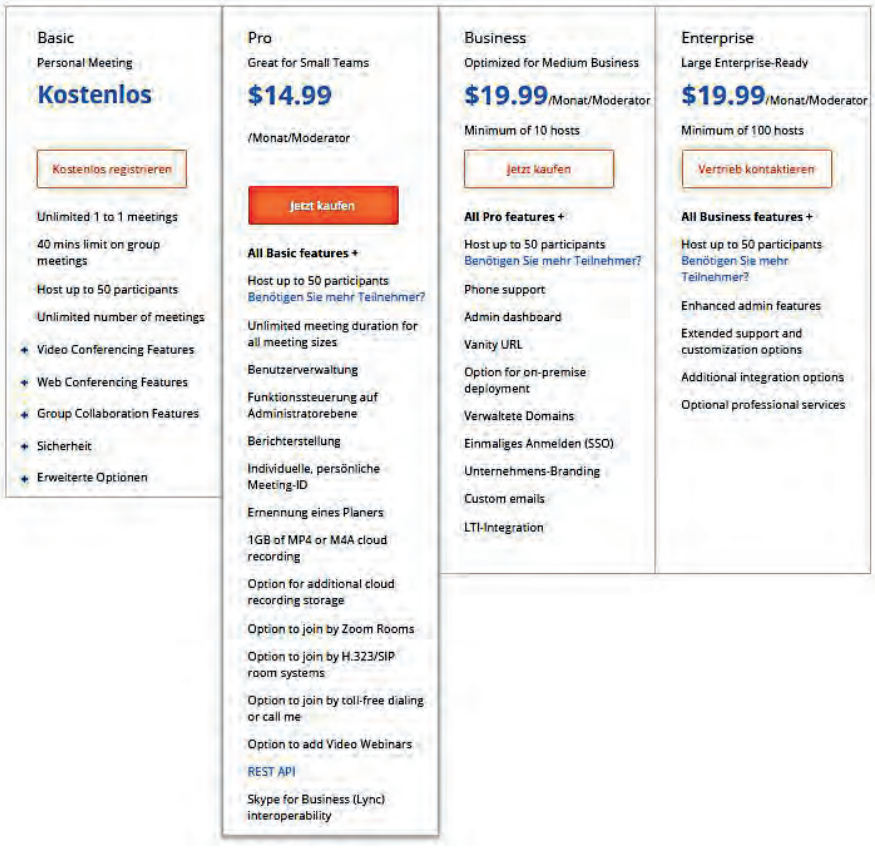


Abbildung 5: Zoom Preismodell Quelle: Zoom; Zugriff am 20.03.2017

langt. Möchten Sie auf eine klassische Erreichbarkeit über IP-Telefonie nicht verzichten, so sind Sie jedoch bei beiden Lösungen auf eine UC Umgebung im Sinne einer Hybrid Cloud angewiesen.

Beide Lösungen müssen hinsichtlich der Möglichkeiten zur Einbindung externer Teilnehmer abgestraft werden: Selbst rudimentärste Funktionalitäten wie die Audiokommunikation können bei beiden Anbietern nicht über den Browser durchgeführt werden. Die zwingend notwendige Installation einer proprietären Software zur Nutzung des vollständigen Funktionsumfangs, passt nicht in eine Zeit in der Standards wie WebRTC von über 60 % der Browsernutzer theoretisch ohne zusätzlichen Aufwand nutzbar wären. [11] Darüber können auch telefonische Einwahlmöglichkeiten in Meetings (die u.U. mit zusätzlich entstehenden Kosten für den Kunden verbunden sind) nicht hinwegtrösten.

Hinsichtlich der Video- bzw. Audioqualität der Übertragungen sowie der Sicherheitsmerkmale können beide Lösungen mit einem hohen Standard punkten. Aus Sicht des Funktionsumfangs und der Usability hat Zoom jedoch klar die Nase vorne. Hier spielt die über die Jahre angeeignete Expertise natürlich eine große Rolle. Entsprechend gut möchte der Anbieter für seine Leistungen bezahlt werden - Amazon Chime könnte dadurch ggf. die preiswertere Alternative darstellen.

On-Premises vs. Cloud-Service

Anhand dieses Einblicks in die Welt der UCaaS Lösungen lassen sich bereits einige Fallstricke der aktuellen UCaaS Welle erahnen. Um die Deployment Varianten gegeneinander abwägen zu können, bedarf es jedoch zunächst einem klaren Verständnis des Begriffes „UCaaS“ und dem funktionellen Abdeckungsgrad entsprechender Dienstleistungen. Der Begriff wird häufig in irreführender Weise auf Produkte angewendet, die nur teilweise oder gar nicht der eigentlichen UCaaS Definition entsprechen. An dieser Misere haben die Cloud Service Provider mindestens eine Teilschuld. Teilweise werden schier unüberschaubare Produktportfolios angeboten, bei deren Produktbeschreibungen mit Schlagwörtern wie „UCaaS“, die aus Marketing Perspektive attraktiv wirken, nicht gegeizt wird.

„Unified Communications as a Service“ beschreibt ein Auslieferungsmodell, bei dem eine Vielfalt von Kommunikations- oder Kollaborationsfunktionen bzw. -applikationen von einem Drittanbieter, im Sinne eines flexiblen und hochautomatisierten Managed Service, über ein IP-Netzwerk bereitgestellt werden (UCaaS fällt daher auch unter den Begriff „Software as a Service“, bzw. „SaaS“). In Abbildung 6 wird ein solcher Funktionsumfang beispielhaft dargestellt. Theoretisch sind der reinen Funktionsvielfalt von UCaaS Leistungen im Vergleich zu On-Premises Diensten daher keine Grenzen gesetzt, d.h. eine UC Lösung die über die Cloud angeboten wird, könnte in der Theorie dasselbe leisten wie eine UC Infrastruktur die in den eigenen Räumen bereitgestellt wird. In diesem Artikel beschränken wir uns bei der Betrachtung jedoch auf die Multi-Tenancy Bereitstellung der UCaaS Leistung: Mehrere Kunden teilen sich eine Software-Plattform und damit einhergehend die entsprechenden Hardware-Ressourcen.

Charakteristika, die eine Cloud-Leistung von einer On-Premises Lösung abgrenzen, sind bspw. zentralisiertes Management, Automatisierung, Virtualisierung sowie Standardisierung (z.B. bezügl. Schnittstellen). In dieser Hinsicht schmerzt der Verlust eines IT-Mitarbeiters bei Nutzung einer On-Premises Lösung oft mehr als ein Wechsel des Cloud-Service Providers, da die gewonnene Expertise und eigenwillige Konfigurationen des Systems mit dem Weggang des Mitarbeiters verloren gehen. Eine Cloud-Leistung zeichnet sich außerdem durch ein OPEX Preismodell aus, wohingegen das CAPEX Preismodell einer On-Premises Lösung anfangs erhöhte Investitionskosten verursacht.

Die steigende Beliebtheit von Cloud-Services kommt nicht von ungefähr: In punkto Verfügbarkeit, Sicherheit und Performanz hatten On-Premises Lösungen bis vor einigen Jahren deutlich die Nase vorne. Durch den Breitbandausbau, die steigende Zuverlässigkeit von Cloud Computing Diensten und die gewonnene Erfahrung der Cloud Dienstleister müssen sich Cloud Provider mittlerweile nicht mehr vor ihren On-Premises Konkurrenten verstecken. Insbesondere bei der Skalierbarkeit können UCaaS Leistungen mit ihrer Flexibilität glänzen: Ändern sich Unternehmensstrukturen, -anforderungen oder -größe, so können UCaaS Lösungen meist schnell und unkompliziert durch Zu-/Abbuchen von Leistungen dynamisch reagieren. Im Falle von On-Premises Lösungen würde dies meist umständliche und ggf. kostspielige Hardwareänderungen nach sich ziehen. Am Beispiel von Zoom sieht man anschaulich, wie sich die Meeting-Teilnehmergröße flexibel erweitern bzw. verringern ließe – Umstellungen, die bei On-Premises UC Diensten meist wochenlange Planungs- und Umsetzungsphasen nach sich ziehen würden.

Doch was, wenn im Unternehmen bereits eine UC Infrastruktur existiert und lediglich ausgewählte Funktionalitäten hinzugefügt werden sollen? Hybride Mischlösungen können zwar Abhilfe schaffen, führen aber in den meisten Fällen zu inkonsistenten Benutzererfahrungen im Umgang mit den unterschiedlichen Kommunikationsdiensten. Bei den hier betrachteten Lösungen Zoom und Amazon Chime, spielt dieser Punkt jedoch nur eine untergeordnete Rolle. Eine Anbindung an das PSTN über eine On-Premises IP-PBX, in Ergänzung zu den multimedialen Kommunikationsmöglichkeiten der UC Dienste, erscheint hier als eine durchaus denkbare Option, auch wenn

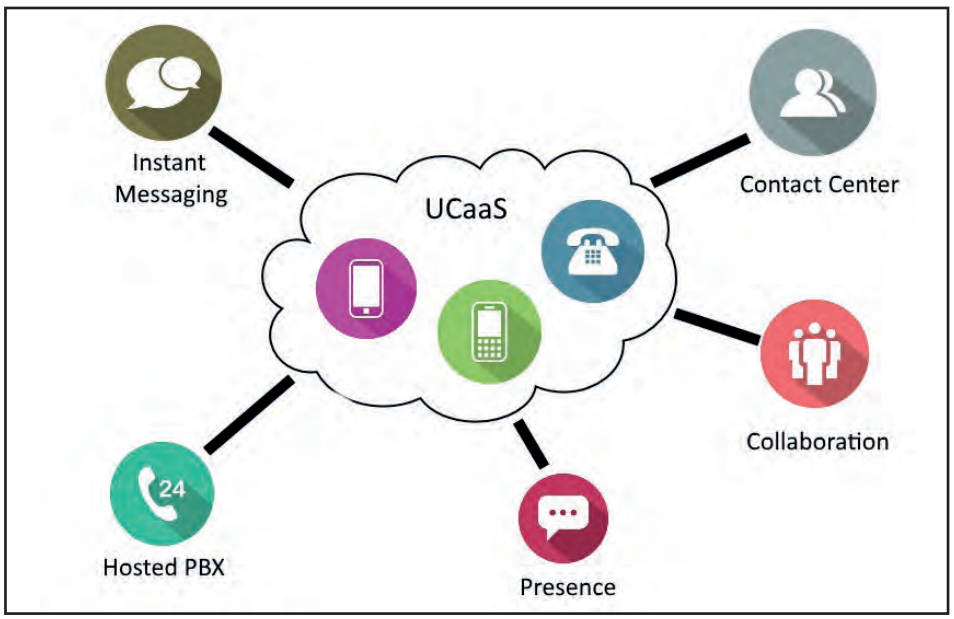


Abbildung 6: Beispiel eines UCaaS Funktionsumfangs

beide Anbieter dies heute (noch?) nicht unterstützen. Andere Anbieter wie z.B. Mitel, Unify, Microsoft oder Cisco ermöglichen dies bereits. Ohne vorhandene Infrastruktur können andere UCaaS Anbieter, wie z.B. die eben genannten, alternativ mit einer Cloud-PBX Lösung aushelfen. Grundsätzlich ist aber eine Langzeitmigration auf UCaaS Lösungen bei Unternehmen, die bisher stark auf On-Premises Lösungen setzen, eher fraglich. Angeschaffte Infrastrukturen und aufgebaute Expertise werden eher widerwillig aufgegeben, so dass eine UCaaS Lösung meist nicht einmal in Betracht gezogen wird. Gerne wird dabei ganz allgemein mit Datenschutz und IT-Sicherheit argumentiert. Bitte verstehen Sie uns nicht falsch: Datenschutz und Informationssicherheit sind zwei der wichtigsten Faktoren bei einer Entscheidung für oder gegen die Cloud. Legitim ist eine solche Argumentation allerdings nur, wenn sie sich auf faktischen Sicherheitsvorteilen einer On-Premises-Installation begründet und nicht auf einem „Bauchgefühl“. Das höhere Maß an Kontrolle, welches eine On-Premises UC Lösung ermöglicht, kann aus Gründen der IT-Compliance durchaus die attraktivere Wahl darstellen. Dies bedingt jedoch die ausführliche Auseinandersetzung mit den jeweiligen Richtlinien und die regelmäßige Überwachung von deren Einhaltung.

Die Datenhoheit bzw. die Kontrolle über den Datenschutz ist – je nach dem Grad der Vertraulichkeit der übermittelten Informationen – dennoch einer der größten Hinderungsgründe, die Unternehmen derzeit vom Komplettumstieg auf eine UCaaS Leistung abhalten. Möchte man trotzdem auf eine Cloud- Variante umsteigen, so empfiehlt sich ein Blick auf den Standort der jeweiligen Server, auf denen die Daten gelagert werden, und die im entsprechenden Land geltenden Datenschutzstandards. Hier gilt weiterhin die Faustregel: Europa besitzt deutlich strengere Datenschutzregelungen als transatlantische Cloud-Angebote. Das gilt insbesondere seitdem sich die EU-Datenschutzgrundverordnung materialisiert. Die Wahrheit ist natürlich viel komplizierter, doch in die Tiefen der Datenschutzgesetzgebung wollen wir uns an dieser Stelle nicht begeben.

Hinsichtlich einer ggf. erforderlichen oder gewünschten Redundanz können UCaaS Lösungen hingegen attraktiv sein, da die Cloud Service Provider diese standardmäßig implementieren. Wichtig ist, dass man dem jeweiligen Dienstleister ein hohes Vertrauen hinsichtlich der Einhaltung und qualitativen Umsetzung entsprechender Maßnahmen entgegen bringen muss. Dieses Vertrauen muss durch Zertifizierungen, aber auch den proaktiven Nachweis der Sicherheit und durch turnusmäßige Auditierungen durch den Cloud Service Provider aufgebaut werden. Darüber hinaus ist ein Monitoring von Sicherheits-, Performance- und Qualitätskenndaten durch den Kunden eine wesentliche Voraussetzung für eine geeignete Cloud-Lösung. All dies gilt für Zoom und Chime (noch) nicht, wobei wenigstens die Chime-Basis AWS über eine ISO-27001-Zertifizierung verfügt.

Apropos AWS: Das Thema Redundanz spielt insbesondere in Hinblick auf Disaster Recovery und Dienstverfügbarkeit eine tragende Rolle. Das Risiko, unverhofft ohne Kommunikationsmöglichkeiten dazustehen, kann im Einzelfall sogar durch Cloud-Services erheblich gemindert werden. Dies ist der Fall, wenn ein Unternehmen aus eigener Kraft keine zeitgemäßen Verfügbarkeitswerte für die selbst produzierten IT-Services realisieren kann. Entgegen der landläufigen Meinung ist dies nicht nur bei IT-fernen oder sehr kleinen Unternehmen der Fall, sondern auch in Großunternehmen mit einer starken IT immer noch an der Tagesordnung. Hochverfügbarkeit im Sinne einer 99,99 prozentigen Verfügbarkeit im Jahresmittel ist in der Cloud im Allgemeinen zwar nicht zu realisieren; die meisten Anbieter sichern eine Verfügbarkeit des Dienstes (bezogen auf den Netzübergang des Cloud-Rechenzentrums) von 99,9% oder maximal 99,95% vertraglich zu. Die normalen Anforderungen an Standard-IT-Services erfüllt dies jedoch allemal. Die, im Cloud Computing Bereich übliche, verteilte Serverstruktur ist auf solche Verfügbarkeitsanforderungen in der Regel optimal vorbereitet. Auf der anderen Seite übergibt man die Kontrolle über den Wiederanlauf auch hier vollständig in die Hände des Cloud Service Providers. Dies kann ggf. zu fatalen Ausfällen führen, was die eingangs erwähnten AWS Probleme noch einmal deutlich vor Augen geführt haben. So gewinnt man kein nachhaltiges Vertrauen in die Leistungsfähigkeit und Verlässlichkeit von Cloud Services.

Fazit

Aktuellen Prognosen [12] zufolge, ist der Kampf um die Gunst des Kunden im UC Sektor auch in den kommenden Jahren nicht zu bremsen. Als primäre Treiber des Trends werden die verstärkte Nutzung von mobilen Geräten wie Smartphones und Tablets, die zunehmende Nutzung von privaten Endgeräten sowie das bedarfsgerechte Abrechnungsmodell genannt. Um den Anschluss nicht zu verlieren, entscheiden sich viele etablierte UC Anbieter wie Cisco, Avaya und Microsoft, parallel zur klassischen On-Premises Deployment-Variante, ebenfalls für die Bereitstellung von Public und Private-Cloud UC Lösung.

Welche Bereitstellungsvariante derzeit am besten zu Ihrem Unternehmen passt, hängt weiterhin von den jeweiligen Rahmenbedingungen, Geschäftsanforderungen und dem vorhandenen Budget ab. Sicher ist jedoch: Der Cloud-Trend ist unumkehrbar. IT-Abteilungen müssen sich heutzutage mit der Wirtschaftlichkeit, Agilität und Flexibilität messen lassen, die Nutzer von Cloud-Anwendungen gewöhnt sind. Schlechtere Rahmenbedingungen bei der Nutzung unternehmenseigener IT werden nicht mehr hingenommen; Missstände werden angeprangert. Es entwickelt sich schnell Unverständnis, wenn die hausinterne IT-Abteilung für die Bereitstellung und Einrichtung einer Applikation mehrere Wochen braucht, wenn dem gegenüber Cloud-Dienste wie bspw. Skype, Spark, Chime, Zoom & Co. stehen, mit denen innerhalb weniger Minuten eine VoIP Konferenz mit beliebigen weltweit verteilten Personen aufgebaut werden kann.

Wirft man einen Blick in die Zukunft, so lässt sich die These formulieren, dass UCaaS-Angebote disruptiv auf den UC-Markt wirken und damit das Geschäft der Telefonie- und UC-Anbieter vollständig in die Nische verdrängen werden. Das Potenzial dazu ist bereits vorhanden, auch wenn Lösungen wie Chime und Zoom dieses Versprechen noch nicht einlösen. Fraglich ist jedoch, wann die breite Masse der Unternehmen bereit sein wird, den Weg in diese Richtung einzuschlagen. Vor dem Hintergrund der bevorstehenden Inkraftsetzung der EU-Datenschutzgrundverordnung (EU-DSGVO) in 2018 wird es außerdem spannend sein zu beobachten, wie die Service Provider sich an die neuen Bedingungen anpassen und entsprechende Änderungen an ihren Angeboten vornehmen werden. U.U. werden dadurch Sicherheitsbedenken ausgeräumt, die die Kunden bisher von einem Umstieg auf eine UCaaS Lösung abhielten.

Letztlich profitieren die Kunden vom derzeit herrschenden Wettkampf um Funktionsvielfalt und niedrige Preise. Die Zeit wird zeigen, wie sich die Anforderungen an Kommunikationslösungen weiterentwickeln und wie die Cloud Service Provider darauf reagieren werden. Bis dahin wird man um eine unternehmensindividuelle Einschätzung hinsichtlich der optimalen Kommunikationslösung nicht umhin kommen.

Abkürzungen

AD FS	Active Directory Federation Services
AES	Advanced Encryption Standard
AWS	Amazon Web Services
CAGR	Compund Annual Growth Rate
CAPEX	Capital Expenditures
EaaS	Everything as a Service
HTML	HyperText Markup Language
OPEX	Operational Expenditures
PBX	Private Branch Exchange
PSTN	Public Switched Telephone Network
SAML	Security Assertion Markup Language
SIP	Session Initiation Protocol
SSO	Single Sign-on
TCO	Total Cost of Ownership
UCaaS	Unified Communications as a Service
VoIP	Voice over Internet Protocol
WebRTC	Web Real-Time Communication

Verweise

[1] https://aws.amazon.com/de/about-aws/whats-new/2017/02/announcing-amazon-chime-frustration-free-online-meetings-with-exceptional-audio-and-video-quality/; Zugriff am 20.03.2017

[2] http://www.networkworld.com/article/3169618/cloud-computing/amazon-releases-chime-a-new-cloud-based-ucaas.html; Zugriff am 20.03.2017

[3] https://chime.aws/features/; Zugriff am 20.03.2017

[4] https://www.chriskranky.com/amazon-chime-webrtc/; Zugriff am 20.03.2017

[5] https://chime.aws/dialinrates/; Zugriff am 20.03.2017

[6] https://www.heise.de/newsticker/meldung/Stoerung-bei-Amazons-Web-Service-behindert-viele-Websites-3639678.html; Zugriff am 20.03.2017

[7] http://www.businessinsider.de/zoom-ceo-eric-yuan-interview-2017-1?r=US&IR=T; Zugriff am 20.03.2017

[8] http://www.marketwired.com/press-release/zoom-raises-30m-in-series-c-funding-led-by-emergence-capital-1988574.htm; Zugriff am 20.03.2017

[9] https://zoom.us/webinar; Zugriff am 20.03.2017

[10] http://status.zoom.us/; Zugriff am 20.03.2017

[11] http://gs.statcounter.com/; Zugriff am 20.03.2017

[12] http://blog.tmcnet.com/on-rads-radar/2016/12/ucaas-growth-forecasts.html; Zugriff am 20.03.2017

Aktuelles Seminar

Betriebsvereinbarungen und Mitarbeiterdatenschutz bei IT- und TK-Systemen

19.06. - 20.06.2017 in Bonn

Die ComConsult Akademie veranstaltet vom 19.06. bis 20.06.2017 ihr Seminar "Betriebsvereinbarungen und Mitarbeiterdatenschutz bei IT- und TK-Systemen" in Bonn mit Rechtsanwalt Ulrich Emmert.

Jede Maßnahme, die auch zur Mitarbeiterüberwachung genutzt werden könnte, und jede Einführung neuer IT- oder TK-Systeme unterliegt der vollen Mitbestimmung des Betriebs- oder Personalrats nach dem Betriebsverfassungsgesetz bzw. den Personalvertretungsgesetzen. Neben den rechtlichen Grundlagen vermittelt das Seminar auch Strategien, wie konstruktiv mit der Arbeitnehmervertretung im Bereich Datenverarbeitung und Mitarbeiterüberwachung zusammengearbeitet werden kann.

- Übersicht Betriebsverfassungsrecht
- Grenzen der Mitarbeiterüberwachung
- Überwachung vs. Sicherheit bei Computern des Betriebsrates
- Datenübertragung in die USA nach dem EU-US-Privacy Shield
- Standortbestimmung von Mitarbeitern
- Private Nutzung von IT und TK
- Zugriff auf Mailpostfächer
- Mithören und Aufzeichnen von Telefonaten
- Überwachung bei Einsatz von Datenverschlüsselung
- Weitergabe von Verbindungsdaten von Mitarbeitern
- Videoüberwachung

- Mitschneiden von Bildschirminhalten
- Verwendung von Fotos
- Verwendung von Biometrie
- Trennung privater Daten und geschäftlicher Daten
- Regeln für geschäftliche und private Nutzung bei Instant-Messaging-Diensten und sozialen Netzwerken
- Anforderungen an Einwilligungserklärungen
- Änderungen durch die neue EU-Datenschutzverordnung
- Besonderheiten beim Europäischen Betriebsrat einer SE
- Zusammenarbeit bei der Einführung neuer IT- und TK-Systeme
- Zusammenarbeit zwischen Betriebsrat / Personalrat und Datenschutzbeauftragtem
- Anforderungen an Ausbildung und Schulung von Mitarbeitern
- Anforderungen Führungszeugnis/ Sicherheitsüberprüfungsgesetz
- Sonderregelungen für Parteien und Religionsgemeinschaften
- Nutzung von Internet und E-Mail
- Nutzung von Funknetzen
- Regeln für Home Office Arbeitsplätze
- Regeln für Fernwartungszugriffe
- Einführung von VoIP Telefonanlagen oder CTI-Systemen
- Einführung von Dokumentenmanagementsystemen
- Einführung von Mail- und Dokumentenarchivierungssystemen
- Einführung von Secure File Sharing
- Einführung von Bring your Own Device
- Einführung von Mobile Device Management

Das Seminar richtet sich an Mitglieder der Geschäftsleitung, IT-Verantwortliche, Betriebs- oder Personalräte, Datenschutzbeauftragte von Behörden und Unternehmen, kaufmännische Leiter, Leiter der Revision, Systemadministratoren, die sich über Fragen des Beschäftigtendatenschutzes und der Mitbestimmung, insbesondere bei Unternehmensrichtlinien im Bereich der IT-Nutzung und der IT-Sicherheit sowie bei der Einführung neuer IT- und TK-Systeme informieren möchten.

Anmeldung an kundenservice@comonsult-research.de

Betriebsvereinbarungen und Mitarbeiterdatenschutz bei IT- und TK-Systemen

Ich buche das Seminar
Betriebsvereinbarungen und Mitarbeiterdatenschutz bei IT- und TK-Systemen

☐ 19.06. - 20.06.2017 in Bonn
zum Preis von € 1.590,-- netto

☐ Bitte buchen Sie mir ein Hotelzimmer

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

Vorname	Nachname
Firma	Telefon/Fax
Straße	PLZ,Ort
eMail	Unterschrift

Standpunkt

Ist Windows für Produktions-umgebungen geeignet?

Der Standpunkt von Dr. Joachim Wetzlar greift als regelmäßiger Bestandteil des ComConsult Netzwerk Insiders technologische Argumente auf, die Sie so schnell nicht in den öffentlichen Medien finden und korreliert sie mit allgemeinen Trends.

So ein Unsinn, was soll diese Frage? Selbstverständlich ist es das. Windows findet sich fast überall und also auch in Systemen der industriellen Produktion, zur Prozessvisualisierung, zum Messen, Steuern und Regeln, usw. So rüstet z.B. ein bekannter Deutscher Hersteller von Hochfrequenzmesstechnik seine Produkte mit Windows aus, oft in einer „Embedded Version“. Interessanterweise setzt ausgerechnet ein amerikanischer Hersteller solcher Geräte auf LINUX, aber das nur am Rande. Mir geht es um etwas anderes.

Eine typische Aufgabe des Betriebssystems ist bekanntlich das Bereitstellen wohldefinierter Schnittstellen für die Peripherie eines Rechners. Der Programmierer einer Anwendung soll Ein-/Ausgabefunktionen ohne genaue Kenntnis der Rechner-Hardware verwenden können. Moderne Betriebssysteme besitzen derlei „abstrakte“ Schnittstellen für alle denkbare Peripherie. Ein Peripheriehersteller liefert mit seiner Schnittstellen-Hardware gleich den passenden Treiber mit, insbesondere für Windows.

Ein gutes Beispiel dafür ist WLAN. Die große Verbreitung von Laptops mit diesem Betriebssystem hat im Laufe der Jahre eine betriebssichere WLAN-Unterstützung entstehen lassen. Warum soll man das nicht auch für mobile Anwendung in Fertigung und Logistik nutzen?

Doch hier offenbart die Praxis immer wieder Fallstricke. Ein Laptop steht eben meist am selbem Ort, z.B. am Arbeitsplatz oder im Besprechungsraum. Das Roaming-Verhalten im WLAN ist für diesen Anwendungsfall optimiert. So hat der Programmierer des WLAN-Treibers in meinem Laptop als Auswahlkriterium für einen Access Point (AP) dessen „Modernität“ bestimmt. Der Laptop assoziiert sich eher an einem entfernten Access Point mit Unterstützung für IEEE 802.11ac, selbst wenn in Sichtweite ein AP hängt, wenn dieser nur 11n unterstützt.

Für eine mobile Anwendung ist solches Verhalten möglicherweise fatal. Die Zellenplanung in einer Halle geht nur dann auf, wenn Endgeräte sich am nächstgelegenen AP anmelden. Oft finden sich aber gerade in solchen Umgebungen APs aus unterschiedlichen Epochen. Mein Laptop würde dann zum „sticky client“, er klebte also quasi an bestimmten APs und reduzierte seine Bitrate mit steigendem Abstand. Dadurch verbrauchte er mehr Zeit für das Senden von Daten, wodurch andere Clients ausgebremst würden.

Grundsätzlich lässt sich das Roaming-Verhalten von WLAN-Adaptern parametrieren. Allerdings muss man mit den Möglichkeiten vorliebnehmen, die einem die Adapter-Hersteller in den Treibern anbieten. Dort findet man beispielsweise „Roaming Dynamik“ in fünf Stufen. Was bedeutet das? Wir haben in Tests festgestellt, dass letztlich ein Schwellwert für die Signalstärke verändert wird, unterhalb dessen der Adapter beginnt, sich einen neuen AP zu suchen. Wie er das letztlich macht, bleibt im Dunkeln. Und andere Hersteller wählen wieder andere Konzepte und Begriffe.

Wenn man schon Windows einsetzt, bietet es sich an, auch dessen ausgefeilte Sicherheitsfunktionen zu nutzen. Die Einbindung in ein Microsoft Active Directory ermöglicht das Verteilen von Zertifikaten (z.B. per „Autoenrollment“) und damit die Nutzung starker Authentisierung am WLAN. Es liegt daher nahe, Windows-Standard-Clients auch in Fertigung und Logistik einzusetzen. Das will jedoch wohlüberlegt sein. Denn auf einmal werden Sie von einer Infrastruktur abhängig, die außerhalb des Verantwortungsbereichs der Produktions-IT liegt. Mehr noch, die sichere Authentisierung verlängert die Zeiten für ein Handover. Und auf derlei Standard-Clients installierte Virenscanner können unerwünschte Seiteneffekte auf „Echtzeit“-Anwendungen haben.

Überlegen Sie also gut, welche Systeme Sie in Nicht-Büroumgebungen einsetzen möchten. Manchmal ist ein LINUX von Vorteil, bei dem der Entwickler den WLAN-Treiber optimiert hat. Grundsätzlich geeignet sind auch WLAN Bridges, mit denen man Ethernet-basierte Steuerungs-Rechner an WLAN anbindet. In Controller-basierten WLAN sind dann zwar einige Besonderheiten zu beachten, jedoch lassen sich derlei Bridges oft besser parametrieren als der Standard-Windows-WLAN-Treiber. Und ob es in diesem Umfeld wirklich die Active-Directory-Integration sein soll, ist aus meiner Sicht genau abzuwägen.

Sonderveranstaltung

Das PSTN stirbt: Die neue Kommunikation mit SIP/IP 22.06.2017 in Bonn

Die ComConsult Akademie veranstaltet am 22.06.2017 ihre Sonderveranstaltung "Das PSTN stirbt: Die neue Kommunikation mit SIP/IP" in Bonn.

Die Deutsche Telekom hat angekündigt, bis 2018 das klassische PSTN-Netz, respektive analoge und ISDN-Anschlüsse abzuschalten. Dies betrifft alle Unternehmen, die weltweit kommunizieren wollen und müssen. Diese Sonderveranstaltung analysiert, wie der Wechsel von PSTN auf All-IP im Unternehmen verläuft. Sie zeigt auf, welche Funktionalität heute erreicht werden kann und mit welchem Aufwand für Anpassung und Fehlersuche zu rechnen ist.

Abgesehen von den rein technischen Unterschieden: bei Leitungsvermittlung vs. Paketvermittlung, E.164 Telefonnummer vs. URI gibt es erhebliche funktionale Unterschiede, denn das Dienstspektrum bei All-IP wird erheblich umfangreicher sein als es im PSTN jemals der Fall war.

Soll sich eine globale SIP / All-IP Kommunikation auf breiter Ebene etablieren, muss dies auf der Basis von genormten oder de facto Standards erfolgen. Hierfür gibt es sowohl bei ECMA als auch dem SIP Forum Ansätze. Welcher hat das größte Marktpotenzial? Gibt es Zertifizierungsmöglichkeiten? Wie sieht die aktuelle Praxis aus?

Die Perimeter-Anschaltung des SIP/All-IP Trunks zwischen Enterprise und Provider wird heute typischerweise mit einem SBC realisiert. Wir analysieren, wie die Anschaltung aussieht, welche Funktionalität von einer solchen Komponente erwartet werden sollte und wie sich der SBC-Markt präsentiert.

Im Rahmen der Veranstaltung analysieren wir, wie der Wechsel von PSTN auf All-IP im Unternehmen verläuft. Wir zeigen auf, welche Funktionalität heute erreicht werden kann und mit welchem Aufwand für Anpassung und Fehlersuche zu rechnen ist. Wie gut ist die Unterstützung durch den Enterprise-Hersteller und Provider? Wie ändert sich Betriebs- und Kostenaufwand?

Nicht nur klassische PSTN-Provider werden diesen Markt unter sich aufteilen, sondern auch Kabelnetzbetreiber, Mobilfunkanbieter und ISPs werden ihr Dienstspektrum auf den All-IP Kommunikationsmarkt ausdehnen. Wir analysieren, wie das aktuelle Angebotsspektrum aussieht und welche Roadmap erkennbar ist.

Für die Provider ist All-IP kein Neuland, aber dennoch ein Technologiewechsel mit großen Herausforderungen. Wir diskutieren, welche Anforderungen ein Provider an den Enterprise-Kunden stellt, wie SLAs gestaltet werden können, wie ein typischer Projektablauf aussieht und mit welchen Problemen zu rechnen ist.

Der Ersatz von E.164 durch All-IP muss zu einer neuen globalen Kommunikations-Architektur führen. Stand heute gibt es kein einheitliches, standardisiertes SIP-Interconnect zum Provider-Peering oder als Meta-Ebene. Wir zeigen die aktuellen Standardisierungs-Vorschläge, Möglichkeiten und Trends auf, über die die Provider diskutieren.

Das Seminar richtet sich an die Verantwortlichen, Entscheidungsträger, Planer und Betreiber von IP-Netzwerken, TK-Anlagen und Call Centern, die sich über die zukünftige, optimale und erfolgreiche Anbindung bestehender klassischer oder IP-basierter TK-Lösungen an das öffentliche Kommunikationsnetz informieren wollen.

Anmeldung an kundenservice@comonsult-research.de

Das PSTN stirbt: Die neue Kommunikation mit SIP/IP

Ich buche die Sonderveranstaltung
Das PSTN stirbt:
Die neue Kommunikation mit SIP/IP

☐ 22.06.2017 in Bonn
zum Preis von € 1.090,-- netto

☐ Bitte buchen Sie mir ein Hotelzimmer

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

_____ Vorname	_____ Nachname
_____ Firma	_____ Telefon/Fax
_____ Straße	_____ PLZ,Ort
_____ eMail	_____ Unterschrift

Programmübersicht - Das PSTN stirbt: Die neue Kommunikation mit SIP/IP

Beginn der Veranstaltung 9:30 Uhr

Einführung: Warum wird ein Einstieg in All IP unvermeidlich und welche Änderungen sind damit verbunden?
- Die weltweite Abschaltung der öffentlichen PSTN-Netze ist angekündigt
- Bisheriges Design einer VoIP-Enterprise-Lösung
- Zukünftiges Design einer VoIP-Enterprise-Lösung
- Die „VoIP"-Welt wird auf UC erweitert werden
- Welche Probleme müssen in der neuen All-IP Welt gelöst werden?
- All-IP und IPv6?

SIP vs. PSTN. Was ist anders?
- Leitungsvermittlung vs. Paketvermittlung
- Überbuchungssituation, CAC
- Comfort Noise: Woran erkenne ich eine freie Leitung?
- Die Abhängigkeit der Sprachqualität von Zeitinformationen und deren Herkunft
- Über welche Datenleitung kommuniziere ich?

SIP Trunking Standards für Enterprise-Kunden
- Welche Standards gibt es?
- Wo steht SIPconnect?
- Wo stehen die Provider und die UC Hersteller?

Der SBC Markt
- Funktionsweise eines SBC
- Welche Leistungsmerkmale sollte ein SBC haben?
- Herstellerübersicht der führenden Anbieter

Der Provider Markt
- Wo stehen Telekom und Co?
- Wie sieht die technische Umsetzung aus?
- Welche Leistungsmerkmale kann man erwarten?
- Anschluss- und Verrechnungsmodelle

Provider Vortrag
- Welche Leistungsmerkmale gibt es jetzt und welche kommen?
- Anschlussmodell: direkter Anlagenanschluss oder SBC
- Wie lange dauert die Inbetriebnahme?
- Wie wird abgerechnet?
- Skalierbarkeit
- Verfügbarkeit
- Projekt Beispiele

Anwendervortrag: Der Wechsel von PSTN auf SIP Trunking bei einer großen Krankenkasse
- Die Private Telefonie Cloud der TK
- Was steckt in der Private Cloud drin?
- Herausforderungen bei der Implementierung
- Entwicklungsstrategie All over IP
- Fazit

Der Weg zu All IP
- Was fehlt für die globale SIP/IP Kommunikation?
- Welche Lösungsansätze gibt es?
- Wo liegen die Probleme?

Ende der Veranstaltung 17:30 Uhr

Der Veranstalter behält sich Änderungen im Programm vor

Diese Referenten führen Sie durch den Tag

Markus Emde ist Berater und Projektmanager bei der ComConsult Beratung und Planung GmbH im Competence-Center „Kommunikationslösungen". Zu seinen Arbeits-Schwerpunkten zählt die Konzeption, Ausschreibung und Umsetzungsbegleitung von VoIP und Unified Communication & Collaboration Lösungen.

Dipl.-Ing. **Wilfried Meer** hat über 30 Jahren Berufserfahrung in den Bereichen Elektronik, IT und Telekommunikation. Als TC Marketing Consultant bei T-Systems verantwortet er u.a. die Kommunikation und Konzeption von Voice-/Data-Migrationsszenarien im Enterprise-Segment

Dipl.-Ing. **Rolf Nagelfeld** ist Fachreferatsleiter bei der Techniker Krankenkasse in Hamburg. Er blickt auf 30 Jahre Berufserfahrung im Bereich Netzwerk, Telekommunikation und Systems Management zurück, davon rund 25 Jahre in leitender Position.

Seit über 10 Jahren ist **Markus Geller** bei der ComConsult Research GmbH erster Ansprechpartner für die Themen VoIP und Lokale Netze. Der Schwerpunkt seiner Trainer Tätigkeit liegt dabei auf den Gebieten SIP, PSTN Migration, WebRTC sowie Layer 2 und 3 Techniken für MAN und LAN. Markus Geller verfügt über eine langjährige Erfahrung beim Aufbau und der Planung von Netzwerken im large Enterprise Umfeld, inkl. RZ-Netzwerken, WLAN und Multicastverfahren.

In seiner über 20-jährigen IT-Laufbahn beschäftigt er sich mit der Evaluierung neuer Technologien und deren Einsatz in der Praxis. Zudem ist er als Autor diverser Fachartikel für den ComConsult Netzwerk Insider und das Wissensportal tätig.

Zweitthema

Abwehr zielgerichteter Angriffe - die Paradedisziplin der Informationssicherheit

Fortsetzung von Seite 1

Dr. Hoff ist technischer Direktor der ComConsult Beratung und Planung GmbH und blickt auf jahrelange Projekterfahrung in Forschung, Standardisierung, Entwicklung, Planung und Betrieb in den Bereichen IT-Sicherheit, lokale Netze und mobile Kommunikationssysteme zurück.

Dipl.-Math. Simon Oberem ist als Berater bei der ComConsult Beratung und Planung GmbH in dem Bereich IT-Sicherheit tätig. Im Projektgeschäft befasst er sich maßgeblich mit den Aspekten von ISMS nach ISO 27001, auch auf Basis BSI-Grundschutz sowie deren praxistauglicher Umsetzung.

Es wäre nun fatal zu denken, man selber könnte nie Ziel eines solchen Angriffs werden. Eine typische Frage ist hier: „Was könnte ein Angreifer bei mir schon holen?“. Eine Antwort kann z.B. einfach sein: Identitäten. Es hat schon APTs gegeben, die zunächst eine Institution angegriffen und kompromittiert haben, um das eigentliche Angriffsziel durch E-Mails, die nachvollziehbar von einer vertrauenswürdigen Quelle (nämlich der zunächst angegriffenen Institution) stammen, leichter angreifen zu können. Als Beispiel kann hier ein Angriff auf das Weiße Haus in den USA im Jahr 2015 [1] genannt werden. Hier hatte der Angreifer zunächst das Außenministerium gehackt, um dann von dort aus am Weißen Haus mit bösartigen Phishing Mails anzugreifen [2].

Außerdem gibt es einen weiteren gefährlichen Trend. Wie dem Lagebericht des BSI 2016 zu entnehmen ist, „findet ein Technologietransfer aus dem Bereich der Advanced Persistent Threats (APT) hin zu den allgemeinen Schadprogrammen statt“ [3]. Dieser Technologietransfer hat sich z.B. im Bereich der Kryptotrojaner schon deutlich gezeigt.

Um Abwehrstrategien gegen APTs entwickeln zu können, ist es entscheidend die Vorgehensweise und den Werkzeugkasten der Angreifer zu verstehen („Know your enemy!“) und die eigene IT mit den Augen eines potentiellen Angreifers zu sehen.

.1. Was genau ist ein zielgerichteter Angriff?

Ein zielgerichteter Angriff hat ein fest umrissenes Angriffsziel, läuft typischerweise in mehreren Phasen ab und kombiniert unterschiedliche, aufeinander aufbauende Angriffstechniken. Der englische Begriff APT beschreibt die Charakteristiken sehr treffend:

- **Advanced:** Der Angreifer hat Know-how und nutzt fortgeschrittene Techniken. Das heißt natürlich nicht, dass der Angreifer nicht auch auf frei verfügbare Werkzeuge zurückgreift.

- **Persistent:** Ein APT kann sich über einen längeren Zeitraum hinziehen und der Angreifer arbeitet sich ausdauernd zum Angriffsziel vor und wartet auch geduldig auf sich bietende Angriffsgelegenheiten. Je nach Angriffsziel kann der Angreifer zum Dauergast in der angegriffenen Infrastruktur werden.

- **Threat:** Der Angreifer nutzt systematisch Schwachstellen aus, die er in der angegriffenen Infrastruktur vorfindet. Im Extremfall werden auch sogenannte Day Zero Exploits eingesetzt, d.h. bisher unbekannte Ausnutzungen von (ggf. bis dato unbekannten) Schwachstellen, die die Organisation des Angreifers selbst entwickelt oder in der dunklen Seite des Internets eingekauft hat.

Typischerweise läuft ein APT in fünf Phasen ab (siehe Abbildung 1).

Phase 1: Auskundschaften / Zielerfassung

In der ersten Phase werden Spear Phishing, Watering-Hole-Angriffe und andere Varianten des Social Engineering eingesetzt. Beim Spear Phishing enthält eine als seriös getarnte E-Mail ein Attachment mit Schadsoftware oder einen Link auf eine schadenstiftende Web-Seite. Watering-Hole-Angriffe infizieren zielgerichtet Web-Seiten, die das Ziel potentiell besucht, z. B. eine spezielle Community, wie ein Developer-Forum.

Phase 2: Eindringen und Erstinfektion

In Phase 2 wird der in Phase 1 eingebrachte schadenstiftende Code dann ausgeführt und lädt typischerweise den eigentlichen Schädling auf das angegriffene System. Hierzu muss lediglich ein Internet-Zugang für das infizierte System erlaubt sein, das dann beispielsweise ein sogenanntes Remote Administration Tool (RAT) herunterlädt und ausführt. Das RAT unterhält dann eine Verbindung zur zentralen Infrastruktur des Angreifers, dem Command and Control Server (C&C). Diese Kommunikation ist natürlich nach den Regeln der Kunst verschleiert, d.h. die Kommunikation erfolgt verschlüsselt über mehrere Stufen (z.B. Systeme in einem Bot-Netz), die eine Nachverfolgung ausgesprochen schwer macht.

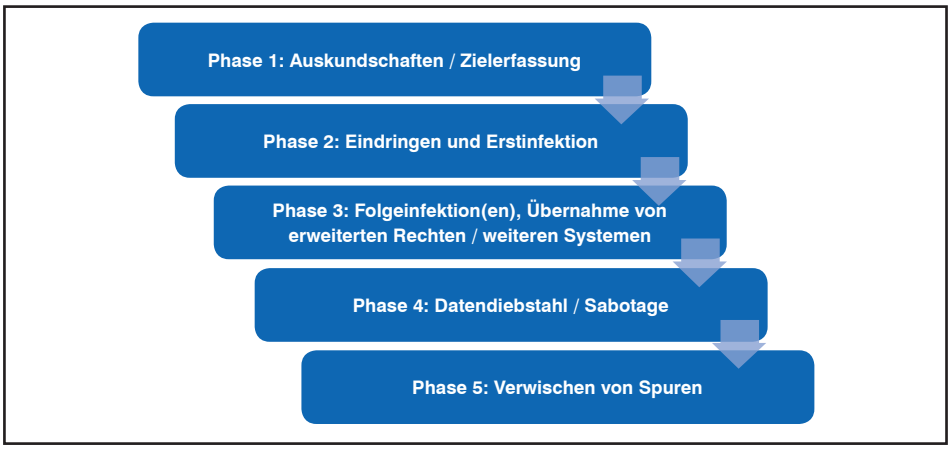


Abbildung 1: Typische Phasen eines zielgerichteten Angriffs

Phase 3: Folgeinfektion(en), Übernahme von erweiterten Rechten / weiteren Systemen

Nicht selten ist das zunächst angegriffene System nicht das eigentliche Ziel bzw. nicht das einzige Ziel. In der dritten Phase erfolgt dann die Ausbreitung des Angriffs im Netzwerk, indem Server, PCs von Administratoren und sonstige Systeme angegriffen werden. Ggf. wird hierfür zusätzliche Schadsoftware vom C&C geladen. Alternativ können auch auf dem kompromittierten Rechner vorgefundene Tools wie Shells, Windows Terminal Services, NetBIOS-Befehle oder Virtual Network Computing verwendet werden.

Phase 4: Datendiebstahl / Sabotage

In Phase 4 verrichtet der Angreifer über die Schadsoftware in der angegriffenen Infrastruktur seinen Dienst, indem er z. B. Systeme sabotiert oder Passworte, Dokumente, etc. überträgt. Bei einem Datendiebstahl befindet sich der eigentliche Ziel-Server wie eben skizziert über mehrere Stufen versteckt im Internet.

Phase 5: Verwischen von Spuren

Zuletzt vernichtet sich der Schädling selbst, mutiert, indem er neuen Schadcode nachlädt, oder löscht lediglich einen Teil seiner Komponenten bzw. Daten und legt sich zur Ruhe.

2. Warum sind zielgerichtete Angriffe so oft erfolgreich?

Der Erfolg zielgerichteter Angriffe hat zwei grundlegende Ursachen:

- **Das Ganze ist mehr als die Summe seiner Einzelteile**
  Es werden system- und anwendungsübergreifende Angriffe ausgeführt. Hierdurch entsteht ein Kumulationseffekt hinsichtlich der ausgenutzten Schwachstellenlage. Hinzu kommen das mangelnde Bewusstsein bei Nutzern und Administratoren, die oft unzureichende Umsetzung von Sicherheitsmaßnahmen und zugehörigen Prozessen sowie auch eine Überschätzung der eigenen Security.

- **Ausnutzung längst bekannter Schwachstellen in der IT**
  Oft müssen gar keine High-End-Angriffswerkzeuge eingesetzt werden, sondern es reichen allgemein verfügbare Freeware Tools. Beim oben genannten Bundestags-Hack 2015 haben die Angreifer unter anderem auch auf das in der Praxis bewährte Tool mimikatz [4] urückgegriffen, um über Schwachstellen in Windows-PCs an Credentials für die Anmeldung an Admin-Konten heranzukommen [5].

3. Gibt es Symptome eines zielgerichteten Angriffs?

In den Phasen 1 und 2 des Angriffs finden sich z. B Malware in E-Mail-Anhängen oder auf Web-Seiten und in Folge Backdoor-Trojaner auf Endgeräten. Hier ist zwar eigentlich der Virenschutz gefordert, nur gelingt es den Angreifern immer wieder sich erfolgreich am Virenschutz vorbei zu schmuggeln.

In den weiteren Phasen eines APT gibt es gewisse Symptome, die auf den Angriff hindeuten können.

In der dritten Phase des Angriffs kann beispielsweise die Zahl der Anmeldungen an Konten mit erweiterten Rechten zunehmen. Dies ist oft auch häufig außerhalb der regulären Arbeitszeit zu verzeichnen. Auch Log-Einträge, die auf gehäufte Fehlanmeldungen an einem System / Konto hindeuten, oder solche, die auf den Stopp / Neustart sicherheitsrelevanter Dienste wie Virenschutz oder Firewall hindeuten, können ein Indiz für einen zielgerichteten Angriff in der Phase 3 sein. An dieser Stelle wird oft die Rolle einer (zentralen) Protokollierung unterschätzt. Die typische Maßnahme, fehlerhafte Anmeldeversuche an Systemen und Anwendungen zentral zu protokollieren und ggf. eine Alarmierung auszulösen, kann solche Angriffe nämlich durchaus aufdecken. Wie die WirtschaftsWoche im Dezember 2016 berichtet hatte, ist z. B. ein massiver Cyberangriff auf Thyssen Krupp dadurch aufgefallen, dass mehrere fehlerhafte Anmeldeversuche auf einem Server verzeichnet wurden.

Während der Phase 4 eines zielgerichteten Angriffs können große Datenbestände an ungewöhnlichen Speicherorten und / oder komprimierte Daten in einem für die betreffende Institution unüblichen Format auffallen. Auch ausgehende Verbindungen zu Servern mit schlechter Reputation, z. B. für schadenstiftende Inhalte bekannte Server oder bekannte C&C Server, deuten auf einen zielgerichteten Angriff hin. Ein weiteres Indiz können ungewöhnliche bzw. große insbesondere ausgehende Datenströme oder ungewöhnliche verschlüsselte Netzverbindungen sein.

4. Maßnahmen

Um zielgerichtete Angriffe erkennen und abwehren zu können, werden system- und anwendungsübergreifende Strategien benötigt. Hierzu reichen jedoch technische Maßnahmen alleine nicht aus! Mindestens genauso wichtig sind organisatorische Maßnahmen, wie beispielsweise die Sensibilisierung aller Mitarbeiter. Damit diese Maßnahmen nachhaltig zusammenwirken und sich ergänzen, ist als Basis ein Information Security Management System (ISMS) unentbehrlich (siehe Abbildung 2).

4.1 Was taugen traditionelle Maßnahmen zur Abwehr von APTs?

Zunächst muss an dieser Stelle festgehalten werden, dass bestehende, traditionelle technische IT-Sicherheitsmaßnahmen ihren festen Platz auch in der Bekämpfung zielgerichteter Angriffe haben (siehe Abbildung 3). Denn jede Maßnahme, die es einem Angreifer erschwert seinen Angriff durchzuführen, ist eine sinnvolle Maßnahme.

Traditionelle technische IT-Sicherheitsmaßnahmen

Intrusion Detection and Prevention Systems (IDPSs) ermöglichen auf der Basis von Signaturen und mit statistischen Methoden eine Erkennung von Anomalien im Netzverkehr, die auf Schadsoftware bzw. allgemein auf einen Angriff hindeuten können. Je nach Policy kann dann ein als schadenstiftend erkannter Verkehr vom IDPS geblockt werden. Da der Einsatz einer IDPS-Funktion z.B. in einer Firewall mit

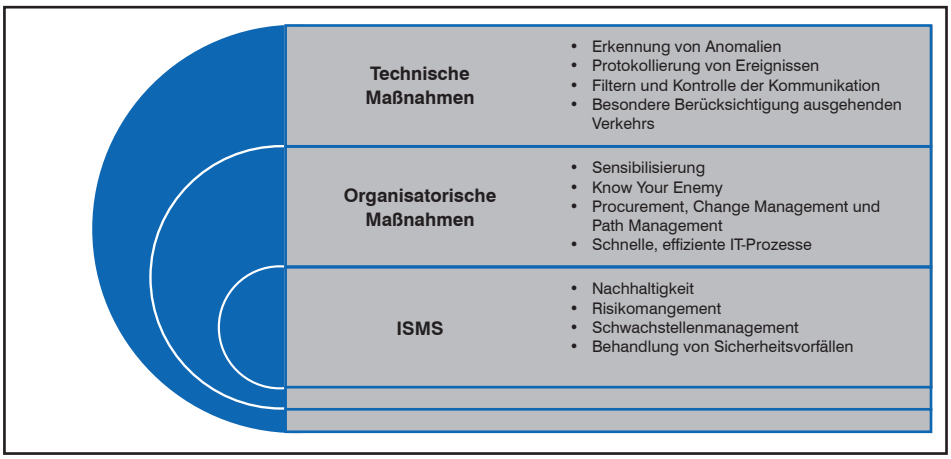


Abbildung 2: System- und anwendungsübergreifende Strategien gegen zielgerichtete Angriffe

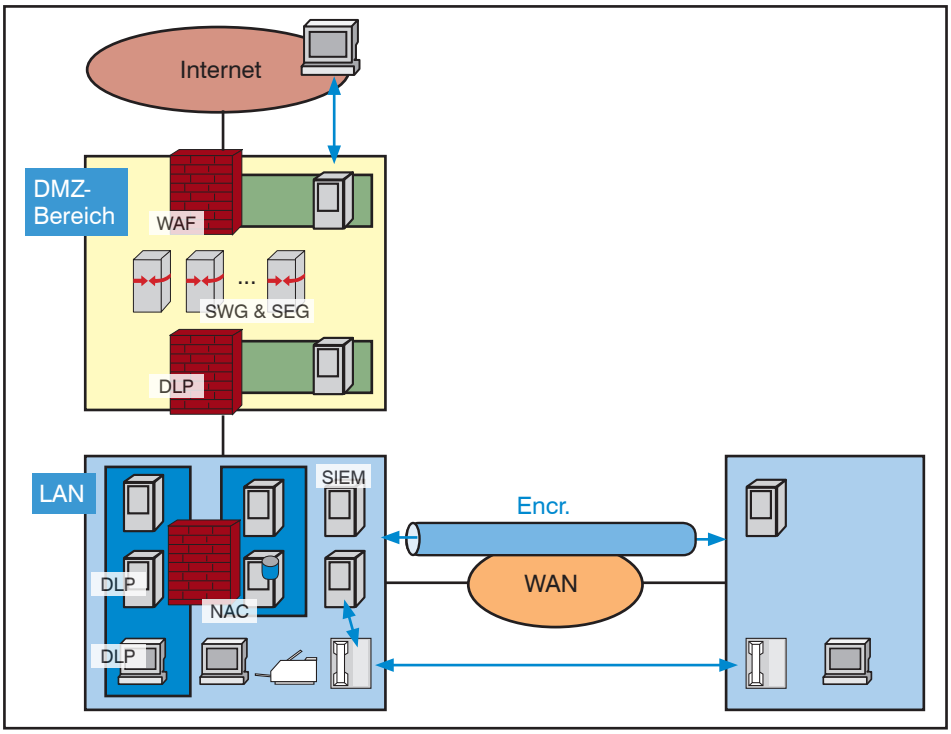


Abbildung 3: Traditionelle technische Sicherheitsmaßnahmen

erheblichen Einbußen in der Performance verbunden ist, erfolgt meist nur ein punktueller Einsatz an kritischen Netzübergängen. Damit hat ein IDPS das grundsätzliche Problem, dass es nur einen kleinen Ausschnitt der Gesamtinfrastruktur sieht und daher system- und anwendungsübergreifende Angriffsmuster ggf. gar nicht wahrnehmen kann. Außerdem analysiert ein IDPS den Verkehr auf Ebene einzelner Pakete, d.h. sehr feingranular und kann daher kaum Ereignisse, zwischen denen eine längere Zeitspanne liegt, korrelieren.

Secure Web Gateways (SWGs) sind im Prinzip Proxies mit zusätzlichen Sicherheitsfunktionen und dienen zur Absicherung des Web-Zugriffs durch URL-Filterung, Malware-Scanning, Content-Filterung sowie Erkennung und Kontrolle von Anwendungen. Die Grenzen von SWGs sind für die Abwehr von APTs jedoch spätestens erreicht, wenn verschlüsselter Verkehr untersucht werden muss, da das Entschlüsseln von Verkehr oft nicht erlaubt ist. Außerdem erfordert der Einsatz von zentralen SWGs in den eigenen Rechenzentren, dass bei mobilen Mitarbeitern der Web-Zugriff ausschließlich über VPN erfolgt, was die Nutzung von Hotspots und auch für diverse Apps auf Smartphones und Tablets unmöglich machen kann.

Secure Email Gateways (SEGs) setzen neben dem klassischen Spam-Filter ähnliche Funktionen wie bei einem SWG ein, d.h. Virenschutz und Entfernen von schadhaften Anhängen, URL-Filterung und Überprüfung in E-Mail-Inhalten. Zur Lösung der offensichtlichen Probleme bezüglich Datenschutz und Postgeheimnis (z.B. Entschlüsselung zur Kontrolle von E-Mails) werden bei SEGs Nutzer-Quarantänen angeboten, wohin verdächtige E-Mails zur Untersuchung verschoben werden. Dies ist jedoch gerade bei einem Verdacht, der sich als falsch herausgestellt hat (sogenannter False Positive), mit Unbequemlichkeiten und einem Zeitverzug für den Nutzer verbunden. Nun ist der Dienst E-Mail aber auch nicht so Zeitunkritisch, wie vielfach behauptet wird. Dieser Aspekt betrifft auch eine weitere Funktion von SEGs: die Sandbox – hierzu später mehr.

Unter den bewährten Schutzmethoden gibt es neben den eben genannten teils auf spezifische Anwendungszwecke bezogene Lösungen auch übergreifende, ganzheitliche Ansätze.

Hierzu zählen neben Netzzugangskontrolle **(Network Access Control, NAC)**, um den Zugang zum Netz zu kontrollieren, die **Verschlüsselung bei Transport und Ablage** von Daten, **Data Loss Prevention (DLP)**, um den Abfluss von Daten zu erkennen, und Lösungen für das **Security Information and Event Management (SIEM)**, um Protokolldaten zu korrelieren und Sicherheitsvorfälle zu erkennen. Gerade die system- und anwendungsübergreifende Korrelation von Ereignissen in einem SIEM-System erweist sich als wichtiges Instrument zur Erkennung von APTs.

Als eine weitere Kernmaßnahme ist die Segmentierung von Netzen zu nennen. **Zonenkonzepte** sehen eine Trennung von Netzen sowohl in Rechenzentren als auch in Campus-LANs in Sicherheitszonen vor, um Kommunikation mit (kritischen) Systemen über ein kontrollierendes Sicherheitselement (Firewall ggf. mit IDPS-Funktion) zu führen. Mit den Mitteln der Netztrennung kann die Ausbreitung von schadenstiftender Software eingegrenzt und insbesondere die Angriffsfläche reduziert werden. Obwohl Zonenkonzepte recht aufwändig in Aufbau und Betrieb sind, haben sie sich zu einem Standardinstrument der Netzwerksicherheit etabliert. Interessant ist in diesem Zusammenhang ein Bericht des FBI, der einen APT analysiert, bei dem im letzten Jahr die Demokratische Partei im Rahmen der Präsidentenwahl in den USA angegriffen wurden [6]. Der Bericht listet in den empfohlenen Top-7-Sicherheitsmaßnahmen gegen APTs an der Position Nr. 4 Zonenkonzepte. An Position Nr. 3 wird in dem Bericht die Einschränkung und Kontrolle von administ-

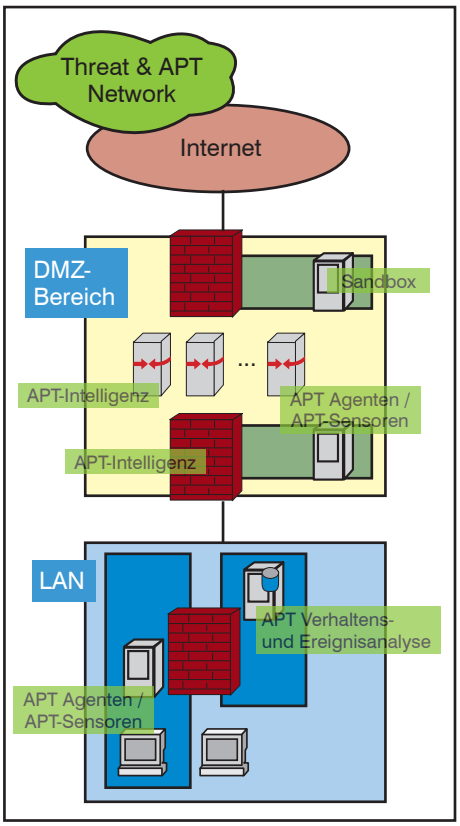


Abbildung 4: Erweiterte technische Sicherheitsmaßnahmen

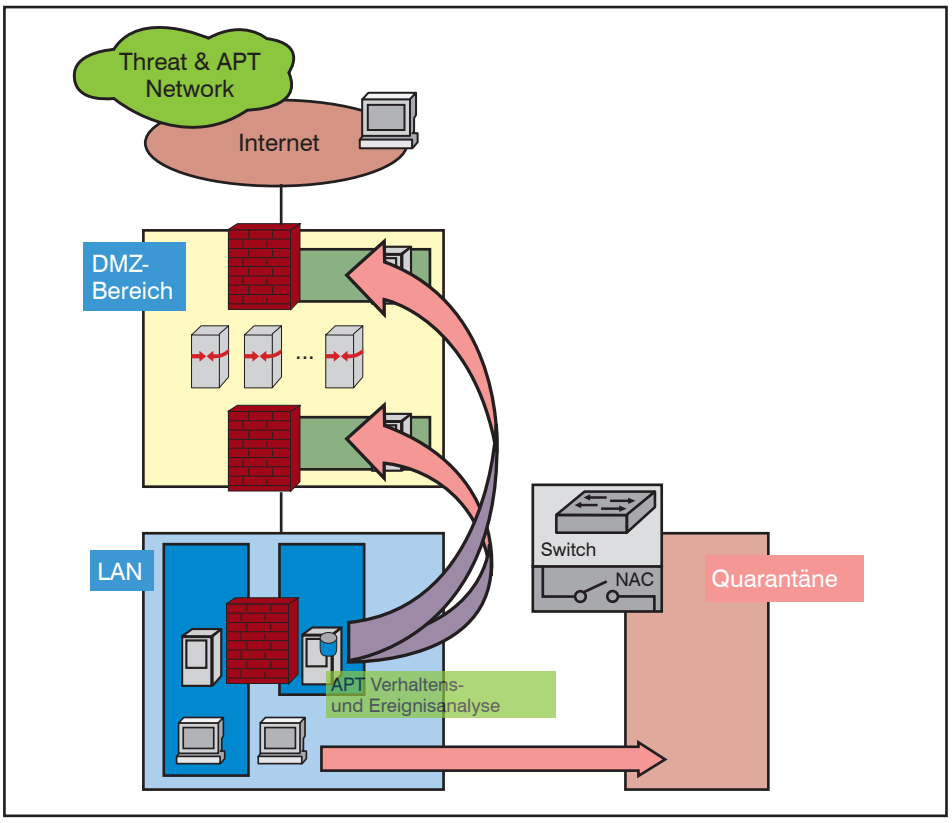


Abbildung 5: Interaktion der erweiterten mit den klassischen technischen Sicherheitsmaßnahmen

rativen Privilegien genannt und auch hier leisten Zonenkonzepte einen wesentlichen Beitrag.

4.2 Erweiterte technische Maßnahmen zur Abwehr von APTs

Die genannten traditionellen Maßnahmen sind zwar wichtig, haben aber nur eine eingeschränkte Wirkung gegen zielgerichtete Angriffe. Durch den speziellen Charakter von APTs sind erweiterte Maßnahmen notwendig, die oft unter dem Namen (Advanced) Threat Protection geführt werden (siehe Abbildung 4). Zu diesen gehören u.a. die Ausführung von Code in einer (virtualisierten) Sandboxumgebung, der Einsatz einer system- und anwendungsübergreifenden angriffsspezifischen Intelligenz zur Korrelation von Ereignissen über einen längeren Zeitraum, zur globalen Analyse von Angriffsschemata und Verhaltensmustern.

Dabei ist es wichtig, dass diese erweiterten Sicherheitsmaßnahmen mit den klassischen Sicherheitsmechanismen bzw. -komponenten interagieren können. Kommunikation, die über eine erweiterte Sicherheitsmaßnahme als zu einem Angriff gehörend identifiziert wurde, muss z.B. an der klassischen Sicherheitskomponente Firewall blockiert werden können. Ebenso könnte der klassische Sicherheitsmechanismus NAC dafür genutzt werden, Systeme, von denen durch erweiterte Sicherheitsmaßnahmen erkannt Angriffe ausgehen, in ein Quarantäne-Netz zu isolieren. (siehe Abbildung 5)

Die wesentlichen erweiterten Sicherheitsmaßnahmen werden im Folgenden vorgestellt.

Sandboxing

Die Funktion des Sandboxing, d.h. der Installation, Ausführung und Beobachtung von verdächtigem Code in einer dediziert bereitgestellten Umgebung, kann unterschiedliche traditionelle Sicherheitselemente sinnvoll ergänzen.

Neben Stand-Alone-Sandbox-Lösungen, wie z. B. von FireEye, findet man die Funktion inzwischen zum einen in Next Generation Firewalls (NGFWs) / IDPS / Unified Threat Management (UTM) Appliances, wie z. B. von Check Point Software, Palo Alto Networks, oder Fortinet. Zum anderen wird Sandboxing häufig als Erweiterung von SWGs (z. B. von Blue Coat oder Zscaler) oder SEGs (wie z. B. Proofpoint oder Cisco) genutzt.

Unabhängig von der Komponente, welche die Sandbox-Funktion realisiert, folgt die Technik einem gleichen Muster. Zunächst muss im Datenverkehr ein ausführbares Objekt (z.B. eine Datei) erkannt werden. Dann wird dieses Objekt in einer meist virtuellen Umgebung auf einem oder mehreren vorgefertigten VMs (z.B. einmal Windows XP, einmal Windows 7 und einmal Windows Server 2012) ausgeführt. Da dies immer Standard-Images sind, kann aufgrund eines geänderten Verhaltens der Maschine festgestellt werden, ob sich mit der Datei z.B. ein RAT mitinstalliert hat, das versucht Kontakt mit dem C&C Server aufzunehmen. Welches Systemverhalten nun auf welche Angriffsart Rückschlüsse erlaubt, muss nun mittels einer (immer aktuellen) Datenbank abgeglichen werden, die Muster für bekannte Angriffe beinhaltet.

Für unterschiedliche Realisierungen der Sandboxing-Funktion ergeben sich natürlich auch unterschiedliche Varianten der Integration in die Infrastruktur (siehe Abbildung 6).

Bei dieser Technik gibt es natürlich auch Tücken. Von der Abbildung von unternehmensspezifischen Images auf Prüfung gegen herstellerspezifischen Standardimages mal abgesehen, gibt es klassische Probleme wie Speicherplatz für virtuelle Maschinen, Datenschutzaspekte bei der Verwendung von Cloud-Lösungen, etc.. Darüber hinaus kann die geringe Akzeptanz von Wartezeit / Latenz, die durch Hochfahren, Ausführung und Scan-

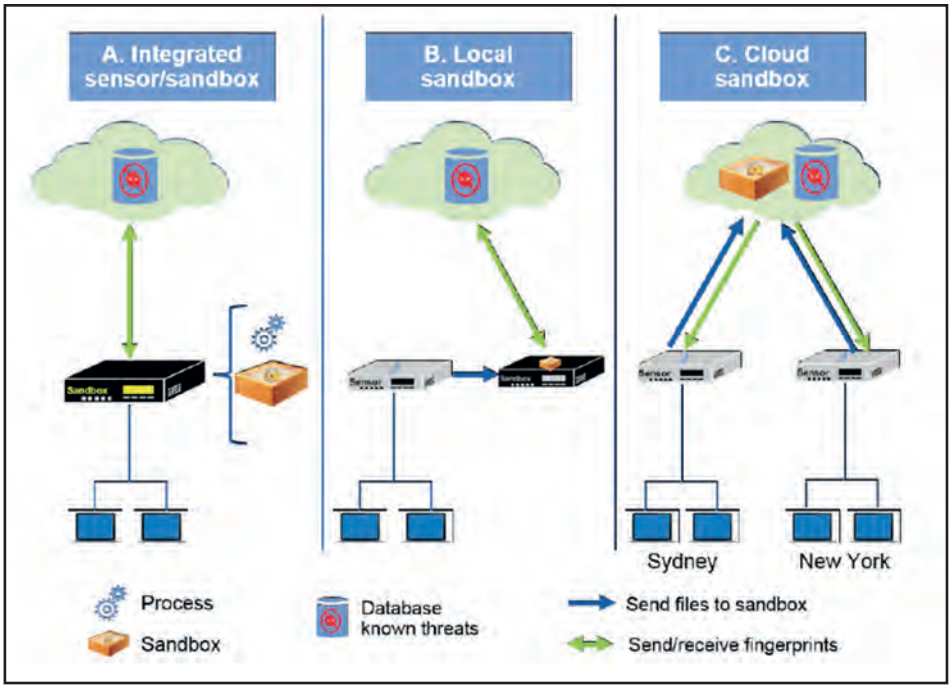


Abbildung 6: Beispiele für die Integration des Sandboxing in die Infrastruktur [7]

ning entsteht, bei (zumindest gefühlt) zeitkritischen Diensten dazu führen, dass die Sandbox ggf. nicht ausreichend effektiv konfiguriert wird. Außerdem passen Angreifer ihre Schadsoftware an Sandboxes an und vermeiden (z.B. einfach durch Passivität) ein Verhalten, das in einer Sandbox zur Einstufung als Schadsoftware führen würde.

Korrelation von Ereignissen mit Big Data

Big-Data-Analysemethoden können gut als Technologie für die Analyse von Merkmalen von zielgerichteten Angriffen genutzt werden, denn bei der Bekämpfung von APTs müssen Informationen aus unterschiedlichsten Quellen zusammengetragen und korreliert werden, um Verhaltensmuster extrahieren zu können, die potentiell auf einen APT schließen lassen.

Wenn alle Sicherheitskomponenten (inklusive Firewalls, IDPSs, SWGs, SEGs, Sandboxing-Lösungen) und zumindest alle exponierten oder kritischen IT-Systeme all ihre Ereignisprotokolle an eine zentrale Stelle bündeln, entsteht innerhalb kürzester Zeit eine enorme Datenmenge. Traditionelle SIEM-Lösungen können nun durch Big-Data-Techniken unterstützt werden, um mit statistischen Modellen und Methoden der Künstlichen Intelligenz in der Ereignisflut Muster von Angriffen herauszulösen. Inzwischen spricht man sogar von einer 2. Generation von SIEMs, die mit Big-Data-Techniken arbeiten. Ein Beispiel ist IBM InfoSphere BigInsights, eine Big-Data-Plattform, welche die traditionelle Sicherheitsplattform QRadar von IBM zur Erkennung von APTs um die Analysemöglichkeiten mit Big Data ergänzt. (siehe Abbildung 7)

4.3 Beitrag eines Information Security Management System

Ohne ein stabil laufendes und nachhaltiges ISMS ist keine erfolgreiche Abwehr zielgerichteter Angriffe möglich. Warum ist das so?

Zunächst bildet ein ISMS die Grundlagen für die Informationssicherheit, indem Organisation, Rollen und Verantwortlichkeiten sowie ein Richtlinienapparat für die Informationssicherheit festgelegt werden. Grundlegende Prozesse der Informationssicherheit müssen erstellt und umgesetzt werden. Hierzu gehören das Risikomanagement, die Behandlung von Sicherheitsvorfällen sowie das Schwachstellenmanagement. Diese stellen die Festlegung und nachhaltige Umsetzung von Sicherheitsmaßnahmen sicher. Außerdem wird die Informationssicherheit durch Schnittstellen zu IT-Prozessen zum integralen Bestandteil der Prozesslandschaft.

Kernprozesse in der Informationssicherheit

Im Rahmen eines ISMS werden die in Abbildung 8 dargestellten Kernprozesse der Informationssicherheit erstellt und umgesetzt, die alle einen wesentlichen Beitrag für den Umgang mit zielgerichteten Angriffen und deren Abwehr liefern.

Der Prozess „Erstellung und Aktualisierung Sicherheitskonzepte“ stellt einen effektiven, effizienten und nachhaltigen Maßnahmenkatalog sicher.

Im Prozess „Schwachstellenmanagement“ erfolgt ein systematisches Management von Schwachstellen bestehend aus systematischer Informationsbeschaffung, Bewertung gefundener Schwachstellen, Maßnahmen zur Behebung der Schwachstellen und einem Risikomanagement bei nicht schnell genug beseitigten Schwachstellen. Dies ist wesent-

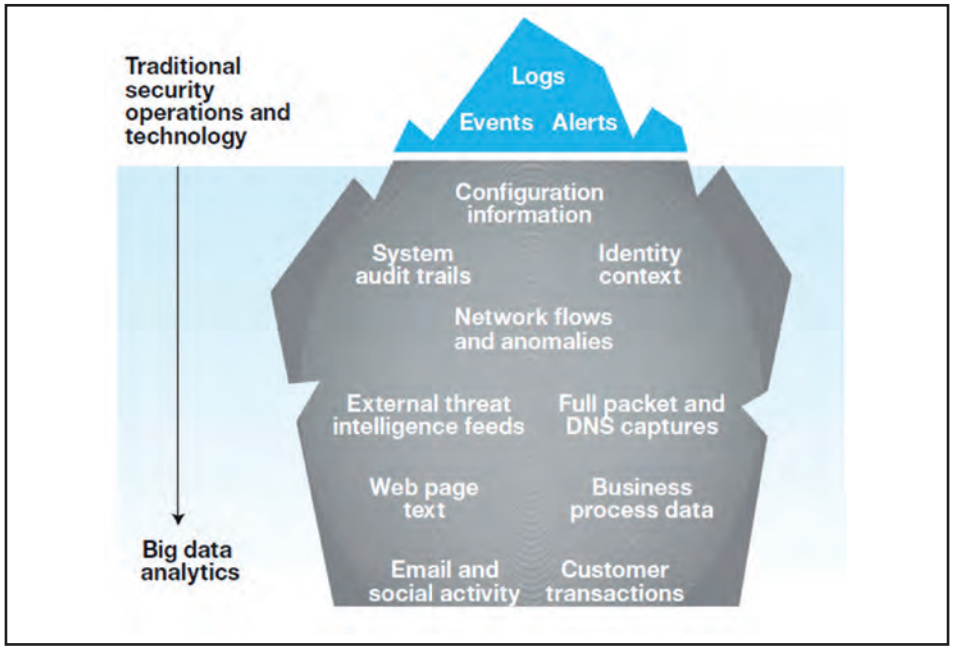


Abbildung 7: Erweiterte Möglichkeiten zur Analyse von Merkmalen von zielgerichteten Angriffen durch Big Data
Quelle: IBM

Abbildung 8: Kernprozesse in der Informationssicherheit

lich für die Abwehr zielgerichteter Angriffe, weil diese vorgefundene Schwachstellen systematisch ausnutzen. Wer also die eigenen Schwachstellen nicht kennt, ist hier schnell verloren. Daher ist es auch wichtig, dass sich an der systematischen Informationsbeschaffung über Schwachstellen alle System- und Anwendungsverantwortlichen beteiligen und diese durch (automatisiertes) Scanning und Penetration Testing ergänzt wird.

Der Prozess „Behandlung von Sicherheitsvorfällen“ sorgt dafür, dass im Fall eines zielgerichteten Angriffs eine schnelle Reaktion durch ein Computer Emergency Response Team (CERT) erfolgen kann. Hierzu gehören die Identifikation und Isolation betroffener Systeme, eine Analyse des Schadens, Maßnahmen zur Schadensbegrenzung, Spurensicherung, Risikomanagement, Nachbearbeitung bzw. forensische Analyse sowie die Verhinderung erneuter Angriffe unter dem Motto „nach dem Angriff ist vor dem Angriff“. Wenn der Angreifer anwendungs- und systemübergreifend denkt, muss die Abwehr mindestens genauso gut sein! Hier zahlt sich eine gute Protokollierung besonders aus. Und umgekehrt gilt auch: Unzureichende Protokollierung und Mängel im Monitoring können Angreifer unsichtbar machen.

Der Prozess „Sensibilisierung und Schulung“ regelt die Sensibilisierung und Schulung der Mitarbeiter. Leider wird dies oft unterschätzt. Gerade gegen Social Engineering in den ersten beiden Phasen eines APT ist ein sensibilisierter IT-Nutzer die stärkste Waffe. Auch in den späteren Phasen ist es immer wieder ein Mensch, der eine Anomalie in der IT entdeckt, und keine Maschine. Außerdem sind bei einem Sicherheitsvorfall und insbesondere bei einem APT Nutzer und Administratoren gefragt, die nicht in Panik verfallen, sondern kühl und sachlich bleiben und wissen, was zu tun ist.

Eine Abwehrschlacht gegen einen Angriff wird vielleicht zunächst zu hemdsärmeligen Maßnahmen zur ersten Schadensbegrenzung führen und es sind noch nicht alle Systeme von Schädlingen bereinigt. Ggf. wird man feststellen, dass auch nach der Abwehr des Angriffs Systeme übrig bleiben, die nicht angemessen abgesichert werden konnten, weil z.B. Schwachstellen sich nicht durch einen Patch beseitigen ließen oder ganz einfach gewisse Sicherheitsmaßnahmen noch nicht umgesetzt werden konnten. Von entscheidender Bedeutung ist hier eine systematische Bewertung des dadurch entstehenden Risikos und wenn am Ende der Betrachtung eine bewusste Risikoübernahme durch die Chefetage erfolgt, so geschieht dies wenigstens sehenden Auges. Das Risikomanagement ist daher in der Informationssicherheit ein entscheidender Kernprozess.

Erst durch eine systematische Überwachung der Informationssicherheit und der zugehörigen Prozesse durch die Messung von Kennzahlen und durch eine regelmäßige Prüfung (Auditierung) kann eine kontinuierliche Verbesserung der Informationssicherheit geschaffen werden. Dies erfolgt durch Anwendung eines PDCA-Zyklus [8], wie in Abbildung 9 dargestellt und in diesem kontinuierlichen Verbesserungsprozess muss sich auch die Abwehr von zielgerichteten Angriffen wiederfinden.

5. Fazit

In diesem Artikel wurden die typischen Phasen eines zielgerichteten Angriffs beschrieben und es wurde aufgezeigt, welche Merkmale auf einen solchen Angriff hinweisen können. Für die technischen Maßnahmen zur Abwehr von zielgerichteten Angriffen wurde der wesentliche Maßnahmenkatalog vorgestellt aber auch dessen Grenzen aufgezeigt. Von entscheidender Bedeutung war dabei, dass die Maßnahmen, wie der Angreifer selbst, system- und anwendungsübergrei-

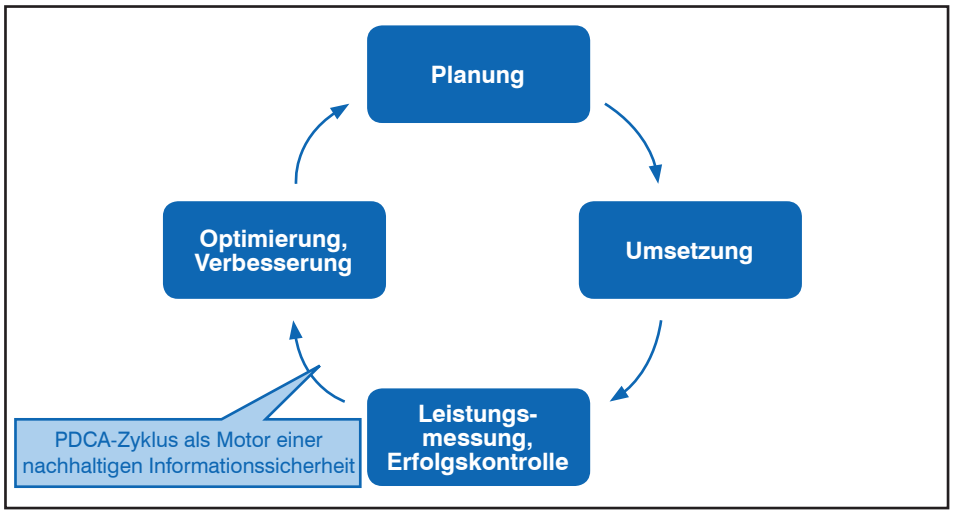


Abbildung 9: PDCA-Zyklus

fend vorgehen. Da ein zielgerichteter Angriff vielschichtiger ist als herkömmliche Angriffe, müssen die traditionellen technischen Maßnahmen durch weitere Maßnahmen ergänzt werden, die Hand in Hand mit den traditionellen Maßnahmen arbeiten. Von besonderer Bedeutung haben sich dabei SIEM-Systeme einer neuen Generation herauskristallisiert. Außerdem wurde die Wichtigkeit eines ISMS für die Abwehr von gezielten Angriffen herausgestellt. Durch die nachhaltige Umsetzung der Kernprozesse eines ISMS wird die Basis für die Abwehr von zielgerichteten Angriffen geliefert und eine schnelle sinnvolle Reaktion auf diese Angriffe ermöglicht.

Alle diese Maßnahmen können zielgerichtete Angriffe zwar nicht grundsätzlich verhindern, aber sie können einen zielgerichteten Angriff erschweren bzw. erkennen und seine Auswirkungen durch eine schnelle sinnvolle Reaktion verhindern oder zumindest abschwächen.

6. Abkürzungen

APT	Advanced Persistent Threat
BSI	Bundesamt für Sicherheit in der Informationstechnik
C&C	Command and Control Server
CERT	Computer Emergency Response Team
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
EVAS	Endpoint Visibility, Access, and Security
IDPS	Intrusion Detection and Prevention System
IPS	Intrusion Prevention System
ISMS	Information Security Management System
IS	Informationssicherheit
IT	Informationstechnologie
KRITIS	Kritische Infrastrukturen
LAN	Local Area Network
NAC	Network Access Control
NGFW	Next Generation Firewall
PDCA	Plan, Do, Check, Act
RAT	Remote Administration Tool
SEG	Secure E-Mail Gateway
SIEM	Security Information and Event Management
SWG	Secure Web Gateway
URL	Uniform Resource Locator
UTM	Unified Threat Management
VPN	Virtual Private Network
WAF	Web Application Firewall
WAN	Wide Area Network

7. Verweise

[1] Siehe http://www.spiegel.de/netzwelt/web/cyberattacke-auf-bundestag-es-droht-ein-millionenschaden-a-1038178.html

[2] Siehe http://www.spiegel.de/politik/ausland/usa-russland-soll-computersystem-des-weissen-hauses-gehackt-haben-a-1027422.html

[3] Siehe https://www.bsi.bund.de/DE/Publikationen/Lageberichte/bsi-lageberichte.html

[4] Siehe http://blog.gentilkiwi.com/mimikatz

[5] Siehe https://netzpolitik.org/2016/wir-veroeffentlichen-dokumente-zum-bundestagshack-wie-man-die-abgeordneten-im-unklaren-liess/

[6] FBI, „GRIZZLY STEPPE – Russian Malicious Cyber Activity", Reference Number JAR-16-20296A, 29. Dezember 2016, verfügbar unter https://www.us-cert.gov/security-publications/GRIZZLY-STEPPE-Russian-Malicious-Cyber-Activity

[7] Quelle: Gartner, „Market Guide for Network Sandboxing"

[8] PDCA: Plan, Do, Check, Act

ComConsult Veranstaltungskalender

MDM: juristische Rahmenbedingungen und sicherheitstechnische Abhängigkeiten, wie Recht und Technik zusammenwachsen, 08.05. - 09.05.2017 in Frankfurt

Garantietermin

Die Anforderung an IT-Abteilungen, mobile (und teilweise auch privat genutzte) Geräte wie Smartphones und Tablets in das Firmennetz einzubinden, wächst rasant. Dieses Seminar erläutert ausgehend von typischen technischen Implementierungen detailliert die rechtlichen Maßnahmen, um einerseits die IT-Sicherheit zu gewährleisten und auf der anderen Seite Verstöße gegen Datenschutzrecht, Persönlichkeitsrecht und Betriebsverfassungsrecht auszuschließen.

Preis: € 1.590,-- *

IT-Projektmanagement Kompaktseminar, 08.05. - 10.05.2017 in Aachen

Garantietermin

Seminar über Projektmanagement in der IT. Es wird speziell auf die Anforderungen und Herausforderungen von IT-Projekten eingegangen. Lernen Sie wie Sie Projekte sauber aufsetzen und überwachen und mit welchen Methoden und Hilfsmitteln Sie die Termineinhaltung sicherstellen können.

Preis: € 1.890,-- *

Umfassende Absicherung von Voice over IP und Unified Communications, 08.05. - 10.05.2017 in Frankfurt

Garantietermin

Dieses Seminar zeigt die Risiken beim Einsatz von Voice over IP und Unified Communications auf und gibt den Teilnehmern einen Überblick über die zu ergreifenden Sicherheitsmaßnahmen. Auf Grundlage von Best Practices aus dem Beratungsgeschäft sowie den marktrelevanten Standards, wie z.B. der „Technischen Leitlinie für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf“ (TLSTK II) des BSI, werden den Teilnehmern die Anforderungen an eine Sicherheitskonzeption für TK und UC vermittelt. Das Seminar richtet sich vorrangig an Sicherheitsverantwortliche, Planer, Architekten und Betreiber von TK- und UC-Systemen.

Preis: € 1.890,-- *

Lokale Netze für Einsteiger, 08.05. - 12.05.2017 in Aachen

Garantietermin

Dieses Seminar vermittelt kompakt und intensiv innerhalb von 5 Tagen die Grundprinzipien des Aufbaus und der Arbeitsweise Lokaler Netzwerke. Der Intensiv-Kurs vermittelt die notwendigen theoretischen Hintergrundkenntnisse, vermittelt den praktischen Aufbau, den Betrieb eines LANs und vertieft die Kenntnisse durch umfangreiche, gruppenbasierende Übungsbeispiele. Ausgehend von einer Darstellung von Themen der Verkabelung und Übertragungsprotokolle wird die Arbeitsweise von Switch-Systemen, drahtloser Technik, den darauf aufsetzenden Verfahren und der Anbindung von PCs und Servern systematisch erklärt.

Preis: € 2.490,-- *

Verkabelungssysteme für Lokale Netze, 15.05. - 16.05.2017 in Düsseldorf

Garantietermin

Dieses Seminar erklärt praxisnah und herstellerneutral wie Sie hohe Qualität, Verfügbarkeit und lange Nutzbarkeit bei der Planung und im Betrieb einer Verkabelungs-Lösung erreichen. Die Bausteine einer Verkabelung werden vorgestellt und zu einem handhabbaren Gesamtsystem kombiniert. Lernen Sie wo sich gute von schlechten Lösungen unterscheiden. Dabei werden die Normen diskutiert und die praktische Handhabung der Normungsvorgaben erklärt. Der 2. Tag widmet sich der konkreten Durchführung einer Planung in kleinen Übungsgruppen.

Preis: € 1.430,-- *

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen, 15.05. - 17.05.2017 in Düsseldorf

Garantietermin

Dieses Seminar vermittelt alle notwendigen Projektschritte zu einer erfolgreichen Umsetzung von VoIP Projekten. Diese erstrecken sich über die Einsatz- und Migrations-Szenarien, die einsetzbaren Basis-Technologien und Komponenten und die erweiterten TK-Anwendungen wie IVR, UM oder UC. Es werden Bewertungskriterien für eine TK-Lösung und eine Übersicht über den bestehenden TK-Markt mit allen etablierten Hersteller vorgestellt.

Preis: € 1.890,-- *

Sonderveranstaltung: Implementierung von IPv6 – Erkenntnisse und Erfahrungen, 22.05.2017 in Bonn

Garantietermin

IPv6 Projekte sind angelaufen. IPv6 existiert nicht mehr nur in Forschungsumgebungen, bei den Providern und in Testnetzen von Unternehmen. Immer mehr Firmen haben mit der Migration begonnen, von DAX 30 bis Mittelständler, von Finanzinstituten bis zur Fertigung. Nicht nur der Internet-Auftritt, der Provider-Anschluss und die Homeoffice VPNs werden migriert. Auch in den Unternehmen selbst hat die Migration begonnen. Profitieren Sie in dieser Sonderveranstaltung von den Erfahrungen, die bei laufenden Projekten gesammelt wurden.

Preis: € 1.090,-- *

Recht und Datenschutz bei Einführung von VoIP, 29.05. - 30.05.2017 in Frankfurt

Garantietermin

Ziel der Schulung ist es, den Teilnehmern einen Überblick über die aktuelle Situation im Bereich des Datenschutzes im Kommunikationsumfeld zu verschaffen. Datenschutz und Datensicherheit werden zunehmend wichtiger im Umgang mit Kunden und Mitarbeitern. Gerade mit der Einführung von IP basierten Lösungen in den Bereichen Telefonie oder Contact Center, stellen sich neue Herausforderungen in Bezug auf personenbezogene Informationen.

Preis: € 1.590,-- *

SIP – Basis-Technologie der IP-Telefonie, 29.05. - 31.05.2017 in Frankfurt

Garantietermin

Ziel der Schulung ist die Erläuterung von SIP als Schlüsseltechnologie für eine offene, leistungsfähige und kostenoptimale Kommunikationslösung. Es umfasst nahezu alle Dienste, die wir heute für UC benötigen: Sprache, Video, Daten und Präsenz. Lernen Sie was SIP leistet, worin sich wesentliche Herstellerlösungen unterscheiden und wie Sie das Beste aus beiden Welten zukunftsorientiert nach Ihrem Bedarf optimieren.

Preis: € 1.890,-- *

* alle ausgewiesenen Preise sind netto-Preise

Zertifizierungen

ComConsult Certified Network Engineer

Lokale Netze für Einsteiger
18.09. - 22.09.17 in Aachen

TCP/IP-Netze erfolgreich betreiben
29.05. - 31.05.17 in Aachen
09.10. - 11.10.17 in Bremen

Internetworking
19.06. - 23.06.17 in Göttingen
13.11. - 17.11.17 in Aachen

Paketpreis für ein 5-tägiges, ein 4-tägiges und ein 3-tägiges Intensiv-Seminar € 6.000,--* (Summe der Einzelpreise: € 6.670,--*)

ComConsult Certified Trouble Shooter

Trouble Shooting in vernetzten Infrastrukturen
26.09. - 29.09.17 in Aachen

Trouble Shooting für Netzwerk-Anwendungen
27.06. - 30.06.17 in Aachen
07.11. - 10.11.17 in Aachen

Paketpreis für beide Seminare inklusive Prüfung € 4.280,--*
(Seminar-Einzelpreis € 2.290,--* , mit Prüfung € 2.470,-- *)

ComConsult Certified Voice Engineer

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen
15.05. - 17.05.17 in Düsseldorf
16.10. - 18.10.17 in Frankfurt

Session Initiation Protocol Basis-Technologie der IP-Telefonie
29.05. - 31.05.17 in Frankfurt
08.11. - 10.11.17 in Stuttgart

Umfassende Absicherung von Voice over IP und Unified Communications
10.07. - 12.07.17 in Düsseldorf

Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter
18.09. - 19.09.17 in Düsseldorf

Wir empfehlen die Teilnahme an diesem Seminar **"IP-Wissen für TK-Mitarbeiter"** all jenen, die die Prüfung zum ComConsult Certified Voice Engineer anstreben, ganz besonders aber den Teilnehmern, die bisher wenig bis kein Netzwerk Know How, insbesondere TCP/IP, DNS, SIP usw., vorweisen können.

Basis-Paket: Beinhaltet die drei Basis-Seminare
Grundpreis: € 5.100,--* statt € 5.670,--*
Optionales Einsteigerseminar: Aufpreis € 1.190,--* statt € 1.590,--*

* alle ausgewiesenen Preise sind netto-Preise

Impressum

Verlag:
ComConsult Research Ltd.
64 Johns Rd
Christchurch 8051
GST Number 84-302-181
Registration number 1260709
German Hotline of ComConsult-Research:
02408-955300

E-Mail: kundenservice@comconsult-research.de
http://www.comconsult-research.de

Herausgeber und verantwortlich
im Sinne des Presserechts:
Dr. Jürgen Suppan
Chefredakteur: Dr. Jürgen Suppan
Erscheinungsweise: Monatlich,
12 Ausgaben im Jahr

Bezug: Kostenlos als PDF-Datei
über den eMail-VIP-Service
der ComConsult Akademie