ComConsult Research

Der Netzwerk Insider

September 2016

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

DNSSEC und Zertifikate: Symbiose oder Widerspruch

von Markus Schaub

Was haben die Domain Name System Security Extensions und IPv6 gemeinsam: sie sind „uralt“ und kommen nur langsam in Fahrt. Aber noch etwas anderes haben sie gemeinsam: für die Zukunft des Internets sind beide von enormer Bedeutung.

Das Grundproblem der Zertifikate ist, dass jede CA jede Domain zertifizieren kann. Nimmt man nun hinzu, dass das DNS unter multiplen Schwachstellen leidet, ist es durch eine Kombination beider Verfahren möglich einen Man-in-the-Middle-Angriff zu generieren, indem man mittels gefaktem DNS-Eintrag auf einen Server mit falschem Zertifikat verweist.

Zugegeben, das ist nichts für die Script-Kiddis, aber für staatliche Spionage bspw. ist es vergleichsweise einfach.

Hier verspricht eine Kombination aus DNSSEC und Zertifikaten Abhilfe zu schaffen, genannt DNS-based Authentication of Named Entities (DANE). Im Folgenden werden die dafür notwendigen Verfahren vorgestellt und auf ihre Alltagstauglichkeit bewertet.

weiter auf Seite 6

Zweitthema

Die Zukunft von VoIP und UC liegt in der Cloud

von Markus Geller

Seit geraumer Zeit beobachten wir bei ComConsult Research die Vorgänge am deutschen und am europäischen Markt. Das Fazit, das sich hieraus ergibt, wird dem ein oder anderen Leser nicht gefallen, aber es wird sich mittelfristig nicht mehr verhindern lassen: VoIP und UC Lösungen werden zukünftig aus der Cloud erbracht werden.

Natürlich fragen Sie sich jetzt, was denn an dieser Erkenntnis neu sein soll, da doch schon seit mehreren Jahren hierfür massiv geworben wird. Dafür muss man zunächst einmal einen Blick auf die aktuelle Situation der VoIP und UC Verbreitung und auf die Akzeptanz von Cloud Lösungen werfen und in einem dritten Schritt die aktuellen Neuerungen und Anforderungen auf Seiten der Kommunikation von Unternehmen und Kunden betrachten.

Doch zunächst ein Blick auf die aktuelle Situation im Enterprise UC, oder besser, Telefonie Markt.

weiter auf Seite 16

Geleit

Gibt es eine tragfähige IT-Strategie unter Vermeidung der Cloud?

auf Seite 2

Statement

Microsoft-Urteil: Ein Meilenstein für Datenschutz in der Cloud

auf Seite 14

Aktuelle Kongresse

ComConsult Technologie-Tage 2016 UC-Forum 2016

auf Seite 4/5 und Seite 23-25

Aktuelles Seminar

Crashkurs IT-Recht für Nichtjuristen

auf Seite 15

Zum Geleit

Gibt es eine tragfähige IT-Strategie unter Vermeidung der Cloud?

Unsere eher kritische Grundhaltung zur Infrastructure as a Service IaaS-Cloud ist bekannt und kann zum Beispiel dem Geleit des letzten Netzwerk Insiders entnommen werden. Trotzdem kann man nicht ignorieren, dass auch große und sehr Sicherheits-bewusste Unternehmen einen Teil ihrer IT in der Cloud betreiben. Zur Vorbereitung der ComConsult Technologie-Tage 2016 im November arbeiten wir an einer Analyse der Cloud-Situation und untersuchen dabei folgende Fragen:

- was ist die Motivation von Unternehmen die Cloud zu nutzen?
- welche Art von Anwendungen werden in der Cloud betrieben?
- wie kann man die Sicherheits-Situation in der Cloud einschätzen?
- was kann man von Unternehmen, die diesen Schritt gemacht haben, lernen?

Unsere Untersuchungen konzentrieren sich dabei auf Unternehmen, die Anwendungen selber in einer IaaS-Lösung in der Cloud betreiben beziehungsweise solche Anwendungen dorthin migriert haben. (Wie schon häufiger angemerkt sehen wir Software as a Service sehr positiv und grenzen diesen Bereich deutlich von Infrastructure as a Service ab. Von daher bezieht sich diese Analyse nicht auf SaaS-Angebote) Wir haben uns für diese Analyse auf Amazon AWS konzentriert. Amazon ist im Moment mit weitem Abstand der Marktführer (auch wenn sich das schon in wenigen Jahren durch das sehr starke Wachstum von Microsoft Azure ändern kann). Als Basis haben wir eine Auswahl der von Amazon benannten Referenzkunden und deren Eigendarstellung zu ihren Cloud-Projekten genommen.

Wir sind dabei zu einer ganzen Reihe wesentlicher und auch interessanter Erkenntnisse gekommen:

- Anbieter wie Amazon haben sich in den letzten drei Jahren komplett neu positioniert. Aus den einfachen Dienst-Strukturen des Cloud-Beginns sind inzwischen hoch-komplexe und sehr weitgehende Gesamtangebote geworden. Im Kern bedeutet das, dass Produkte wie AWS heute klar Platform as a Service PaaS Angebote sind und immer weniger den Fokus auf die reine Rechenleistung legen (im Moment bietet Amazon 73 Dienste an)

- Dies drückt sich auch im Kundenverhalten aus: Amazon wurde noch vor wenigen Jahren vor allem wegen seiner Agilität genutzt. Software-Anbieter konnten während der Markteinführung eines Produkts ohne die Bindung von Kapital ihre Leistung ohne Risiken skalieren. Sobald der Markterfolg klar war und der Kapazitätsbedarf der nächsten Jahre abschätzbar war, sind diese Kunden aber dann auf den Eigenbetrieb gewechselt. Dies hat sich inzwischen gewandelt. So sehen wir mittlerweile Kunden, die einen ausgeprägten Eigenbetrieb haben, mit genau klassifizierbaren Anwendungen zu Amazon wechseln.

- Tatsächlich ist die direkte Wirtschaftlichkeit bzw. das Einsparpotenzial für die Mehrheit der Referenzkunden nicht der entscheidende Grund für die Nutzung der Cloud. Dies entspricht interessanterweise genau den Erfahrungen, die wir im SaaS-Markt machen. Auch deckt sich das mit unserer Sicht zu den Gesamtprozess-Kosten einer Anwendung im Unternehmen. Vereinfacht ausgedrückt muss ein Cloud-Service einen Mehrwert liefern, der über eine simple Einsparung bei einer ausgewählten Ressource hinaus geht.

Ein Beispiel aus dem Bankenbereich soll die Motivation der von uns untersuchten AWS-Kunden verdeutlichen. Die Umsetzung eines Internet-Bankings in der Cloud widerspricht erst einmal allen Erwartungen. Intuitiv hätte man hier erhebliche Sicherheits-Bedenken vermutet. Allerdings muss man die Rahmenbedingungen des Marktes verstehen, um diesen Schritt nachvollziehen zu können. Banken bauen weltweit den Filialbetrieb ab. Die Situation in Deutschland ist dabei noch als sehr positiv einzuschätzen. In England ist es zum Beispiel mit erheblichen Problemen verbunden überhaupt noch einen persönlichen Kontakt zu erhalten. Mit dem Abbau der Filialen geht aber ein wichtiges Kunden-Bindungs-Instrument verloren. Damit kommt dem Internet-Banking eine besondere Bedeutung zu. Hier geht es nicht nur um den technischen Aspekt einer Kontoverwaltung sondern vor allem um die Schaffung einer neuen “Erlebnis-Welt”. Und viele Banken tun sich damit sehr schwer. Meine Hausbank ANZ hat 8 Jahre gebraucht um eine 2-Faktoren Authentifizierung einzuführen und 6 Jahre um die Datenbank der gespeicherten Kontakte von 20 auf unendlich zu erhöhen. Und immer noch gibt es keine Suchfunktion nach einer bestimmten Buchung, auch gibt es keine automatische Erkennung von Transaktionen so wie dies externe Banking-Pakete unterstützen. Auch die deutschen Sparkassen sind hier so träge wie ein Öltanker ohne Ruder. Der Projektbericht der Westpac-Bank, die ihr Internet-Banking auf AWS verlagert hat, spricht von 18 Monaten Vorlaufzeit für relativ kleine Änderungen in ihrer alten Lösung. Mit dem Wechsel auf AWS hat sich diese Vorlaufzeit angeblich auf Tage und Wochen reduziert. Und die Gründe dafür liegen nicht nur in der Agilität der Plattform (ein Hauptargument für IaaS) sondern vor allem im Gesamtfunktionsumfang der AWS-Lösung. Die resultierende Situation für die Westpac-Bank ist damit klar. Im Verbund mit dem weiteren Filialabbau entsteht ein direkter und erheblicher Vorteil im Wettbewerb mit den anderen Banken. Die Tatsache, dass der Hardware-Betrieb dabei 30% günstiger ist, ist dabei komplett unerheblich. Es geht um den Gesamtprozess der Kundenansprache und Kundenbetreuung. Und der wird nach der Wirtschaftlichkeit der angebotenen Bankdienste und nicht nach den Kosten der Rechnerleistung bewertet. Hätte die Westpac das nicht in einer Private Cloud realisieren können? OpenStack liefert heute die notwendige Agilität für Basis-Kapazitäten in einer PrivateCloud-Lösung. Aber die Lösung steckt noch in den Kinderschuhen und liegt in der Grundfassung weit hinter dem Funktionsumfang einer AWS-Lösung zurück (das ist tatsächlich schwer zu bewerten, da OpenStack-Lösungen ja im Prinzip um alles mögliche angereichert werden können). Und was ist mit der Sicherheit? Die Westpac folgt hier der Argumentation, dass sie auch in der Cloud der Gestalter ihrer eigenen Sicherheit ist und kein direkter Nachteil mit der Lösung

Gibt es eine tragfähige IT-Strategie unter Vermeidung der Cloud?

verbunden ist. Andere Unternehmen wie die New Zealand Defense Forces nutzen die Cloud als Frontend und halten die eigentlichen Daten (dies sind zum Beispiel die Daten, die nicht von aktuellen Transaktionen betroffen sind) weiterhin lokal.

Wir werden das Thema der Sicherheit in der Cloud auf den ComConsult Technologie-Tagen vertiefen. Es gibt natürlich das Argument, dass der Amazon Hypervisor ein herausragendes Angriffsziel für potenzielle Angreifer ist. Und natürlich muss man sich der Frage stellen was es bedeuten würde, wenn ein Angreifer die Kontrolle über den Hypervisor erlangen würde. Aber dies gilt auch und noch mehr für VMware und Konsorten, die zudem den Nachteil haben direkt zugreifbar und testbar zu sein während die Details des Amazon-Hypervisors nach Außen unbekannt sind. Trotzdem ist und bleibt dies das dominante Thema für ein Arbeiten in der Cloud. Mit der Ausweitung der Funktionalität und einer damit verbundenen Verlagerung der Nutzungsmotivation weg von den Kosten und hin zur Funktionalität konzentriert sich alles auf die Sicherheitsfrage. Die Architekturelemente, die in der Cloud für einen Kunden zur Umsetzung von Sicherheit gegeben sind, sind dabei ähnlich denen in der lokalen Umgebung. Im Prinzip kann die komplette bestehende Architektur umgesetzt werden. Nur muss man dabei physikalische Komponenten durch virtuelle Instanzen wie NFV ersetzen. Dies wird ergänzt um Georedundanz und Cloud-spezifische Skalierungsfragen. Wenn also der Angreifer in der Cloud auf dieselben Hindernisse stößt wie in der lokalen Installation, dann muss sich die Diskussion auf die Sicherheit des Frameworks konzentrieren. Aus der Sicht der Betreiber bildet die Cloud neue Zonen ab und passt damit konzeptionell zum bisherigen Zonenmodell. Wie gesagt mehr dazu auf unseren Technologie-Tagen im November.

Unsere Schlussfolgerungen daraus in Kombination mit unserer Gesamtsicht zur Cloud sind:

- die Mehrheit der in einem RZ betriebenen Anwendungen sollte auch dort bleiben. Aber es gibt bestimmte Typen von Anwendungen, bei denen die Cloud-Frage gestellt werden sollte. Wir werden diese Nutzungsmuster zusammen mit der Sicherheitsfrage auf den Technologietagen 2016 diskutieren.

- eine Entscheidung für die Cloud ist nicht zwingend eine rein wirtschaftliche Entscheidung. Alle untersuchten Unternehmen haben neben der bereits bekannten Agilität (der schnellen von Verfügbarkeit von Ressourcen) die Funktionalität und Qualität der Gesamtumgebung als wesentlichen Grund angegeben.

- nach wie vor stellt die Cloud keine existenzielle Bedrohung für ein Rechenzentrum dar. Viele der vorhandenen Anwendungen lassen sich gar nicht in die Cloud migrieren und eine Neuprogrammierung ist jenseits jeder Wirtschaftlichkeit.

- auch bei den untersuchten Unternehmen wird eine 1:1-Migration mit Fragezeichen versehen. Selbst wenn die bestehende Architektur Cloud-fähig ist, bieten die Cloud-Umgebungen wie AWS viele Dienste, die es so bisher lokal nicht gab. Umgekehrt gibt es lokale Dienste, die es in der Cloud nicht gibt. Zum Beispiel müssen alle physikalischen Instanzen durch virtuelle ersetzt werden (inkl. Firewall, IDS, …). Damit wird selbst im Idealfall eine 1:1 Migration in Frage gestellt.

- wie im Geleit des September Insiders beschrieben ist es bei dem Vergleich der Wirtschaftlichkeit dringend geboten, Gesamtprozesse als Basis zu nehmen. Die von Cloud-Anbietern zum Teil veröffentlichten Wirtschaftlichkeits-Daten zum Beispiel zum Betrieb von Servern sind Ausschnitte aus Prozessen, die es so in normalen Unternehmen nicht gibt. Dafür sind die Betriebsprozesse in einem Standard-Rechenzentrum am Endanwender orientiert und decken Bereiche wie den Help-Desk oder ein 24/7-Operating ab.

- die Zeit, in der man die Cloud mit dem simplen Argument der Sicherheit abblocken konnte, sind vorbei. Die Anbieter wie Amazon haben dieses Argument gesehen und bieten heute weit entwickelte Infrastrukturen für Verfügbarkeit und Sicherheit. Die Tatsache, dass das neuseeländische Militär oder auch marktführende Banken mit ihrem Internet-Banking zu den Amazon-Kunden gehören, unterstreicht das. Allerdings wird bei näherer Betrachtung auch klar, dass diese Kunden ihre Lösungen entsprechend ausgelegt haben.

Daher analysieren wir auf den Technologie-Tagen 2016 unter anderem folgende Fragen:

- welches Grundmuster kann man bei den Cloud-Referenzkunden von Amazon erkennen?
- inwieweit kann das auf andere Unternehmen und Behörden übertragen werden?
- welche Arten von Applikationen sollten besser in der Cloud positioniert werden?
- was bedeutet der Übergang von IaaS auf PaaS für den Markt?
- wie sehen die Projekterfahrungen ausgewählter Amazon-Kunden aus?
- wie sieht eine gut strukturierte Sicherheits-Lösung unter Einbeziehung der Cloud aus?
- welche Technologieelemente werden in der Cloud genutzt und können auch lokal im Rechenzentrum zu einem Effizienzschub führen?
- wo sind die Grenzen der Cloud und was wird auf Dauer immer im lokalen Eigenbetrieb bleiben müssen?

In diesem Sinne und in der Hoffnung diese Fragen auf den ComConsult Technologie-Tagen mit Ihnen lebhaft diskutieren zu können

Ihr
Dr. Jürgen Suppan

Kongress

ComConsult Technologie-Tage 2016
07.11.-08.11.16 in Köln

Dieses Jahr haben wir folgende zentrale Themenbereiche in den Vordergrund gestellt:

1. Strategien für das Rechenzentrum der Zukunft
2. Kommunikations-Strategie 2020 im Mittelpunkt
3. Skalierbarkeit in einem Technologie-Mix
4. Sicherheits-Strategie 2020

Moderator: Dr. Jürgen Suppan - Preis: 1.990,- € netto

Buchen Sie über unsere Web-Seite

www.comconsult-akademie.de

Aktueller Kongress

ComConsult Technologie-Tage 2016 07.11.-08.11.16 in Köln

Die ComConsult Akademie veranstaltet vom 07.11. bis 08.11.16 ihre "ComConsult Technologie-Tage 2016" in Köln.

Dieses Jahr haben wir folgende zentrale Themenbereiche in den Vordergrund gestellt:

1. Strategien für das Rechenzentrum der Zukunft

Würde man heute ein Rechenzentrum komplett neu ausstatten oder bauen, würde es sich deutlich von der Situation vor 5 Jahren unterscheiden. Skalierbarkeit und Wirtschaftlichkeit führen zu deutlich veränderten Schwerpunkten: der Wunsch bestehende Kapazitäten schnell und preiswert in kürzester Zeit anpassen zu können erfordert geeignete Architekturen über Technologie-Grenzen hinweg. Die Abgrenzung zur Cloud ist dabei ebenso eine treibende Kraft wie eine Chance. Zum einen haben Cloud-Rechenzentren Technologien und Architekturen marktreif und allgemein nutzbar gemacht, die es so vorher nicht gab. Zum anderen wird eine teilweise Integration von Cloud-Leistungen für die meisten Betreiber auf 5 Jahre gesehen unvermeidbar sein. Die Schlüsselfrage ist: wie kann ein Rechenzentrum zu einer fundierten technischen und wirtschaftlichen Identität kommen, die die Vorteile der Cloud erfolgreich integriert, aber die Kernleistung weiterhin lokal erbringt.

2. Kommunikations-Strategie 2020 im Mittelpunkt

Betrachtet man den Technologie-Mix aus Server, Speicher, Endgerät und Kommunikation, dann sind die ersten drei genannten Technologie-Bereiche relativ stabil im Sinne einer kontinuierlichen und ggf. etwas verlangsamten Evolution. Die aktuellen Analysen von ComConsult Research sehen aber einen dringenden Bedarf zur Positionierung der Kommunikations-Strategie für die nächsten 3 bis 5 Jahre. Dafür gibt es im Kern zwei Auslöser: All-IP und 5G auf der einen und mobile Endgeräte und Sensoren im Rahmen von IoT auf der anderen Seite. Diese beiden Auslöser werden insbesondere auf der Wireless-Seite eine neue Situation schaffen. Parallel dazu gibt es durch das Zusammenwachsen von WAN und Internet eine neue Form von "Corporate Network".

3. Skalierbarkeit in einem Technologie-Mix

Wenn wir über Strategien für die Zukunft sprechen, muss Skalierbarkeit in jedem Fall im Mittelpunkt stehen. Trotz einer verlangsamten Technologie-Entwicklung bei Servern und Speichern führt der Planungs-Aspekt Skalierbarkeit zu veränderten Produktentscheidungen, bei Speicher-Systemen gar zu veränderten Architekturen. In jedem Technologiebereich wird Skalierbarkeit zum dominanten Planungs-Kriterium. Die Frage ist, welche Ausprägung von Technologien hier einen wesentlichen Zugewinn bringen und wie diese zum Kern einer Zukunfts-Strategie beitragen können. Da wir gleichzeitig eine weiter zunehmende Abhängigkeit zwischen unseren Kern-Technologien haben, muss Skalierbarkeit auch Technologie-übergreifend gesehen werden. Schnell wachsende Kapazitäten bei Servern und Speichern erfordern zwangsläufig eine Anpassung auf der Kommunikationsseite. Skalierbarkeit in einem Technologie-Mix ist deshalb eine zentrale Herausforderung.

4. Sicherheits-Strategie 2020

Das Kernproblem aller Sicherheits-Lösungen ist die schnelle Anpassung an einen veränderten Bedarf. Skalierbarkeit im Technologie-Mix wird parallel zu einer Herausforderung für Sicherheit. Sowohl die Gefahren als auch die Lasten verändern sich in so hohen Geschwindigkeiten, dass eine statische Sicherheits-Lösung auf Dauer nicht den erforderlichen Grad an Sicherheit liefern wird. Auch im Sicherheits-Bereich brauchen wir ebenfalls eine erhebliche Skalierbarkeit, die im Rahmen eines Gesamtkonzepts flexibel mit dem Bedarf wachsen kann.

Fax-Anmeldung an ComConsult 02408/955-399

ComConsult Technologie-Tage

Ich buche den Kongress
ComConsult Technologie-Tage 2016

☐ 07.11.-08.11.16 in Köln - € 1.990,-- 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 ComConsult Technologie-Tage 2016

Montag 07.11.2016

9:30 - 10:30 Uhr
Keynote: Rechenzentrum kontra Cloud: Bausteine einer Zukunfts-Strategie für Rechenzentren
- Anforderungen an das Rechenzentrum der Zukunft
- Technologie-Situation der Basis-Technologien und Ausblick
- Abhängigkeiten zwischen Technologien und deren Handhabung
- Leistungs-Übersicht und Bewertung der Cloud
- Vor- und Nachteile: wer kann was besser, wo liegen die Nachteile
- Strategie für das erfolgreiche Rechenzentrum der Zukunft

Dr. Jürgen Suppan, ComConsult Research GmbH

10:30 - 11:15 Uhr
5G: Rückgrat der nächsten industriellen Revolution
- 5G: Anwendungsbereiche, Technologien und Bedeutung für Unternehmen
- Status von Komponenten, Szenarien und Standardisierung US und EU
- Starten statt Warten: LTE als Übergangstechnologie
- Aktuelle Entwicklungen von LTE Tel. 13 - 15 in 3GPP
- Anforderungen an unterstützende Infrastrukturen

Dr. Franz-Joachim Kauffels, Technologie-Analyst

11:15 - 11:45 Uhr Kaffeepause

11:45 - 12:30 Uhr
Das Software-Defined Data Center - Der Paradigmenwechsel in der IT
- Begriffsbestimmung: Was bedeutet Software-Defined?
- Virtualisierung plus SDN = Private Cloud?
- Technische und organisatorische Anforderungen und Erwartungen:
  - Virtualisierung von Sicherheitsfunktionen
  - Integration von Cloud- und Fog-Computing
  - Unterstützung für Anwendungen
  - organisatorische Anpassungen in der IT

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

12:30 - 14:00 Uhr Mittagspause

14:00 - 14:45
Wie Container das RZ verändern
- Was sind Container und wie funktionieren sie?
- Wie unterscheiden sich Container von klassischen Virtualisierungstechniken?
- Netzwerkschnittstellen von Containern
- Interaktion zwischen Containern und Microprozessen
- Container und DevOps: ein Herz und eine Seele?

Markus Schaub, ComConsult-Study.tv

14:45 - 15:30
Netzzugang zur Cloud
- Zugriff auf Public und Private Cloud
- Warum die Verbindung zum Internet immer wichtiger wird
- Braucht man noch ein Wide Area Network (WAN)?
- Software Defined WAN
- Wie die Umstellung auf Internet Protocol Version 6 (IPv6) sanfter als befürchtet erfolgen kann

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

15:30 - 16:00 Uhr Kaffeepause

16:00 - 16:45 Uhr
Das Ende von PSTN & ISDN
- Welche Änderungen ergeben sich aus der Umstellung?
- Was bieten die Provider?
- Welche Problem sind noch nicht eindeutig gelöst?
- Warum das Thema Session Border Controller wichtig ist

Markus Geller, ComConsult Research GmbH

16:45 - 17:00 Uhr
Zusammenfassung des Tages, Fragen Diskussion

17:00 - 18:00 Uhr
Den Schwarm führen: Organisations- und Führungsprinzipien für Innovation und Veränderung

Dipl.-Kfm. Lars Sudmann, Speaker & Trainer

Happy Hour ab 18:00 Uhr

Dienstag 08.11.2016 - vormittag

9:00 - 9:45 Uhr
Neubau von Rechenzentren
- Digitalisierung und die Auswirkungen für Rechenzentren
- Neue Trends im Rechenzentrumsumfeld
- Bauliche und technische Anforderungen/Security und Verfügbarkeit
- SPOC (Single Point of Contact)
- Energieoptimierungstrends
- Abwärmenutzung, Rechenzentren als dezentrales Kraftwerk

Klaus Dederichs, Drees & Sommer

9:45 - 10:30 Uhr
IoT-Sicherheit - aus Fehlern lernen und damit langfristig Erfolg sichern
- Plattform-Evolution zum Internet der Dinge
- Langfristiges Ziel: Vertrauen und Zuverlässigkeit
- Stand der Sicherheit an Beispielen: Babymonitoring, Industriesteuerungen, Automotive
- IoT der zweiten Generation - wie bekommt man die Risiken in den Griff?

Prof. Dr. Marko Schuba, Fachhochschule Aachen

10:30 - 11:15 Uhr
Funk – das Medium der Zukunft! Ist Ethernet tot?
- Wo steht Wireless LAN heute, wo geht es hin?
- Welchen Bedarf haben Anwendungen heute und in Zukunft?
- Welche Auswirkungen hat das auf Sicherheit?
- Welche Auswirkungen hat das auf die WLAN-Planung?
- Wie investieren Unternehmen zukunftssicher in Funktechnik?
- Weder WLAN noch Ethernet, ist Mobilfunk eine Alternative?

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

11:15 - 11:45 Uhr Kaffeepause

11:45 - 12:30 Uhr
EU Datenschutz-Grundverordnung - Datenschutz in neuer Dimension
- Gesetzgebungsgeschichte und Ziele der EU-Datenschutz-Grundverordnung
- Überblick zu den wichtigsten Regelungen für die Praxis (u. a. Extraterritorialer Anwendungsbereich, Erlaubnistatbestände, Auftragsverarbeitung, Drittstaatentransfers)
- Änderungen im Vergleich zum BDSG – was ändert sich, was bleibt gleich?
- Aufsicht, Sanktion und Haftung

Dr. Jan Byok, Bird & Bird LLP

12:30 - 14:00 Uhr Mittagspause

14:00 - 14:45 Uhr
Der Arbeitsplatz der Zukunft - (k)eine Frage der Endgeräte
- Was sind die bestimmenden Faktoren für den Arbeitsplatz der Zukunft?
- Welche Rolle spielen Endgeräte, Applikationen und Dienste für den Arbeitsplatz?
- Welche Dienste und Applikationen sind relevant für den Arbeitsplatz der Zukunft?
- Sind Standardisierungsbemühungen sinnvoll und erfolgversprechend?
- Welche Arbeitsplatzkonzepte adressiert der Markt heute schon?

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

14:45 - 15:30 Uhr
Informationssicherheit in und aus der Cloud
- Herausforderung sicheres Cloud Computing in Public Cloud, (virtual) Private Cloud und Hybrid Cloud
- Standardisierte und zertifizierte Cloud-Sicherheit
- Data Loss Prevention in der Cloud
- Virtuelle Sicherheits-Gateways und virtuelle Internet DMZ in der Cloud: Mehr als ein Trend!
- Rolle der Cloud bei der Abwehr von Distributed Denial of Service (DDoS)
- Abwehr zielgerichteter Angriffe durch Cloud-Dienste

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

15:30 - 16:15 Uhr
Herausforderungen an die Informationssicherheit in der Industrie 4.0
- Standards zur Sicherheit von IT im Industriebereich und die besondere Bedeutung von IEC 62443
- Warum die Industrie 4.0 nicht ohne Zonenkonzepte auskommt und welche Herausforderungen hier für Sicherheits-Gateways bestehen
- Warum eine starke Öffnung zum Internet notwendig ist und was sich an traditionellen Sicherheitskonzepten ändern muss
- Mit welchen Problemen durch die Industrie 4.0 für die sichere Administration und Überwachung der industriellen IT zu rechnen sind
- Virtuelle Fabrik: Nutzung von Cloud-Diensten in der Industrie 4.0
- Kann das gut gehen: Intelligente Maschinen entscheiden für Menschen?
- Masse statt Klasse: Fließender Übergang zum Internet of Things

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

Schwerpunktthema

DNSSEC und Zertifikate: Symbiose oder Widerspruch

Fortsetzung von Seite 1

Markus Schaub ist seit 2009 Leiter von ComConsult-Study.tv. Er verfügt über umfangreiche Berufserfahrung in den Bereichen Netzwerken und VoIP. Seine Schwerpunkte liegen im Netzwerk-Design, IP-Infrastrukturdiensten und SIP, zu denen er viele Vorträge auf Kongressen hielt, erfolgreich Seminare durchführte und zahlreiche Veröffentlichungen schrieb.

Schwachstellen von Zertifikaten

Das „Vertrauen“ im Internet basiert auf Zertifikaten. Gemäß dem Wiki von Mozilla vertraut der Firefox von Hause aus z. Zt. 174 Zertifikaten, die von 87 unterschiedlichen Organisationen ausgegeben werden. Zu diesen Organisationen gehören einige wenige Staaten wie „Staat der Nederlanden“, die meisten sind jedoch privatwirtschaftliche Unternehmen. So vertraut der Firefox bspw. „Unizeto Sp. z o.o.“, ich habe keinen Schimmer, wer das überhaupt ist, aber ich vertraue denen.

Von diesen „Root Zertifikaten“, die Programme wie Browser oder Email-Clients von Hause aus mitbringen, werden die Zertifikate abgeleitet, die unsere Internetkommunikation absichern sollen. Seien es Zugriffe auf Webseiten oder die Verschlüsselung von Emails. Wenn ich beispielsweise meine Homepage per HTTPS absichern möchte, so gehe ich wie folgt vor:

1. Ich generiere ein asymmetrisches Schlüsselpaar.
2. Den öffentlichen Schlüssel benutze ich, um daraus einen Certificate Signing Request (CSR) zu erstellen.
3. Mit dem CSR wende ich mich an eine Certificate Authority (CA), die diesen CSR dann mit ihrem privaten Schlüssel signiert.

Die „Güte“ eines Zertifikates hängt dann davon ab, was die CA bei der Signierung meines Schlüssels alles überprüft. Im einfachsten Fall wird nur überprüft, ob das Zertifikat von einem Server eingereicht wird, der zu der Domäne gehört, für die das Zertifikat ausgestellt werden soll. Die höchste Stufe der Zertifizierung ist die persönliche Vorstellung bei der CA zum Nachweis der Identität. Je nach Güte wird mal nur das „https“ im Browser grün oder es wird auffällig hervorgehoben, um zu zeigen, dass bei der Erstellung eines Zertifikates einer Seite besonders viel Sorgfalt angewendet wurde. Abbildung 1 zeigt je ein Beispiel für ein besonders „gutes“ Zertifikat und eines mit sehr geringer Güte.

Außer den eigentlichen Root CAs gibt es auch noch Zertifizierungsstellen, die von einer Root ein Zertifikat bekommen haben, mit dem sie wiederum andere Domains zertifizieren können. Prominentes Beispiel ist die Initiative „Let’s Encrypt“ (**https://letsencrypt.org/**) von der Internet Security Research Group (ISRG), die es sich zum Ziel gesetzt hat, die Verschlüsselung im Internet weiter zu verbreiten, indem der aufwendige Zertifizierungsprozess vereinfacht und automatisiert wird. Das Zertifikat dieser Initiative ist von der CA IdenTrust ausgestellt.

Zertifikate können korrumpiert werden, indem es bspw. einem Angreifer gelingt, an den privaten Schlüssel zu kommen. Aber auch bei bekannten Sicherheitsunternehmen wie „Symantec’s Thawte-branded CA“ kommt es zu Fehlern respektive zu Fehlverhalten (vgl. **https://security.googleblog.com/2015/09/improved-digital-certificate-security.html**). Es gibt eine

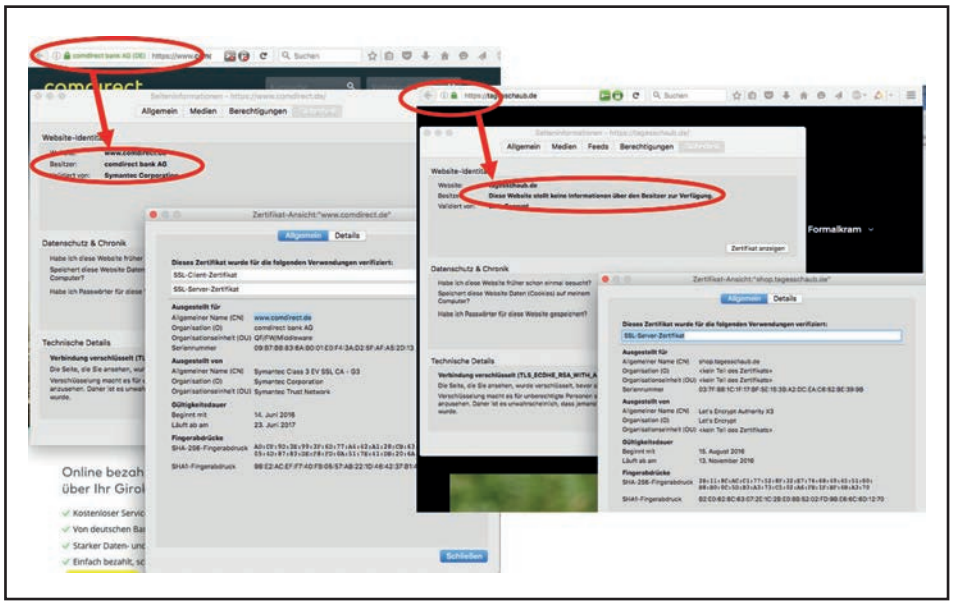

Abbildung 1: Zertifikate unterschiedlicher Güte

DNSSEC und Zertifikate: Symbiose oder Widerspruch

ganze Reihe von prominenten Beispielen, wo Zertifikate von Root CAs fehlerhaft ausgestellt wurden. Einige Beispiele sind:

- 2011 wird bei Comodo eingebrochen und für eine Reihe prominenter Internetfirmen werden daraufhin falsche Zertifikate ausgestellt (google, yahoo...)
- 2011 wird die Root-CA DigiNotar gehackt und es werden falsche Zertifikate für gmail und facebook ausgestellt.
- 2015 wird bekannt / vermutet, dass die chinesische CA CCNIC ebenfalls gefälschte Zertifikate signiert.
- 2015 stellt Comodo dem Inhaber der Email-Adresse hostmaster@live.fi ein SSL Zertifikat für den Inhaber Microsoft aus

Insgesamt kennt der RFC 5280 neun Gründe, aus denen ein Zertifikat zurückgezogen werden kann, zzgl. des Grundes „unspecified". Das ungültige Zertifikat wird dann auf eine Sperrliste (Revocation List") gesetzt und/oder mittels des moderneren „Online Certificate Status Protocol" (OCSP) zurückgezogen.

Schwachstellen im DNS

Nicht nur das aktuelle Zertifizierungsverfahren hat Schwächen. Dasselbe gilt auch für das DNS. Das DNS kann an verschiedenen Punkte angegriffen werden. Einige sind recht einfach, haben jedoch nur geringe Auswirkungen, da sie auf ein LAN begrenzt sind, andere greifen die Server selbst an. Diese sind ungleich schwieriger, aber - wenn sie gelingen - auch ungleich effektiver.

Beispiele für Angriffsverfahren sind:

- DNS Pakete abfangen
  Pakete abzufangen und somit abzuhören oder gar gefälschte Antworten zu geben, ist kein DNS-spezifisches Problem. Jedoch macht gerade das DNS es Angreifern sehr einfach, da die Kommunikation zwischen Client und Server meist nur aus einem Paket mit der Frage und einem weiteren mit der Antwort besteht. Das „klassische" DNS kennt dabei keinen Mechanismus, den Absender zu verifizieren oder die Integrität des Inhaltes gegen Änderungen zu schützen. Dasselbe gilt auch für die Server-Server-Kommunikation.

  Sicherheitsfunktionen anderer Ebenen wie dem IP in Form von IPsec sind samt und sonders überdimensioniert für das DNS. Der Verwaltungsaufwand und Overhead dieser Protokolle würde gerade die zentralen DNS-Server wie Root-Server, TLD-Server oder rekursive Server großer Provider schnell an ihre Grenzen bringen und anfällig gegen DoS-Angriffe machen. Zudem würde ein solches Modell nur eine Hop-by-Hop-Sicherung zulassen. D.h. der Enduser könnte nicht überprüfen, ob bei der Antwort, die er von seinem rekursiven DNS-Server bekommt, die Kette der Anfragen immer durch IPsec gesichert gewesen ist.

- ID raten und Fragen vorhersehen
  Da zwischen Fragendem und Gefragten (Client-Server, Server-Server) kein Verbindungsaufbau stattfindet und die Fragesteller meist viele Fragen offen haben, wird jede Frage mit einer ID versehen, die der Antwortende wiederholt. So kann der anfragende Resolver eine Antwort einer offenen Frage zuordnen und diese dann als beantwortet abhaken.

  Die Idee des ID Guessing ist es diese IDs vorherzusehen. Das alleine bringt einen Angreifer nicht weiter, denn er muss ja auch die Frage kennen, die zu einer ID gehört, denn ansonsten passt seine Antwort nicht zu der Frage und diese wird in den Antworten ebenso wiederholt wie die ID.

  Im Alltagsgeschäft ist es also fast unmöglich vorherzusagen, welche DNS Frage ein Client stellen wird und welche ID dazu gehört. Jedoch gibt es Situationen, bei denen das einfacher ist, als man vielleicht zunächst denkt, dazu gehört bspw. der Neustart eines Systems. Dieser folgt einem vorgegebenen Ritual beginnend mit DHCP – oder PPPoE, wenn man mit Port-Security arbeitet, und arbeitet sich anschließend einmal quer durch die AD-Landschaft (Controler, Kerberos-Server). Bei Telefonen ist es noch schlimmer, die suchen oft ihren Konfigurationsserver.

  Betrachtet man das Beispiel mit dem Telefon, wird klar, welchen Schindluder ein Angreifer mit einem gefälschten DNS-Paket anrichten kann: jubelt er dem Telefon den falschen Konfigurationsserver unter und wird die Konfiguration über das ungesicherte TFTP übertragen, so ist es ein Leichtes Gespräche abzuhören.

  Wo ist der Unterschied dieses eher aufwendigen Verfahrens (richtiges Raten von IDs und Fragen) verglichen mit dem ersten Angriffsmodel, dem Abfangen der Pakete? Dieses Verfahren funktioniert auch remote, d.h. wenn man sich nicht irgendwo in die Transferstrecke der DNS-Antworten einklicken kann. Ein Resolver wird die erste DNS-Antwort akzeptieren, die er bekommt und die Frage danach vergessen. Bekommt er später die Antwort vom richtigen DNS-Server, kann er sie bereits nicht mehr zuordnen und wird sie entsprechend verwerfen.

- Name Chaining / DNS Spoofing / Cache Poisoning
  Unter Name Chaining werden vom RFC 3833 verschiedene Formen von Attacken auf das DNS zusammen gefasst,

denen allen gemein ist, dass sie darauf beruhen DNS-Servern mittels Domain-Namen in DNS-Antworten falsche Informationen unterzujubeln.

Das bekannteste Beispiel ist wohl der von Eugene Kashpureff aus dem Jahr 1997, als es ihm gelang eine Reihe großer Cache Server zu „vergiften“, indem er einen bereits bekannten Bug des BIND ausnutze.

Das Vorgehen dabei ist typisch für Name Chaining Angriffe: ein Cache Server fragt einen anderen, korrumpierten DNS-Server. Zusätzlich zu der eigentlichen Antwort erhält er weitere Informationen. Beispiel: gefragt wird nach www.comconsult-akademie.de. Zusätzlich zur korrekten IP dieser Domain bekommt der Server in den Additional Records noch eine falsche IP Adresse www.comconsult-study.tv genannt. Diese speichert er. Sucht nun jemand nach www.comconsult-study.tv landet er auf der falschen Seite, da der Server die falsche Adresse in seinem Cache gespeichert hat und bei den Nameservern von comconsult-study.tv gar nicht erst nachfragt.

Dieses einfache Vorgehen ist natürlich schon seit rund 20 Jahren nicht mehr möglich, aber seitdem gibt es viele Variationen davon. Die meisten davon beruhen darauf, auf falsche Namen zu verweisen, beispielweise per CNAME Einträgen, daher der Name „Name Chaining“.

Auch wenn der RFC, der diese Angriffsvariante beschreibt, in die Jahre gekommen ist (von 2004), ist er bis heute aktuell. So gibt Microsoft beispielsweise an, dass im Zeitraum von Mai 2012 bis Juni 2013 17 ihrer registrierten Länderdomains zeitweilig korrumpiert waren (vgl. **https://blogs.microsoft.com/microsoftsecure/2014/02/04/threats-in-the-cloud-part-1-dns-attacks/**)

Ablauf von DNSSEC

Das Grundprinzip von DNSSEC ist – wenig überraschend – identisch mit dem von Zertifikaten: es gibt eine Root, deren öffentlicher Schlüssel wohl bekannt ist. Mit dem dazu passenden, geheimen Schlüssel können DNS Einträge signiert werden. Anders als bei Zertifikaten gibt es im DNS jedoch so etwas wie eine „natürliche Ordnung“, da das DNS hierarchisch ist. Statt unzähliger Root-CAs gibt es im DNS genau eine Root: „.“. Zwar gibt es unzählige Root-Server, deren Informationen sind jedoch identisch.

Diese Root bestätigt die Echtheit der so genannten Top Level Domains (TLD), also .org, .de, .info usw. Diese wiederum können dann ihrerseits die Echtheit der Second Level Domains bestätigen, wie bspw. tagesschaub.de, welche ihrerseits damit ihren eigenen Namespace signieren können.

Schauen wir uns im Folgenden das Verfahren etwas detaillierter an:

Am Anfang ist die Root. Für deren Inhalte (nicht Betrieb) ist das Internet Corporation for Assigned Names and Numbers (ICANN) verantwortlich. Dieses hat in einer „Zeremonie“ 2010 das asymmetrische Schlüsselpaar für die Root generiert. Die nächste Zeremonie findet 2017 statt.

Dabei wurde der so genannte Key Signing Key (KSK) erzeugt. Der KSK hat nur eine Aufgabe: andere Schlüssel zu signieren (vgl. Abbildung 2). Davon zu unterscheiden sind die Zone Signing Keys (ZSK). Mit diesen Schlüsseln werden alle anderen Resource Records (RR) einer Zone unterschrieben (vgl. Abbildung 3).

Mit diesem Root-KSK werden die Schlüssel der TLDs nun signiert, ebenso wie der ZSK der Root-Zone selbst. Aktuell sind nicht alle TLD-Zonen signiert, also nicht

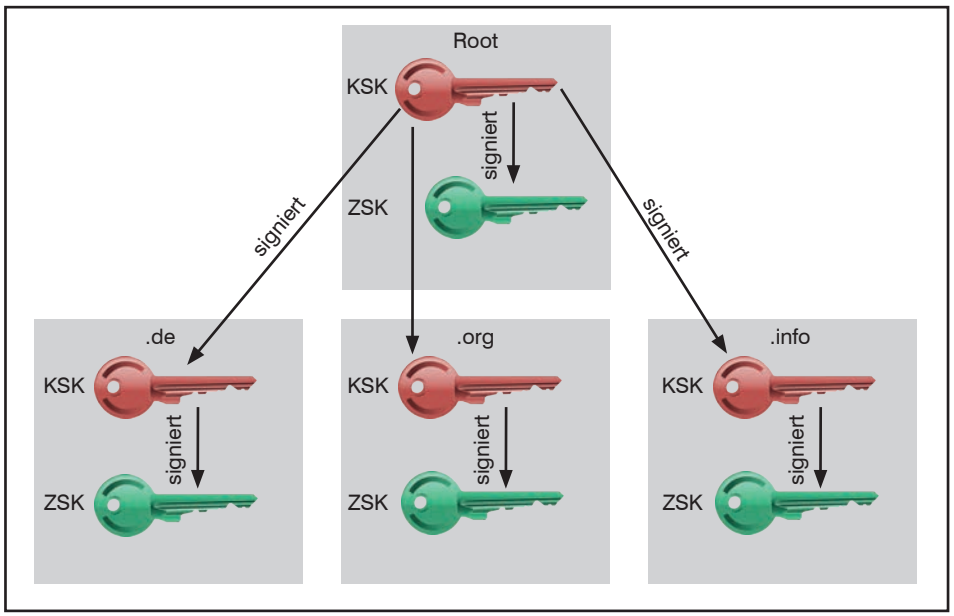

Abbildung 2: Unterzeichnung von Schlüsseln senden

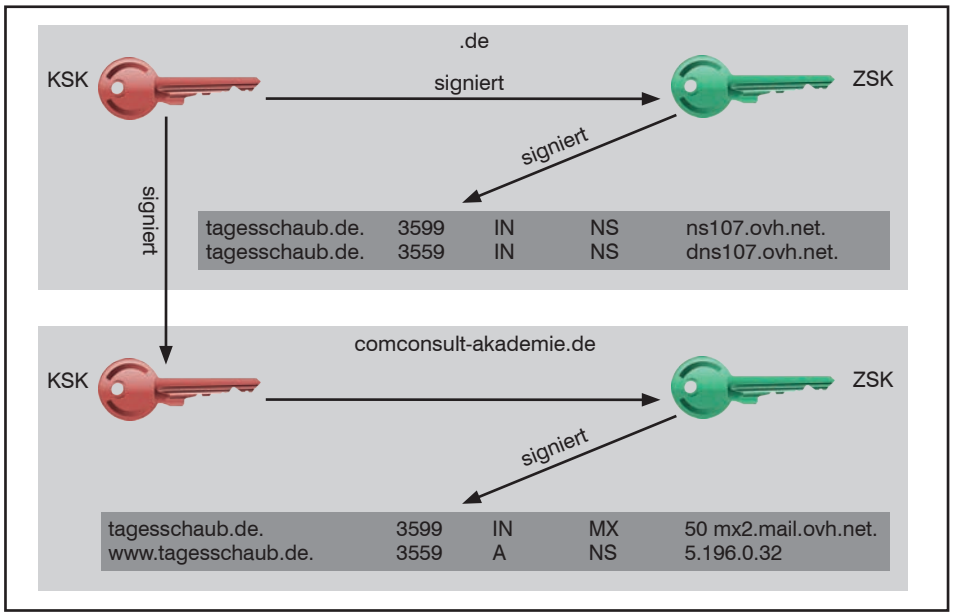

Abbildung 3: Unterzeichnung von Zonen-Daten

alle sind bereits auf DNSSEC umgestiegen. Für die de-Zone ist das jedoch der Fall. Wenn ich also meine Domaine ebenfalls auf DNSSEC umstellen möchte, so kann ich ein asymmetrisches Schlüsselpaar erzeugen und den öffentlichen Schlüssel vom DENIC unterschreiben lassen. Damit habe ich einen KSK für meine Domain.

Dann geriere ich ein weiteres Schlüsselpaar, das ZSK. Dessen öffentlichen Schlüssel unterschreibe ich dann mit dem geheimen Schlüssel meines KSK.

Die öffentlichen Schlüssel werden in der Zonendatei mit dem neuen Record-Typen DNSKEY hinterlegt. (siehe Abbildung 4)

Der KSK ist der Schlüssel mit der 257, der ZSK mit der 256. Das mag sich eines Tages noch ändern, da diese Zahlen durch das Setzen resp. Nicht-Setzen eines bestimmten einzelnen Bits zustande kommen. Die 3 und die 7 geben die Verfahren für Verschlüsselung und das Hashing an.

Warum nun diese Trennung von KSK und ZSK?
Grundsätzlich ist es sinnvoll, den geheimen Schlüssel, mit dem die Zoneneinträge signiert werden, nicht auf dem System zu hinterlegen, auf dem auch die Zonendatei selbst liegt. Jedoch gibt es Situationen, bei denen es technisch nicht anders geht oder es unsinnig ist, diesen im Tresor zu lagern. Ein Beispiel dafür ist das dynamische DNS (DDNS). Jedes Mal, wenn ein Client seinen Eintrag ändert oder neu anlegt, muss dieser neu signiert werden, dafür benötigt der Server den ZSK. DDNS ist somit ein Beispiel dafür, dass es sinnvoll ist, zwischen dem KSK und ZSK zu unterscheiden. Denn den „wichtigeren“ ZSK kann man im Tresor belassen und nur hervorholen, wenn ein neuer ZSK erzeugt wurde. Wird nämlich der geheime ZSK korrumpiert, weil auf meinen DNS-Server eingebrochen wurde, kann ich den Schlüssel einfach austauschen, ohne die Peinlichkeit das auch noch beim DENIC angeben zu müssen.

Ein weiterer Grund für die Trennung liegt darin, dass die Sicherheitsprinzipien eines Unternehmens sich von denen des NIC oder gar der Root unterscheiden. Will ein Unternehmen bspw. die Schlüssel jährlich austauschen, so ist das mit dem ZSK einfach möglich, ohne dass eine erneute Signierung durch das NIC notwendig wäre.

Um das System weiter abzusichern, wird nicht nur der KSK von der übergeordneten Domain unterschrieben, sondern bei der übergeordneten Domain wird auch ein Fingerabdruck dieses Schlüssels hinterlegt. Auf diese Weise kann ein noch gültiger Schlüssel zurückgezogen werden. Beispiel:

```
dig dnskey tagesschaub.de
tagesschaub.de.      3599    IN       DNSKEY     256 3 7
                                       AwEAAd/DPDvPSvjhMQhUZ...
tagesschaub.de.      3599 IN       DNSKEY 257 3 7
                                       AwEAAaX7wWIUxCL/Y1wBxu1...
```

Abbildung 4: Öffentliche Schlüssel (KSK und ZSK) im DNS

```
dig ds tagesschaub.de

tagesschaub.de.      21599  IN     DS     34293 7 2 530EC52A...
```

Abbildung 5: Beispiel für einen hinterlegten Schlüssel-Hash

```
dig +dnssec aaaa www.tagesschaub.de

www.tagesschaub.de.  3599   IN AAAA 2001:41d0:52:300::9b8
www.tagesschaub.de.  3599   IN RRSIG AAAA 7 3 3600
                     20161004100018 20160904100018 17207
                     tagesschaub.de.
                     RLeKV7YvS+S5S38qJyiStq3PdlzRLaJA8jJoNFBlvfc8p
                     YEqmOdyE6d3 Oshyya1pBXYNUc
```

Abbildung 6: Beispiel für eine Signatur mittels RRSIG

Dier Fingerprint des aktuell gültigen KSK wird als DS-Record hinterlegt.

Das Besondere dieses RR ist, dass hierfür die althergebrachten Regeln des DNS geändert werden mussten: für gewöhnlich liegen alle Inhalte einer Zone in einer Zonendatei bei den zuständigen DNS-Servern. Das gilt nicht für den DS Record. Damit das System funktioniert, liegt er **ausschließlich** bei der übergeordneten Instanz. Im Falle von tagesschaub.de also beim DENIC.

Was mit diesen bisher beschriebenen Maßnahmen erreicht wurde, ist, dass es eine „Chain of Trust“, eine Vertrauenskette, gibt: wenn ich der Root vertraue und diese dem DENIC, dann vertraue ich auch dem DENIC. Da das DENIC wiederum der Domain tagesschaub.de vertraut, vertraue ich auch dieser Domain, usw.

Was noch fehlt, ist die Signatur der eigentlichen Inhalte. Denn was wirklich interessiert, ist ja, dass ich nachher eine IP Adresse oder einen Mailserver dieser Domain genannt bekomme und darauf vertrauen kann, dass diese spezifische Information korrekt ist. Dafür wird ein weiterer Typ eingeführt der RRSIG (Ressource Record Signature).

Das Beispiel zeigt: fordert man neben der eigentlichen Information – hier der IPv6 Adresse – auch noch die dazugehörigen DNSSEC Daten, so bekommt man zusätzlich zum AAAA Record noch den dazugehörigen RRSIG zurück geliefert.

Der RRSIG enthält neben der Unterschrift, das ist der Hash am Ende, noch weitere Informationen:

- Das genutzte Unterschriftsverfahren
  Im Beispiel ist das eine Kombination aus RSA und SHA, gekennzeichnet durch die 7 hinter AAAA.

- Anzahl der Namenskomponenten
  Hier 3: www, tagesschaub, de

- Das originale TTL
  Hier 3600. Da bei der Signatur ein Hash über den Eintrag gebildet wird, muss derjenige, der den Hash überprü-

fen will, alle Angaben kennen. Das TTL, das er genannt bekommt, kann jedoch von dem originalen abweichen, da ein Cache-Server das TTL herunter zählt, solange der Eintrag in seinem Cache liegt.

- Die Gültigkeitsperiode der Unterschrift
  Diese Signatur ist gültig bis 20161004100018 und zwar seit 20160904100018. Also vom 04. September bis 04. Oktober 2016.

- Ein Tag zur Schlüsselidentifizierung (Key Tag)
  Wird bspw. der Schlüssel vor Ablauf seiner Gültigkeit geändert, so können durch das Caching von DNS Einträgen noch alte Signaturen im Umlauf sein. Die Gültigkeitsperioden des neuen und des alten Schlüssels sollten sich somit um mindestens die Dauer des längsten TTL einer Zone überschneiden. Damit ein Client den „richtigen" Schlüssel wählt, kann er den mittels Key Tag identifizieren, wenn mehr als einer im Umlauf ist.
  Ungültige/Abgelaufene Schlüssel müssen natürlich verworfen werden.

- Der Besitzer (Owner)
  Der Owner ist der Besitzer des Schlüssels, also die Zone. In diesem Fall ist das tagesschaub.de.
  Interessant wird es bei Einträgen wie www.test.tagesschaub.de, denn dann könnte der Owner test.tagesschaub.de sein, aber auch tagesschaub.de, je nachdem, ob eine Delegation stattgefunden hat oder nicht.

Bleibt noch ein Problem zu lösen: wie kann man gesichert sagen, dass es einen gesuchten Eintrag **nicht** gibt? Einen allgemeingültigen Eintrag zu generieren, der schlicht „nein" sagt, geht nicht, da dieser beispielsweise durch Replay Attacken einfach zu einem Denial of Service genutzt werden könnte. On-the-Fly eine Signatur zu generieren ist aufwendig und würde einfache Denial-of-Service Angriffe gegen einen DNS-Server ermöglichen, indem man diesen überlastet. Der gewählte Lösungsansatz sieht wie folgt aus:

- Die Zone wird zunächst sortiert (canonical order)

- Zu jedem Eintrag wird ein weiterer Eintrag erzeugt, der angibt, wer der nächste in der Liste ist. Das ist der NSEC-Record

- Wird ein nicht existenter Name gesucht, bekommt man den NSEC-Record des vorhergehenden Eintrags genannt.

Beispiel: es gibt a.tagesschaub.de und c.tagesschaub.de. Sucht nun jemand nach b.tagesschaub.de bekommt er als Antwort, dass der Nachfolger von a c ist. Damit ist dem Suchenden klar, dass es b nicht gibt.

```
dig b.tagesschaub.de +dnssec

;; AUTHORITY SECTION:
TL8U8870SC8KRP5RD4NAC1IUD9QIK8AG.tagesschaub.de. 299 IN    NSEC3 1 0 8
                                B0B165692F55397B 4D2OBHG...
TL8U8870SC8KRP5RD4NAC1IUD9QIK8AG.tagesschaub.de. 299 IN    RRSIG NSEC3
                                7 3 300 20161004100018 20160904100018
                                17207 tagesschaub.de. s9e5xKwE4vZv...
4D2OBHGFJTUI8KORDEGHM76RS3HS7SKV.tagesschaub.de. 299 IN    NSEC3 1 0 8
                                B0B165692F55397B
                                6DCSTPDLA68OA3EMQ0FOAML393342IFK
                                SRV RRSIG
4D2OBHGFJTUI8KORDEGHM76RS3HS7SKV.tagesschaub.de. 299 IN    RRSIG NSEC3
                                7 3 300 20161004100018 20160904100018
                                17207 tagesschaub.de.
```

Abbildung 7: Beispiel für NSEC3-Antwort inkl. dazugehöriger RRSIG Records

Dieser Ansatz löst zwar das Problem, wirft aber ein neues auf: mittels der Suche nach nicht existenten Domainnamen ist es einfach sehr schnell alle Domain Namen zu finden, die es in der Domain gibt. Das ist häufig aber nicht gewollt.

Darum wurde der ursprüngliche NSEC Record durch den neuen NSEC3 Record abgelöst.

Dabei bleibt das Grundprinzip erhalten: wird b gesucht, dann bekommt man als Antwort, dass der Nachfolger von A C ist, nur wird das nicht mehr so klar ausgesprochen. Statt A und C im Klartext zu nennen werden die Namen als „gesalzener" Hash zurückgegeben. Somit kann der Anfragende nicht herausfinden, welche Namen sich hinter den Hashes wirklich verbergen.

Auch die NSEC3 Records werden signiert, sprich es wird ein dazugehöriger RRIG Record erzeugt.

Natürlich nützt es nichts, wenn die Einträge im DNS signiert werden und niemand nach den Signaturen fragt. Es reicht also nicht, dass nur die Server DNSSEC unterstützen, auch die Resolver müssen es machen und irgendwie muss die genutzte Software das Ergebnis an den Enduser übermitteln.

Die Standards sehen zwei Varianten vor. Zum einen den security-aware Resolver. Dieser kann die Signaturen selbst überprüfen. D.h. er kennt den Root-Schlüssel und kann die Chain of Trust selbst nachbilden. Dazu muss er über kryptographische Fähigkeiten verfügen und häufig mehr als eine Anfrage stellen, um die notwendigen DNSKEY und DS Einträge abzufragen. Dabei können ihm irgendwelche Middleboxen in die Quere kommen. Gemeint sind Firewalls, IDS oder rekursive Nameserver, die entsprechende Anfragen blockieren. In diesen Fällen überlasst es der Standard lokalen Sicherheitsrichtlinien, wie ein Resolver respektive eine Software zu reagieren hat.

Neben dem security-aware Resolver gibt es noch den security-aware Stub-Resolver. Stub-Resolver sind die Regel bei Clients. Sie lösen die Namen nicht selbst auf, sondern wenden sich an einen rekursiven Nameserver, der die Arbeit für sie übernimmt und sich bei Bedarf durch den DNS-Baum bis zur gewünschten Antwort hangelt. Dieses Prinzip wird für den security-aware Stub-Resovler beibehalten und um die notwendigen Sicherheitsprüfungen ergänzt. Der Resolver signalisiert dem Server dazu, dass er eine Sicherheitsüberprüfung wünscht, dazu setzt er ein Bit, das DO Bit (DNSSEC OK) im erweiterten DNS Header. Der Server setzt in seiner Antwort das Authenticated Data (AD) Bit, wenn die Authentifizierung gelungen ist, wenn sie fehlschlug oder nicht möglich war, setzt der Server das entsprechende Bit nicht. Einen Grund, warum die Sicherheitsüberprüfung fehlschlug, nennt er jedoch nicht.

Sinn macht das mit den security-aware Stub-Resolvern natürlich nur, wenn die Verbindung zwischen Resolver und rekursivem Nameserver sicher ist. Wie das geschehen kann, lässt der Standard offen. Ob sie nun nach guter alter Manier davon ausgehen, dass ihr LAN sicher ist, IPsec verwenden oder auf DNS-eigene Mittel wie TSIG und dessen Derivate vertrauen, bleibt dem Betreiber überlassen.

Bleibt noch die Frage: wie merkt der

User eigentlich, ob eine Domain mittels DNSSEC gesichert wurde und wenn ja, ob die Überprüfung funktioniert hat?

Genau das ist zur Zeit der wohl größte Schwachpunkt. Anders als bei Zertifikatsüberprüfungen bringen Browser oder andere Software wie Email-Server und -Clients diese Fähigkeit von Hause aus nur in Ausnahmefällen mal mit. Bei den Mailservern wäre hier Postfix zu nennen. Für die Browser sieht es mau aus. Es gibt Plug-Ins für Firefox und Chrome. Aktuell funktioniert das für Chrome allerdings nicht. Eine erfolgreiche DNSSEC Überprüfung beim Firefox ist in Abbildung 8 dargestellt.

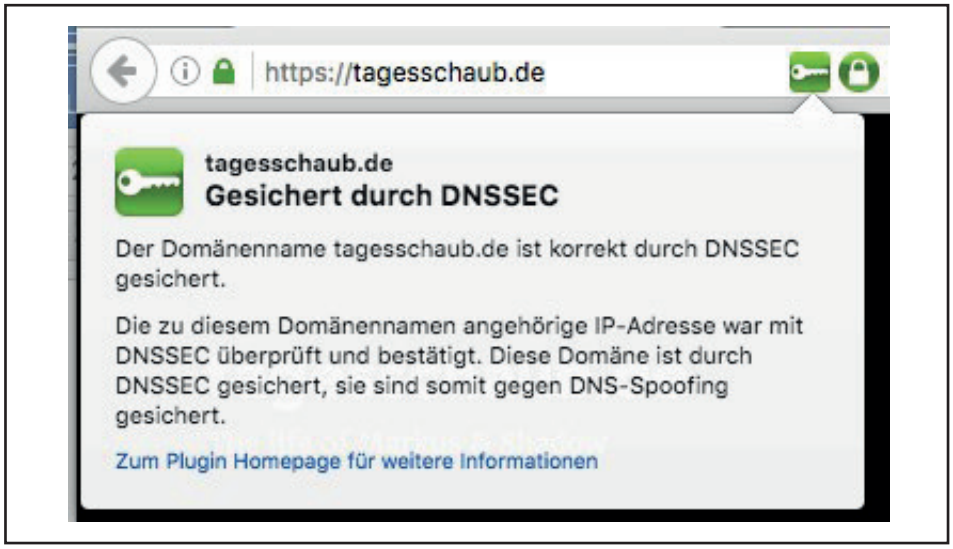

Abbildung 8: Firefox Plug-In für DNSSEC

Bewertung von DNSSEC

Der Clou ist, dass man für jede Instanz nur Instanzen signieren darf, die im DNS-Baum unter ihr aufgehängt sind. Das DENIC darf also comconsult-akademie.de signieren, nicht aber comconsult-study.tv, dafür wäre die TLD-Autorität von .tv notwendig. Auf diese Weise ist es technisch nicht mehr nötig einer unüberschaubaren Anzahl von Organisationen vertrauen zu müssen, sondern es reicht, der Root zu vertrauen, um die Chain of Trust vollständig überprüfen zu können. Wesentlich ist das Wort „technisch“, denn ob man jedem Unternehmen, das eine TLD verwaltet und jedem Staat mit Länderkennung vertraut, bleibt natürlich dem User weiterhin überlassen. Aber anders als bei Zertifikaten kann es nur noch **eine** Instanz geben und damit auch nur **eine** gültige Signatur. UK kann comconsult-akademie.de eben nicht signieren, wohingegen jede Organisation, die über ein Root Zertifikat verfügt, es kann.

Bliebe die Frage, ob man der Root vertraut. Da hat man nur zwei Varianten: entweder man traut ihr oder man faltet sich einen Aluhut. Denn wenn die Root des DNS kompromittiert ist, dann war es das mit dem DNS ohnehin. In diesem Fall können Sie in Ihren Browser eintippen, was sie wollen, nicht mal mehr Ihrer Lieblingsverschwörungstheoriewebseite können Sie dann noch trauen.

Die eigentliche Frage ist aber gar nicht, ob man der Root traut oder nicht, sondern was DNSSEC eigentlich bringt.

Selbst in Deutschland lässt sich da feststellen: erstmal ziemlich wenig.

Bei DNSSEC wird mittels einer „Chain of Trust“ garantiert, dass eine Information zu einer DNS-Domain authentisch ist und während der Übertragung nicht gefälscht wurde. Was DNSSEC nicht garantiert, ist, dass die Domain selbst vertrauenswürdig ist und auch nicht, dass die Inhaberdaten korrekt sind. Zur Erinnerung nochmal das Beispiel www.tagesschaub.de (vgl. Abbildung 9).

Die Chain of Trust kann in diesem Fall komplett überprüft werden. Damit ist garantiert, dass www.tagesschaub.de die IP Adresse 2001:41d0:52:300::9b8 hat. Wer jedoch dieser ominöse Tagesschaub ist, wissen Sie nicht. Das können Sie zwar beim DENIC nachschlagen, aber dort „Müll“ zu hinterlegen ist einfach: mit dem DENIC hatte ich selbst nie Kontakt, nur mit meinem DNS Provider und der prüft nur seine Kontoauszüge, nicht meine Identität.

Weltweit wird das noch unglaubwürdiger: können Sie sich sicher sein, dass www.microsoft.info wirklich die Firma Microsoft aus Redmond ist und nicht irgendein Spaßvogel?

Fassen wir zusammen:

- Zertifikate garantieren die Authentizität des Seitenbetreibers und ermöglichen die Verschlüsselung der Übertragung. Allerdings gibt es viele, die „glaubwürdige“ Zertifikate ausstellen können und der Seitenbetreiber hat keine Möglichkeit einem User mitzuteilen, welches Zertifikat wirklich echt ist.
- DNESSEC garantiert die Authentizität und Integrität von DNS Informationen aller Art. Mehr aber auch nicht.
  Wenn man beides kombiniert, indem man die Echtheit eines Zertifikates mittels DNS sicherstellt, kommt man einen Schritt weiter. Das ist der Ansatz von DANE.

DANE

Die Idee hinter DNS-based Authentication of Named Entities kurz DANE ist es, dem User mittels DNS mitzuteilen, welche Bedingungen ein Zertifikat erfüllen muss, damit es echt ist.

Dafür stehen mehrere Möglichkeiten zur Verfügung, aus denen man die für seine Situation passende auswählen kann:

1. Der Betreiber der Webseite gibt dem User mittels DNS an, welche CA er gewählt hat. Diese CA muss dem User bekannt sein, oder zumindest muss sie von einer ihm bekannten Root CA signiert sein.
   Stellt nun eine andere CA ein Zertifikat für diese Webseite aus, würde das Zertifikat von einem Client, der DANE nutzt, nicht akzeptiert werden.

2. Das Server-Zertifikat wird spezifiziert und der Client wird angewiesen, zu prüfen,

```
dig +dnssec aaaa www.tagesschaub.de

www.tagesschaub.de.  3599   IN     AAAA   2001:41d0:52:300::9b8
www.tagesschaub.de.  3599   IN     RRSIG  AAAA 7 3 3600
20161004100018 20160904100018 17207 tagesschaub.de.
```

Abbildung 9: DNS Antwort mit DNSSEC Signatur

```
dig tlsa _443._tcp.tagesschaub.de +dnssec

_443._tcp.tagesschaub.de. 59 IN TLSA 2 1 2 774FAD8C9A6AFC2...
_443._tcp.tagesschaub.de. 59 IN RRSIG TLSA 7 4 60 20161008131551
                              20160908131551 17207 tagesschaub.de.
                              U8Wx3PcYgoQXDjD...
```

Abbildung 10: Beispiel für einen TLSA Record

ob dieses Zertifikat auch von einer ihm bekannten CA unterschrieben wurde.

3. Es wird auf eine CA verwiesen, die das Zertifikat unterschrieben hat. Der Client prüft zwar die Unterschrift der CA, jedoch ist es egal, ob er die CA selbst kennt oder nicht.

4. Das Server-Zertifikat selbst wird spezifiziert, eine CA wird nicht genannt.

Betrachten wir kurz vier Anwendungsfälle, dann werden diese Varianten deutlicher:

Fall 1: Automatischer Zertifikatsaustausch
Momentan versuchen Cisco, Mozilla, OVH und einige andere große Unternehmen, die irgendwie mit dem Internet zu tun haben, Verschlüsselung von Webseiten so weit zu vereinfachen wie möglich. Das Projekt heißt Let's Encrypt. Wer daran teilnimmt bekommt Tools an die Hand gegeben, die mehr oder weniger automatisch ein Webserverzertifikat erstellen, einpflegen und regelmäßig austauschen. Im regelmäßigen Austausch liegt nun das Problem: ändert sich das Zertifikat, bekommt der User entweder nichts davon mit oder zu spät. D.h. würde man einen Fingerprint des Server-Zertifikates im DNS hinterlegen, hätte man ein Problem. Hier bietet es sich an die erste oder dritte Option zu wählen, da sich die CA hoffentlich nicht ändert. Allerdings muss man auch in diesem Fall prüfen, ob sich das CA-Zertifikat geändert hat. Das dürfte deutlich seltener der Fall sein.

De facto wählen in diesem Fall die meisten die dritte Option, denn diese Variante ist etwas für private User. Diese prüfen nicht regelmäßig, ob die CA noch in allen Browsern vorhanden ist oder nicht.

Fall 2: Selbst erzeugte Zertifikate
Gerade in Unternehmen wird intern mit lokalen Zertifikaten gearbeitet, die von keiner CA unterschrieben wurden und denen trotzdem vertraut werden soll. Dann kann man zwar ein eigenes Root Zertifikat auf allen Systemen ausrollen, das macht aber unter Umständen wenig Spaß oder ist schlicht nicht möglich.

In diesem Fall bietet sich Option 4 an: im DNS wird ein Fingerprint des Server-Zertifikates hinterlegt und der Client wird informiert, dass es völlig egal ist, ob und wer dieses Zertifikat unterschrieben hat.

Fall 3: Öffentlicher Unternehmenswebserver
Für (viel) Geld hat man ein Zertifikat bei einer CA signieren lassen, dass die kommenden N Jahre gültig ist. Da dieser Prozess nicht automatisch ist, weiß man, wann das Zertifikat ausgetauscht wird.

Abbildung 11: DANE Überprüfung mit Firefox Plug-In

Damit ist Option 2 perfekt: man nennt dem Client den Fingerprint des eigenen Zertifikates und weist ihn an, auch den gesamten Pfad inkl. der CA zu prüfen. Das ist die höchste Stufe der Sicherheit, aber auch die am wenigsten flexible.

DANE kennt noch zwei weitere Parameter:
1. Was wurde gehashed
   Der Standard sieht dafür zwei Möglichkeiten vor:
   a. Gesamtes Zertifikat
      Die Daten des gesamten Zertifikates werden genutzt.
   b. Public Key + Algorithmus
      Es wird nur ein Hash über den Public Key und den Algorithmus gebildet.

2. Das Hashing Verfahren
   Hier gibt es bislang drei Varianten
   a. Es wird gar nicht gehashed, stattdessen wird das gesamte Zertifikat per DNS übermittelt.
      Dieses Verfahren wird nicht empfohlen und ist eigentlich auch unsinnig, da das Zertifikat ohnehin über andere Protokolle übertragen wird (bspw. TLS). Bei DANE geht es schließlich nur darum, sicher zu stellen, dass das Zertifikat echt ist, nicht um einen Zertifikatstausch.
   b. SHA-256
   c. SHA-512

Um das DANE Verfahren nun noch in das DNS zu integrieren bedarf es eines neuen Ressource Records. Das ist der TLSA Record (vgl. Abbildung 10). TLSA steht übrigens nicht für TLS Authenticator oder Ähnliches, es steht für gar nichts. Es ist ein Akronym, das keines ist.

Als Beispiel musste bislang die Absicherung von Webseiten herhalten. DANE ist aber nicht darauf beschränkt. Vielmehr kann man es für jede Zertifikats-basierte und an DNS-Namen gebundene Kommunikation nutzen, also bspw. auch für Mail. In der Tat sind es gerade einige Mail-Provider, die DANE aktiv im Einsatz haben, wie Posteo, mail.de oder mailbox.org und einige mehr.

Da für verschiedene Dienste durchaus verschiedene Zertifikate genutzt werden können und auf einem Server mehrere Dienste parallel laufen können, benötigt man für DANE noch eine Dienstunterscheidung. Dafür werden Port und Protokoll genutzt. Der TLSA-Eintrag ähnelt somit einem SRV Ressource Record, da dem eigentlichen Namen noch diese beiden Informationen vorangestellt werden. Vollständig sieht das Ganze dann wie Abbildung 10 aus.

Wie schon bei DNSSEC macht DANE

nur dann wirklich Sinn, wenn Erfolg oder Misserfolg für den User transparent gemacht wird. Dasselbe Firefox Plug-In, das DNSSEC überprüft, kann auch DANE validieren. Abbildung 11 zeigt die erfolgreiche Verifikation eines Zertifikates. Das Plug-In gibt auch an, was geprüft wurde, im Beispiel wurde die der Fingerprint des CA-Zertifikates angegeben und der gesamte Zertifikatspfad geprüft.

Bewertung

Diejenigen, die mit diesem Verfahren das Ende der CAs kommen sehen, beziehen sich ausschließlich auf den 4. Fall der DANE-Prüfverfahren, bei dem nur ein Fingerprint des Zertifikates im DNS hinterlegt wird und eine Überprüfung der Zertifikatskette unterlassen werden soll. Damit ist es in der Tat möglich, ein selbst erstelltes Zertifikat zu nutzen und im DNS für gültig zu erklären. Die Sicherheitsstufe, die damit erreicht wird, entspricht derjenigen, wie sie bspw. von Let's Encrypt erreicht wird: der Nutzer kann sich sicher sein, dass das Zertifikat zu der Domain gehört, mit der er redet (DANE) und dass auch die IP Adresse zu genau dieser Domain gehört (DNSSEC). Mehr aber auch nicht. Wie bereits geschrieben, das DENIC hat meine Identität nie geprüft.

Für viele Webseiten wäre das wahrscheinlich auch völlig ausreichend, wenn es nur darum geht, sicher zu stellen, dass mein Passwort für irgendein x beliebiges Forum sicher übertragen wird, reicht mir das. Für Online-Banking ist das sicherlich nicht zufriedenstellend. Für höhere Sicherheitsansprüche werden Zertifikate weiterhin unerlässlich sein. Aber wenn eben diese gesteigerten Sicherheitsansprüche erfüllt werden sollen, bieten DNSSEC und DANE eine ausgezeichnete – und kostenfreie – Ergänzung zur bestehenden Zertifikatsinfrastruktur.

Das große Manko von DNSSEC – und somit auch von DANE – ist die geringe Verbreitung. Das umfasst alle betroffen Ebenen:

- Nicht alle TLDs nehmen bereits daran teil.
- Serversoftware bspw. Email-Server sind nur zu einem geringen Anteil DNSSEC fähig.
- Die ausgerollten Resolver sind nicht mal security-aware Stub-Resolver.
- Middleboxen blockieren in Unternehmen DNSSEC Fragen und Antworten, da sie den DNS-Typ nicht kennen.
- Kaum Clientsoftware signalisiert den Status von DNSSEC.

Letzteres ist traurig, denn zum einen zeigt das Firefox Plug-In, wie das elegant gemacht werden kann und zum anderen würde die Anzeige den Druck auf alle anderen Beteiligten erhöhen, DNSSEC flächendeckend.

Statement

Microsoft-Urteil: Ein Meilenstein für Datenschutz in der Cloud

Im Streit mit dem US-Justizministerium hat Microsoft einen wichtigen Etappensieg eingefahren. Der US-Konzern muss E-Mails, die auf Servern im Ausland gespeichert sind, nicht US-Ermittlern übergeben. Für Datenschützer und Nutzer von US-Cloud-Lösungen ist das Urteil ein großer Erfolg.

Das Berufungsgericht S*econd U.S. Circuit Court of Appeals* in Manhattan entschied am 14. Juli 2016 in zweiter Instanz, dass Microsoft US-Ermittlungsbehörden keinen Zugriff auf solche Daten gewähren muss, die auf Servern außerhalb der USA gespeichert sind (*Microsoft vs. United States, 2nd U.S. Circuit Court of Appeals, No. 14-2985*). Nach Ansicht der Richter war der richterliche Durchsuchungsbeschluss nicht durch den *Stored Communications Act* gedeckt und reicht daher nicht aus, um die Herausgabe von E-Mails zu verlangen, die auf einem irischen Server einer irischen Tochtergesellschaft gespeichert worden sind.

Microsoft wehrt sich gegen den Durchsuchungsbeschluss

Was war passiert? Das US-Justizministerium hatte im Jahr 2013 einen richterlichen Beschluss gegen Microsoft erwirkt, um an die Daten eines E-Mail-Accounts einer Person zu gelangen, gegen die im Zusammenhang mit Drogendelikten ermittelt wurde. Microsoft weigerte sich jedoch die Daten herauszugeben. Der US-Konzern begründete sein Verhalten damit, dass die betreffenden Daten auf Servern einer Tochtergesellschaft in Irland gespeichert seien und US-Behörden dort keine Befugnisse hätten. Außerdem berief sich Microsoft auf europäisches Datenschutzrecht. Danach kann ein Beschluss oder Urteil eines Gerichts oder einer Behörde eines Drittlandes, der die Übermittlung oder Offenlegung personenbezogener Daten verlangt, nur dann anerkannt oder umgesetzt werden, wenn er auf einer internationalen Vereinbarung wie einem Abkommen für Amtshilfe basiere. Microsoft hatte zudem argumentiert, die Position der US-Behörden stünden mit der Souveränität Irlands in Konflikt.

Keine exterritoriale Anwendung von US-Recht

Das zweite Bundesberufungsgericht in Manhattan kassierte nun ein erstinstanzliches Urteil und schloss sich der Rechtsauffassung von Microsoft an. Die Richter entschieden, dass die Umsetzung des Durchsuchungsbeschlusses einer exterritorialen Anwendung von US-Gesetzen gleichkommt. Der Kongress hat die Anwendung des fraglichen Stored Communication Acts außerhalb der USA jedoch gerade nicht vorgesehen.

Wenn das Urteil Bestand hat, dürfte es Entscheidungen von Unternehmen und Behörden erleichtern, zukünftig verstärkt auf US-Cloud-Lösungen zu setzen. Die Daten wären außerhalb der Vereinigten Staaten vor dem Zugriff von US-Ermittlungsbehörden zunächst sicher. Bei Herausgabeverlangen käme es auf das Recht am den Standort des Servers an, nicht auf das Heimatrecht der ermittelnden Behörde.

Wegweisendes Urteil für die Datensicherheit in der Cloud

Zwischen US-Behörden und den Technologiefirmen besteht schon seit geraumer Zeit Streit darüber, ob eine Pflicht zur Herausgabe von Daten besteht, die von selbstständigen Tochtergesellschaften außerhalb der USA gespeichert worden sind. Ausgangspunkt liegt in den geschäftlichen Interessen der US-Konzerne. Diese beklagen, dass die Skepsis der Kunden im Ausland aufgrund der Zusammenarbeit mit US-Ermittlungsbehörden und US-Geheimdiensten gewachsen sei und hieraus zunehmend handfeste Wettbewerbsnachteile für US-Unternehmen entstünden. Insbesondere die Snowden-Enthüllungen hätten dazu geführt, dass das Vertrauen in die Cloud-Sicherheit beträchtlich gesunken sei. Die Cloud-Dienstleister fürchten daher, dass allzu weitreichende Eingriffsbefugnisse von US-Ermittlungsbehörden Gewinnaussichten im europäischen Markt zunehmend schmälern könnten. Infolgedessen setzen sich US-Konzerne gegen Maßnahmen ihrer nationalen Ermittlungsbehörden verstärkt medienwirksam zur Wehr. So weigerte sich beispielsweise die Firma Apple mit der Strafverfolgungsbehörde FBI zusammen zu arbeiten und die Sicherheitsvorkehrungen eines von einem Terroristen genutzten iPhones außer Kraft zu setzen.

Spürbare Auswirkungen für die Zukunft des Cloud Computings

Vor diesem Hintergrund wurde die Entscheidung des Gerichts von der gesamten IT-Branche mit Spannung erwartet. Schließlich ist die derzeitige Rechtslage sowohl aus Sicht europäischer Unternehmen als auch aus Sicht europäischer Behörden bedenklich. Sie stehen oftmals vor einer Grundsatzfrage. Sind die Daten in der Cloud tatsächlich sicher? Gerade bei US-Anbietern ist diese Sorge besonders stark ausgeprägt, da unklar ist, was US-Cloud-Anbieter US-Ermittlungsbehörden oder Geheimdiensten unter welchen Umständen preisgeben müssen. Diese Ungewissheit nährt die Skepsis gegenüber sämtlichen Cloud-Lösungen.

Das Urteil dürfte diese Sorgen lindern und die Datensicherheit in der Cloud erhöhen. Den US-Richtern ist daher zuzustimmen, wenn sie das das Urteil als Meilenstein für den Datenschutz einordnen. Cloud-Anbieter können nun sicher sein, dass US-Behörden jedenfalls nicht auf Grundlage eines einfachen Durchsuchungsbeschlusses auf Daten zugreifen dürfen, die im Ausland gespeichert sind. Das Urteil ist jedoch noch nicht rechtskräftig. Das US-Justizministerium kann den Supreme Court anrufen. Es bleibt abzuwarten, ob dieser Weg eingeschlagen wird.

Dr. Jan Byok ist Rechtsanwalt und Fachanwalt für Informationstechnologierecht in Düsseldorf und Partner der internationalen Wirtschaftskanzlei Bird&Bird LLP. Sein Fokus liegt in den Gebieten des öffentlichen Vergabe-, Vertrags- und Preisrechts, des ITK-Rechts, des Wettbewerbs- und Kartellrechts und in der juristischen Projektsteuerung. Dr. Byok hat zahlreiche komplexe Technologieprojekte bei der bundesweiten Einführung des BOS-Digitalfunks, der elektronischen Gesundheitskarte, der Umstellung des öffentlichen Rechnungswesens, der Einführung von e-procurement-Systemen, dem Abschluss von Providerverträgen, in der Beschaffung von Hard- und Software und bei IT-Outsourcings erfolgreich umgesetzt oder saniert.

Seminar

Crashkurs IT-Recht für Nichtjuristen
05.10.16 in Düsseldorf

Die ComConsult Akademie veranstaltet am 05.10.16 ihr Seminar "Crashkurs IT-Recht für Nichtjuristen" in Düsseldorf.

Die Veranstaltung bildet eine kompakte Grundorientierung über das unübersichtliche Rechtsgebiet des IT-Rechts. Teilnehmern, die sich wiederkehrend mit rechtlichen Fragestellungen in der Informationstechnologie beschäftigen, wird vermittelt, wo Herausforderungen und Haftungsrisiken liegen, welche Probleme auch als Laie handhabbar sind und in welchen Fällen externes Know-How unerlässlich ist.

Die dritte IT-Revolution hat begonnen. Geschäftsleben, Produktionsprozesse und Freizeitverhalten stehen vor einer umfassenden informationstechnologischen Vernetzung. IT und TK wachsen zusammen. Damit eröffnen sich neue unternehmerische Möglichkeiten. Zugleich nimmt die rechtliche Durchdringung und Komplexität in der Netzwirtschaft stark zu. Zivilrecht, öffentliches Recht, gewerbliche Schutzrechte und Strafrecht sind bedeutende Leitplanken für die rechtssichere und optimale IT-Lösung. Ohne Kenntnis der rechtlichen Einflussfaktoren können IT-Projekte nicht sinnvoll geplant und durchgeführt werden.

- IT-Vertragsrecht: welcher Vertragstyp des BGB passt zu welchem Vorhaben (Mietvertrag, Werkvertrag, Kaufvertrag, Dienstleistungsvertrag usw.)
- Grundlagen des Datenschutzrechts
- Urheberrechtliche Grundlagen zu Softwarelizenzen
- Grundlagen des Lizenzmanagement und Lizenzcontrolling - wie können Lizenzaudits schadlos überstanden werden
- IT-Compliance
- IT-Security (IT-Sicherheitsgesetz und NIS-Richtlinie)
- Haftungsrisiken im IT-Bereich
- aktuelle Themen aus der Informationstechnologie

Diese Veranstaltung wendet sich an IT-Leiter, Compliance-Beauftragte und Geschäftsführer, die sich kompakte und praktische Grundkenntnisse zu den rechtlichen Eckpunkten des IT-Projektes verschaffen wollen. Die Inhalte sind insbesondere an Nichtjuristen gerichtet, die sich nicht alltäglich mit rechtlichen Fragestellungen befassen und eine Grundorientierung suchen. In dem Seminar werden auch Praxisfälle erörtert.

Durch die Veranstaltung führen Sie die Rechtsanwälte Dr. Byok und Dr. Wübbelt.

Dr. Jan Byok ist Rechtsanwalt und Fachanwalt für Informationstechnologierecht in Düsseldorf und Partner der internationalen Wirtschaftskanzlei Bird&Bird LLP. Sein Fokus liegt in den Gebieten des öffentlichen Vergabe-, Vertrags- und Preisrechts, des ITK-Rechts, des Wettbewerbs- und Kartellrechts und in der juristischen Projektsteuerung.

Dr. Benjamin Wübbelt ist seit 2014 Associate der internationalen Wirtschaftskanzlei Bird & Bird LLP. Er gehört dem Praxisbereich Öffentliches Wirtschaftsrecht an. Sein Beratungsschwerpunkt ist das Vergaberecht mit besonderem Bezug zum Informationstechnologie- und Datenschutzrecht.

Fax-Anmeldung an ComConsult 02408/955-399

Crashkurs IT-Recht für Nichtjuristen

Ich buche das Seminar
Crashkurs IT-Recht für Nichtjuristen

☐ 05.10.16 in Düsseldorf
zum Preis von € 1.090,--

☐ 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

Zweitthema

Die Zukunft von VoIP und UC liegt in der Cloud

Fortsetzung von Seite 1

Markus Geller verfügt über langjährige Erfahrung in Forschung, Entwicklung und Betrieb von Lokalen Netzen, IP-TV, Wireless Local Area Networks sowie Sicherheits-Technologien. Als Mitarbeiter der ComConsult Research GmbH ist er verantwortlich für Produkttests und Marktbeobachtung. Zu diesen Themengebieten ist er zudem als Referent bei der ComConsult Akademie tätig.

Laut Aussage vom Alcatel Lucent Enterprise werden heute noch bei Unternehmen mit bis zu 500 Mitarbeitern ca. 60% aller Projekte mit digitalen Telefonsystemen umgesetzt und auch bei größeren Installationen mit bis zu 1000 Nutzern ist der Anteil mit ca. 25% immer noch sehr hoch.

Diese Zahlen entsprechen im Übrigen auch unseren Erfahrungswerten, die wir aus Befragungen unserer Kunden gewonnen haben. Diese besagen, dass ca. 20% aller Neu-Installation in Vermittlungstechnik ausgeführt werden.

Diese Zahlen sind vor allem deshalb interessant, da ja alle Netzprovider angekündigt haben ihre Telefondienste ab 2017 bevorzugt nur noch als VoIP Service zur Verfügung zu stellen.

Dies bedeutet aber auch, dass diejenigen Kunden, die sich heute bewusst für eine digitale Telefonlösung entscheiden, noch nicht erkannt haben, dass sie sich auch von der Zukunft der Kommunikation abkoppeln und die Mehrwerte von UC nicht sehen oder keinen Business Case erkennen können.

Und dieser Business Case muss nicht zwangsläufig bei der Kommunikation im eigenen Unternehmen gesucht werden, sondern kann sich durchaus auch an Prozessen orientieren, die über die eigene Unternehmensgrenze hinausgehen. Doch dazu später.

Zu diesen eher ernüchternden Zahlen kommt zusätzlich die Erkenntnis, dass der Einsatz von UC im deutschen Markt immer noch auf sich warten lässt. Auch hier zeigen die Unternehmen eine starke Zurückhaltung beim Einsatz von erweiterten Kommunikationsdiensten wie IM, Präsenz oder Kollaboration mittels der Enterprise VoIP Plattform. Laut einer Reihe renommierter Lösungsanbieter beschreiten nur ca. 30% aller Neu-Installationen diesen Weg.

Auf der anderen Seite suchen jedoch die Netzbetreiber neue Einnahmequellen, da ihr klassischen Gebührenmodelle zur Abrechnung von Telefongesprächen zunehmend zum Erliegen kommen. Flat Rate-Modelle zur Abrechnung von Telefondienstleistungen sind nach ihrem Durchbruch bei der Mobiltelefonie jetzt auch im Festnetz völlig normal und haben eine erstaunliche Bandbreite erreicht.

- Nationales Festnetz
- Nationale Mobilfunknetze
- Europa
- International

sind nur einige Beispiele, die heute angeboten werden, um die zeit- und/oder entfernungsabhängig tarifierten Verbindungsdienstleistungen abzulösen und damit die Festnetzanbieter in eine schwierige Ertrags-Situation bringen.

Zusätzlich drängen immer stärker Firmen wie sipgate QSC oder NFON in den Markt, so dass große Netzbetreiber wie Vodafon oder auch die Telekom eigene Cloud basierte Telefonanlagenlösungen betreiben müssen um weiterhin wettbewerbsfähig zu sein.

Diese, aktuell sehr sprachorientierten Lösungen, bieten dabei ein erstaunliches Leistungsspektrum, darunter natürlich alle klassischen Merkmale, die man im Büroumfeld zwingend erwartet, wie: halten, makeln, weiterleiten, anklopfen, Rufumleitung permanent oder nach Zeitvorgabe, Rufweiterleitung bei besetzt, Fax-Versand & Empfang am Arbeitsplatz, Voicemail, Speech-to-Text und MWI. Aber auch übergreifende Leistungsmerkmale wie Anrufübernahmegruppen, zeitgesteuerte Ansagen oder einfache Kontaktcenter-Funktionen können umgesetzt werden.

Nun wird der ein oder andere anführen, dass es mit der Qualität und Verfügbarkeit solcher Lösungen nicht weit her sein kann. Dabei verkennen diese Kritiker, dass hinter der Diensterbringung durchaus professionelle Lösungen stehen. Nicht jeder Anbieter setzt auf eine OpenSource Lösung wie Asterisk* oder Kamailio. Viele Anbieter, darunter Telekom oder NetCologne, nutzen z.B. Swyx und haben daher auch einen entsprechenden Support seitens des Herstellers im Rücken.

Natürlich steht und fällt die Gesprächsqualität mit der zur Verfügung stehenden Internet-Bandbreite bzw. mit der Möglichkeit den Sprachverkehr zu priorisieren. Lösungen wie die von NetCologne oder der Telekom sind zudem an die Bereitstellung einer Datenleitung gekoppelt.

Nach nunmehr 5 Jahren Erfahrung mit einer Cloud TK Lösung von sipgate können wir bei der ComConsult Research ein positives Fazit bezüglich der oben genannten Faktoren ziehen: Die Ausfälle in diesem Zeitraum beliefen sich auf wenige Stunden, die dabei genutzte Internetanbindung hatte im Betriebszeitraum (wöchentlich Mo-Fr, 8:00- 17:00) eine Verfügbarkeit von annähernd 100%.

Die Vorteile, die sich aus dieser Lösung ergeben, liegen für uns klar auf der Hand:

Die Zukunft von VoIP und UC liegt in der Cloud

- Einfache Administration im Vergleich zur vorher genutzten Asterisk* Lösung
- Schneller & Qualifizierter Support bei Problemen
- Kein Aufbau von eigenem, TK-spezifischen Know How nötig
- Kurze Vertragslaufzeit
- Geringer CAPEX Bedarf (nur Tischtelefone und Softclients + Zubehör)
- Geringe monatliche Kosten gegenüber dem zuvor genutzten PMX Anschluss (Pay as you grow & pay what you need)

Und dabei reden wir bis jetzt nur über einen reinen Sprachdienst.

Ergänzt wird die eingesetzte Lösung durch diverse andere cloudbasierte Kommunikationsanwendungen. Für Präsenz, IM und Videochat kommt Skype for Business auf Basis von Office365 zum Einsatz. Für Videokonferenzen mit dritten nutzen wir Zoom.

Wie man also sieht sind UC und VoIP als Clouddienst heute schon voll einsatzfähig.

Nun weiß man aber auch, dass wir hier in Deutschland beim Einsatz von Lösungen im Bereich der Kommunikation eher konservativ bzw. abwartend agieren. Oft spielt dabei das Argument der Datensicherheit und der Verfügbarkeit eine entscheidende Rolle, aber auch die Frage nach den einsetzbaren Leistungsmerkmalen ist immer noch immens wichtig.

Gerade der letzte genannte Punkt ist übrigens eines der Hauptargumente für eine Anlage, die auf Basis klassischer Vermittlungstechnik beruht oder ein proprietäres VoIP Protokoll einsetzt. SIP basierte VoIP Lösungen erreichen hier bei Weitem nicht den Leistungsumfang wie ihre „alten“ Mitbewerber. Einen Nachteil, den sie jedoch mit dem Ansatz der Multimediafähigkeit ausgleichen können.

Man ist heute daher immer noch der Meinung, dass eine Kommunikationslösung im Eigenbetrieb gerade in diesen Bereichen einfacher zu beherrschen ist als eine moderne Cloud-Lösung.

Was jetzt aber die Verfügbarkeit und Sicherheit anbelangt, spätestens mit der Umstellung des Primär Multiplex Anschlusses auf einen SIP Trunk verliert die bisher abgeschlossenen TK-Welt ihren Sicherheitsnimbus. Sie wird jetzt genauso angreifbar wie alle anderen Infrastrukturen, die mittels TCP/IP miteinander kommunizieren.

Und was die Bedeutung der Leistungsmerkmale anbelangt zeigt sich, dass die zwischenmenschliche Kommunikation im Büroalltag sich immer mehr von einer verbalen zu einer nonverbalen Verständigung verlagert.

Schauen Sie nur auf die nachfolgende Generation, für diese ist ein Leben ohne WhatsApp bzw. Kurznachrichtendienst kaum vorstellbar, worüber die Sprachfunktion des Smartphones fast in Vergessenheit gerät. (Und auch ich nutzte dieses hauptsächlich um Textnachrichten aller Art zu lesen und immer weniger zum Telefonieren.)

An dieser Stelle möchte ich noch einmal den Faden bezüglich der Netzbetreiber aufgreifen. Wie schon gesagt, sehen wir hier Stand heute ein breites Angebot an Telefonanlagen Lösungen. Dabei spielt es erstmal keine Rolle, ob der Dienst aus einer Privat Cloud (früher nannte man das Outsourcing) oder einer Public Cloud als SaaS (Software as a Service) angeboten wird. Was noch fehlt ist die volle Integration von UC Diensten. Es gibt hier und dort zaghafte Ansätze Funktionen wie IM oder Präsenz in die Produkte mit aufzunehmen, aber der Fokus liegt immer noch auf der Telefonie.

Aber die Provider werden zum Handeln gezwungen. Wie schon eingangs erwähnt, bricht ihnen das Geschäft mit den Vermittlungsentgelten weg. Daher müssen sie sich neue Geschäftsfelder erschließen, denn als reiner Leitungsanbieter werden die Margen in der Zukunft nicht ausreichen um erfolgreich am Markt bestehen zu können. In diesem Zusammenhang möchte ich nur auf die Kosten der Internetanbindungen verweisen. Vor 4 Jahren bewegten sich die Kosten eines 10 Mbit Glasfaseranschlusses auf einem Niveau, für das sie heute durchaus 100 - 200 Mbit erhalten.

Was liegt da also näher als qualifizierte Dienste anzubieten - und genau dies passiert derzeit.

Bevor wir aber jetzt die Cloudlösungen genauer unter die Lupe nehmen, möchte ich noch einmal kurz die Definition der unterschiedlichen Varianten voranstellen um Missverständnisse zu vermeiden.

Laut NIST, dem amerikanischen Pendant zum DIN, lassen sich Cloud-Services in folgende vier Kategorien einteilen:

1. In einer **Private Cloud** wird die Cloud-Infrastruktur nur für eine Institution betrieben. Sie kann von der Institution selbst oder einem Dritten organisiert und geführt werden und kann dabei im Rechenzentrum der eigenen Institution oder einer fremden Institution stehen

2. Von einer **Public Cloud** wird gesprochen, wenn die Services von der Allgemeinheit oder einer großen Gruppe, wie beispielsweise einer ganzen Industriebranche, genutzt werden können und die Services von einem Anbieter zur Verfügung gestellt werden.

3. In einer **Community Cloud** wird die Infrastruktur von mehreren Institutionen geteilt, die ähnliche Interessen haben. Eine solche Cloud kann von einer die-

Die Zukunft von VoIP und UC liegt in der Cloud

ser Institutionen oder einem Dritten betrieben werden.

4. Werden mehrere Cloud Infrastrukturen, die für sich selbst eigenständig sind, über standardisierte Schnittstellen gemeinsam genutzt, wird dies **Hybrid Cloud** genannt.

Nachdem nun die Definition von Cloud Services geklärt ist, können wir uns jetzt den Anbietern und ihren Lösungen zuwenden.

Wichtig bei der Betrachtung ist hier die Art der Cloudlösung, die zur Verfügung gestellt wird. Zur Unterscheidung kann man grob folgende Einteilung hernehmen:

- Reine Cloud PBX Anbieter wie QSC oder sipgate betreiben einen Public Cloud Service
- Netzbetreiber wie die Telekom und Vodafone bieten neben klassischen Lösungen immer auch eine Public Cloud Lösung an
- IT Provider wie Dimension Data oder T-Systems können neben Public Cloud-Diensten auch Privat- und Hybrid-Cloud Services anbieten

Um die Komplexität der Produktvielfalt zu verdeutlichen habe ich mir einmal das Beispiel der Deutschen Telekom herausgegriffen. Hier kann man sehr gut erkennen, wie sich ein Provider bemüht den Umstieg vom Netzbetreiber zum Serviceanbieter zu vollbringen.

Grundsätzlich unterscheidet man hier zwei Produktgruppen. Zum einen sind da die reinen VoIP Dienste und als zweiten Bereich kann man eine Reihe von UC und Kollaboration Services erkennen.

Die VoIP Cloud besteht dabei aus zwei Produkten:

1. DeutschlandLAN Skype for Business mit dem Hauptfocus auf Zusammenarbeit und den daraus resultierenden Einbußen bei den Leistungsmerkmalen im Bereich der klassischen Telefonie
2. DeutschlandLAN Swyx mit dem exakt gegensätzlichen Ansatz (viele Leistungsmerkmale weniger UC)

Hinzu kommen für den Bereich der reinen Kollaboration und für Video- und Webkonferenzen die folgenden Lösungen:

1. iMeet - eine browserbasierte Konferenz- und Kollaborationsplattform der Firma PGi - für bis zu 125 Teilnehmer (Inkl. HD Voice & Video, Screen & Filesharing)
2. Das etablierte Cisco WebEx
3. Das ebenfalls browserbasierten Unify Circuit inkl. einer optionalen Telefonie-Integration (hierfür wird allerdings ein All-IP Anschluss der Telekom benötigt)
4. Und natürlich noch einmal Skype for Business von Microsoft

Wie man an der Produktsituation erkennen kann, ergeben sich eine Reihe von Möglichkeiten eine professionelle Cloud Lösung zu beziehen, die die unterschiedlichen Erwartungen an die Unternehmenskommunikation erfüllen. Der Focus dieser Lösungen liegt allerdings ganz klar auf dem KMU Bereich. Enterprise Kunden mit mehr als 5000 Teilnehmern werden hier bewusst nicht angesprochen.

Möchte man jetzt noch einen Schritt weitergehen und eine VoIP/UC-Lösung nach eigenen Vorstellungen umsetzen, so ist auch das mittels Cloud Ansatz möglich. Hierbei wechselt man dann jedoch das Modell hin zu einer Privat Cloud (s. Definition). Es gilt jedoch auch einige Nachteile gegenüber dem Public Cloud Modell zu beachten.

Der Aufbau einer Public Cloud erfolgt in der Regel mittels eines oder weniger Produkte, welche über eine Mandantenfähigkeit verfügen. Dies bedeutet, dass auf einer Instanz (Sever-Farm) mehrere Kunden parallel verwaltet werden können und dabei für jeden Kunden ein spezifischer, abgeschlossener Bereich zur Verfügung gestellt wird.

Auf der Basis dieser Bereitstellung, ergeben sich für den Service Anbieter eine Reihe von Vorteilen:

1. Er muss nicht für jeden Kunden eine gesonderte Instanz aufsetzen
2. Mengenvorteile beim Einkauf, z.B. bei den Lizenzen, können an die Kunden weitergegeben werden
3. Die Anpassung der zugrundeliegenden Hardware und Software erfolgt Bedarfsgerecht je nach Anzahl der Nutzer
4. Durch die Fokussierung auf wenige Produkte können Betriebskonzepte kostenoptimal gesteuert werden.

Natürlich haben Public Cloud Modelle auch Nachteile. Werden spezielle Zusatzleistungen benötigt wie Call & Contact-Center Integration in bestehende Betriebsprozesse auf Basis selbstentwickelter Software oder revisionssichere Sprachaufzeichnungsdienste, versagen in der Regel alle Public Cloud Lösungen.

Hier schlägt nun die Stunde der IT-Provider und ihrer Privat- bzw. Hybrid-Cloud Lösungen. Diese reichen vom reinen Out-Sourcing der Enterprise VoIP & UC Lösung bis hin zu Baukastenlösungen, die bei Bedarf speziell auf den Kunden angepasst werden können.

Dieses Modell wird vor allem von denjenigen Firmen gewählt, die sich vermehrt auf ihre Kernkompetenz fokussieren möchten. Als Beispiel fällt mir da aus meiner eigenen Erfahrung die Allianz Versicherung ein. Hier hat man vor einigen Jahren den

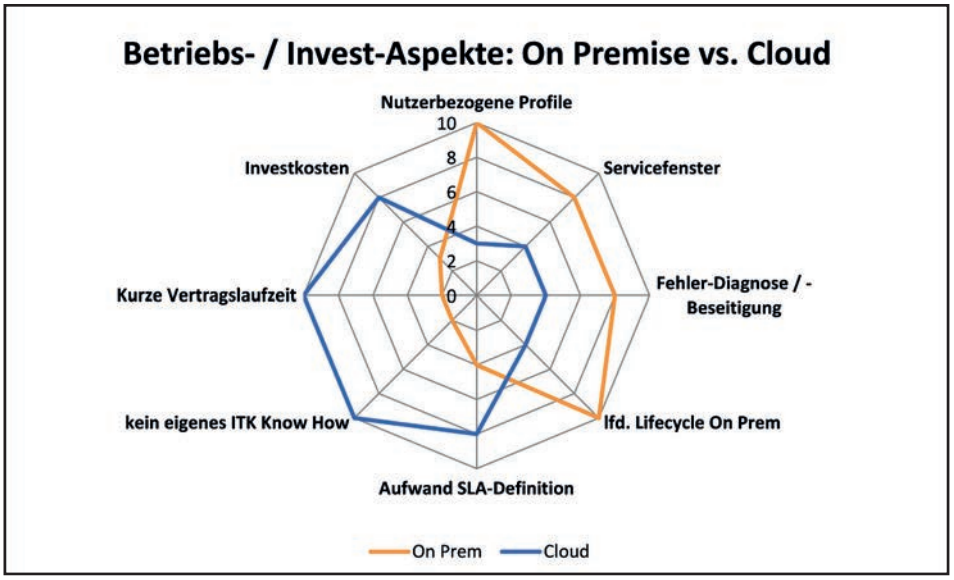

Abbildung 1: Betriebs- & Invest-Aspekte

Quelle: Borowka-Gatzweiler, UBN

Die Zukunft von VoIP und UC liegt in der Cloud

Bereich der TK und Datennetze an einen IT-Provider ausgelagert. Wie gesagt früher nannte man dies Outsourcing heute würde man wohl eher von einer Privat Cloud sprechen.

Die Vorteile, die sich aus dieser Entscheidung ergeben, sind in erster Linie die Verlagerung der Kosten von CAPEX zu OPEX. Aber auch die Einsparung von Personalkosten ist hier ein nicht ganz unwichtiger Faktor.

Vergleicht man jedoch am Ende den Eigenbetrieb mit einer Privat Cloud Lösung wird man erstaunt feststellen, dass die Einsparungen bei Weitem nicht das Niveau erreichen wie bei einem Public Cloud Modell. Zum Teil ist es sogar so, dass der Eigenbetrieb weit günstiger ist als so manches Cloud Modell. Das wiederum liegt zum Teil am fehlenden Mengengerüst und an den speziellen Anforderungen der einzelnen Kunden.

Anderseits bieten gerade cloudbasierte UC Lösungen, egal ob Privat oder Public, einen guten Einstieg um die Vorteile der Mehrwertkommunikation zu erkunden. Ehrlicherweise muss man doch heute immer noch feststellen, dass VoIP und UC Produkte für die Betreiber einer klassischen TK-Anlage vollständiges Neuland sind und das obwohl wir schon das Jahr 2016 schreiben. Unsere Kurse bei der ComConsult Akademie zu diesen Themen erfreuen sich jetzt schon seit über 10 Jahren einer ungebrochenen Beliebtheit und eine Sättigung ist immer noch nicht abzusehen.

Gerade die Kombination aus neuer Basis Technologie (IP & SIP) und den Mehrwertdiensten aus dem UC Bereich erschweren es den Mitarbeitern aus dem klassischen TK Umfeld, schnell neue Lösungen aufzubauen und zu betreuen. Dies und der Mangel an gut ausgebildeten Mitarbeitern im ITK Sektor verstärken mit der Zeit den Trend Services auszulagern.

Jedoch muss der Schritt in Richtung IP basierter Dienste sowieso getätigt werden, möchte man nach 2017 noch telefonieren. Gerade mit dem Wechsel in der Basistechnologie, weg von ISDN hin zu SIP & IP, werden sich auch viele neue Projekte für UC, Video & Web Kollaboration ergeben.

Denn ein Aussitzen dieser Lösungen wird nur dazu führen, dass die Mitarbeiter sich Plattformen außerhalb der Unternehmens IT suchen werden, was zu erheblichen Sicherheitslücken, führt die nur schwer geschlossen werden können.

Aber auch die Unternehmen, die derzeit noch am Eigenbetrieb hängen und nicht planen diesen aufzugeben, werden in den kommenden Jahren immer mehr den Kostendruck zu spüren bekommen.

Wer sich die Quartalszahlen von Microsoft, Amazon, Alphabet und Co aus dem Sommer 2016 anschaut, wird unschwer erkennen, dass die größten Zuwächse dieser Unternehmen im Bereich der Clouddienste angefallen sind. AWS, als Spin Off zur besseren Auslastung der Amazon Rechenzentren gegründet, erwirtschaftet heute die größten Gewinne innerhalb des Konzerns.

Ähnlich sieht die Situation bei Microsoft aus, seit der Einführung von Skype for Business und Office 365 sind dies die am schnellsten wachsenden Umsatz- und Gewinnträger.

Und es sind genau diese Anbieter, die mit immer günstigeren Angeboten den Eigenbetrieb mittelfristig unrentabel werden lassen.

Hinzu kommt, dass auch die etablierten Anbieter von UC und VoIP Lösungen ihre Liebe zur Cloud entdeckt haben.

Egal ob Alcatel, Avaya, Innovaphone, Mitel oder Unify, alle bemühen sich in der Cloud Fuß zu fassen, um das Geschäft von Morgen nicht zu verlieren. Seit der Markteinführung von WebEx, gibt es den klaren Trend, Kommunikation, die nicht auf Telefontechnik beruht, ins Web zu verlagern.

Dazu gehören eben alle Dienste, die UC so reizvoll machen:

- File- & Desktop Sharing
- Web- & Videokonferenzen
- Präsenz & IM

Daher ist es denn auch nicht verwunderlich, dass Unify Circuit, obwohl erst seit zwei Jahren auf dem Markt, schon als etablierte Cloudanwendung zu bezeichnen ist.

Dabei wird die Lösung nicht nur über Partner wie der Deutschen Telekom vermarktet, man kann den Dienst auch direkt bei Unify einkaufen.

Diese Situation lässt daher auch andere Marktteilnehmer wie z.B. Alcatel Lucent Enterprise nicht unberührt. Auch hier hat man sich zu einem offensiven Umgang mit dem Thema entschieden.

Die Lösung hier heißt Rainbow und stellt ähnlich wie bei Unify eine elegante Möglichkeit dar, webbasierte UC Funktionen mit einem Amtszugang bzw. VoIP Diensten zu versehen.

Noch gibt es den Service nur als Testversion, jedoch ist auch hier mit einem raschen Markteintritt zu rechnen.

Nebenbei hat man dabei auch eine Lö-

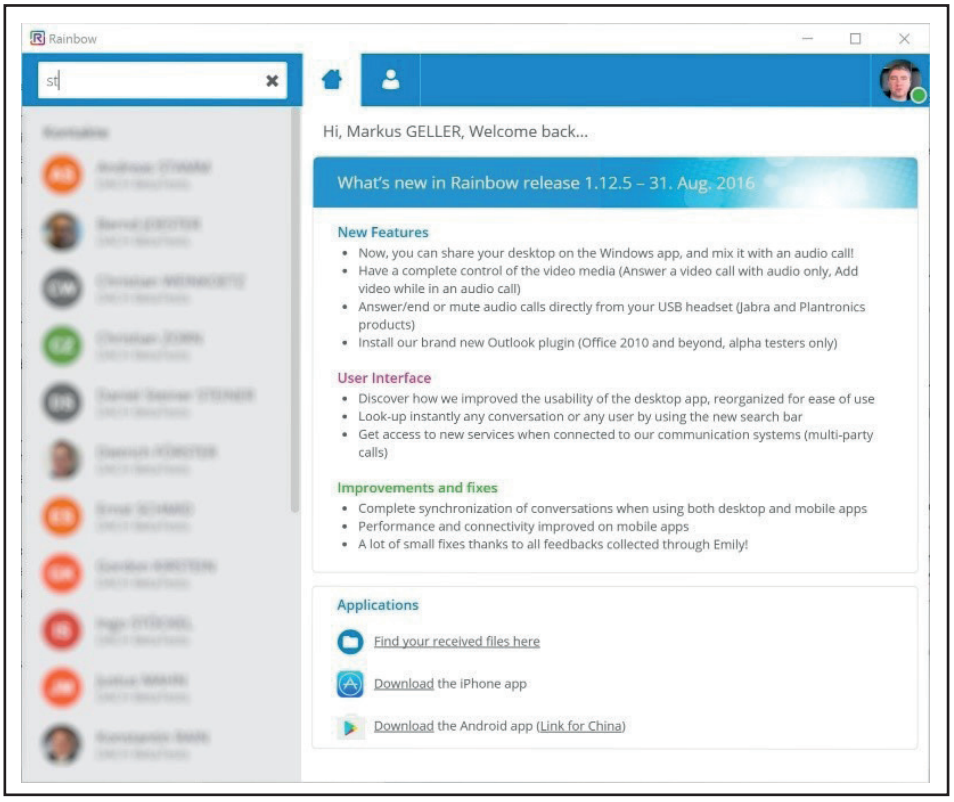

Abbildung 2: ALE Rainbow GUI

sung für VoIP Services erarbeitet. Diese werden zwar nicht direkt über Alcatel Lucent Enterprise vertrieben, sondern über den Partner Dimension Data, bieten aber dafür alle Leistungsmerkmale, die man von der OpenTouch Lösung her kennt.

Außerdem kann diese VoIP Cloud auch mit Spezialanwendungen wie Call & Contactcenter Lösungen oder einer Voice Recording Lösung, die den Regeln von MiFID II entspricht, versehen werden. Dabei läuft der Vertrieb dieser Lösung über Dimension Data, während Alcatel Lucent Enterprise für den Betrieb der Infrastruktur verantwortlich zeichnet.

Wie man daraus unschwer erkennt, folgt nun auch die Enterprise Telefonie dem Weg in die Cloud.

Diese Annahme lässt sich durchaus belegen. Im vergangenen Jahr stellte Nemertes Research eine Studie vor, in der die Bereitschaft abgefragt wurde Kommunikationsanwendungen aus der Cloud zu beziehen. Diese Studie ist zwar eine weltweite Betrachtung, aber es zeigt sich, dass es einen globalen Trend hin zu Cloud Lösungen unverkennbar gibt.

Um dies zu verdeutlichen hier zwei Statistiken auf die entscheidende Frage:

- Wie hoch ist die Akzeptanz von Cloud basiertem VoIP & UC?

Doch es sind nicht nur die Kosten, die heute über den Frage Cloud vs. Eigenbetrieb entscheiden. Zunehmend rückt auch der Faktor der unternehmensübergreifenden Kommunikation in den Focus. Dabei spielen rein sprachgebundene Dienste heute nur noch eine Rolle unter vielen. Immer öfter werden daher auch Video und Datendienste als Echtzeitmedium genutzt um effektiv in einem Team zu agieren.

Das folgende Beispiel ist zwar schon ein paar Jahre alt, zeigt aber immer noch sehr gut, was sich Unternehmen von UC erhoffen:

UC ist mit dem Grundversprechen angetreten, die Nutzung aller möglichen Kommunikationskanäle zum reibungslosen und verlustfreien Austausch von Informationen zu ermöglichen. Dabei sollte dies über die Integration verschiedenster Technologien und Protokolle, wie Email, Telefonie, Multiuser Videokonferenz oder Dokumentenbearbeitung und Chatfunktion erfolgen.

Die grundlegende Einschränkung, die bis heute besteht, ist jedoch:

Die Funktionen beschränken sich auf einen geschlossenen Benutzerkreis, der mit dem System verbunden ist und (in fast allen Fällen) über eine spezielle Client-Software verfügt.

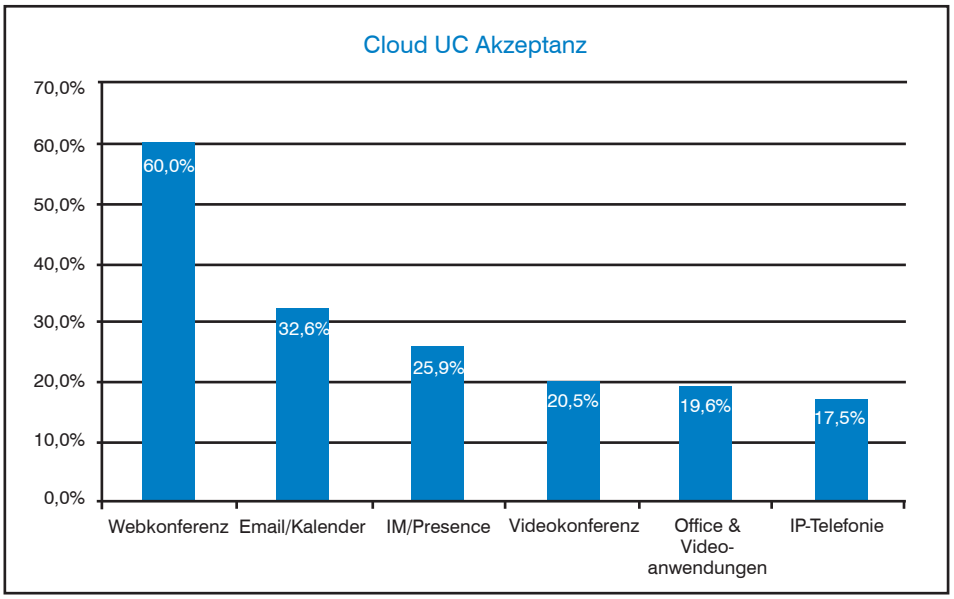

Abbildung 3: Cloud Akzeptanz in 2014 Quelle: Nemertes Research

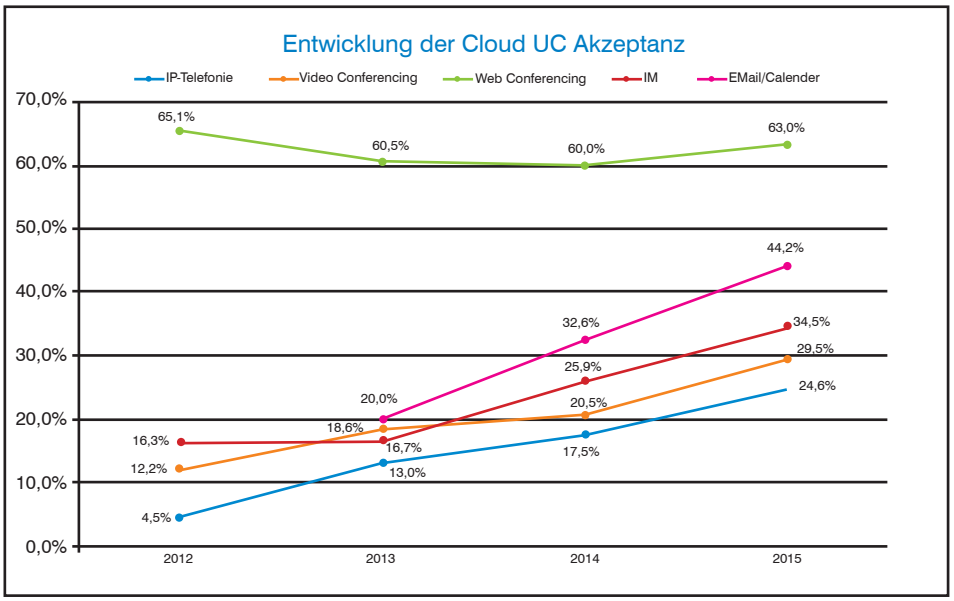

Abbildung 4: Entwicklung der Cloud Akzeptanz Quelle: Nemertes Research

Bei Personen außerhalb dieses Benutzerkreises versagen heutige UC Enterprise Implementierungen.

Dass aber eine übergreifende Kommunikation gewünscht und gewollt ist, zeigt das von mir angeführte Beispiel.

Auf MSNBC erschien vor einiger Zeit ein Artikel mit der Überschrift, "***Hunderte von Lieferanten, eine Boeing 737***"

Die Herausforderung, die hier von einem leitenden Mitarbeiter von Boeing beschrieben wurde, ergab sich aus folgenden Punkten:

- Montage eines Produktes
  - das aus 367.000 Teilen besteht,
  - mittels hunderter verschiedener Lieferanten hergestellt wird,
  - bei einer Produktionsgeschwindigkeit von mehr als einem Flugzeug pro Tag
  - mit einem Bestellvolumen, das die Produktion für über 6 Jahren auslastet

Eine Microsoft Fallstudie zitiert dazu einen Boeing IT-Produkt-Manager mit den Worten: "*Wir versuchen so oft wie möglich UC Föderationen mit unseren Lieferanten zu schließen, so dass sie leicht mit unseren Engineering-Teams zusammenarbeiten*

können. Unsere Teams können dabei ihre Präsenz-Informationen und Meldungen sehen, als ob sie Teil unseres UC-Lösung wären. Dies hat dazu beigetragen, die Entwicklung zu beschleunigen und die Kosten zu reduzieren. "

Aber auch aktuelle Fallbeispiele zeigen, dass Kommunikation über Unternehmensgrenzen hinweg in Betriebsprozesse eingebunden werden muss, die weit mehr zur Verfügung stellen als den bloßen Austausch von Sprachinformationen.

Viele von ihnen kennen das Problem, dass, wenn sie online ein Girokonto eröffnen möchten, die kontoführende Bank die Identität des Antragstellers überprüfen muss. Bisher war dies nur über Verfahren wie Post-Ident oder durch einen persönlichen Besuch in einer Bankfiliale möglich, was in beiden Fällen immer einen gewissen Aufwand mit sich brachte. Diese Vorgehensweise kann nun ad acta gelegt werden. Internet Banken wie die DKB nutzen hierzu seit einiger Zeit die Möglichkeit von Web-ID.

Dabei werden alle Kundendaten online übermittelt und geprüft und anschließend mittels eines Video-Calls, z.B. Skype, die Identität des Antragstellers überprüft, indem dieser ein Ausweisdokument vor die Videokamera hält.

Wie dieses Beispiel zeigt wird hier mittels UC, in diesem Fall ein Video-Call, ein Betriebsprozess gestaltet, der zusätzlich Teilnehmer außerhalb der eigenen Institution erfasst. Dies wäre mit einer Lösung basierend auf Vermittlungstechnik nur schwer möglich.

Diese neuen Anforderungen an die Prozesse im Unternehmen fallen dabei zusammen mit zwei einschneidenden technischen Neuerungen. Zum einen wäre da die aufgedrängte Migration zu All-IP durch die Netzbetreiber und zum anderen der kometenhafte Aufstieg von WebRTC.

Beide Entwicklungen werden dem Cloudmarkt einen starken Schub mit auf den Weg geben.

Die Gründe hierfür sind leicht zu erklären. Schauen wir dabei zunächst auf die Auswirkungen von All-IP.

Durch die zwangsweise Umstellung des Zugangs zum öffentlichen Telefonnetz werden viele Betreiber einer klassischen non-VoIP TK-Anlage gezwungen sich über deren Zukunft Gedanken zu machen. Dabei stehen ihnen zwei Optionen zur Verfügung:

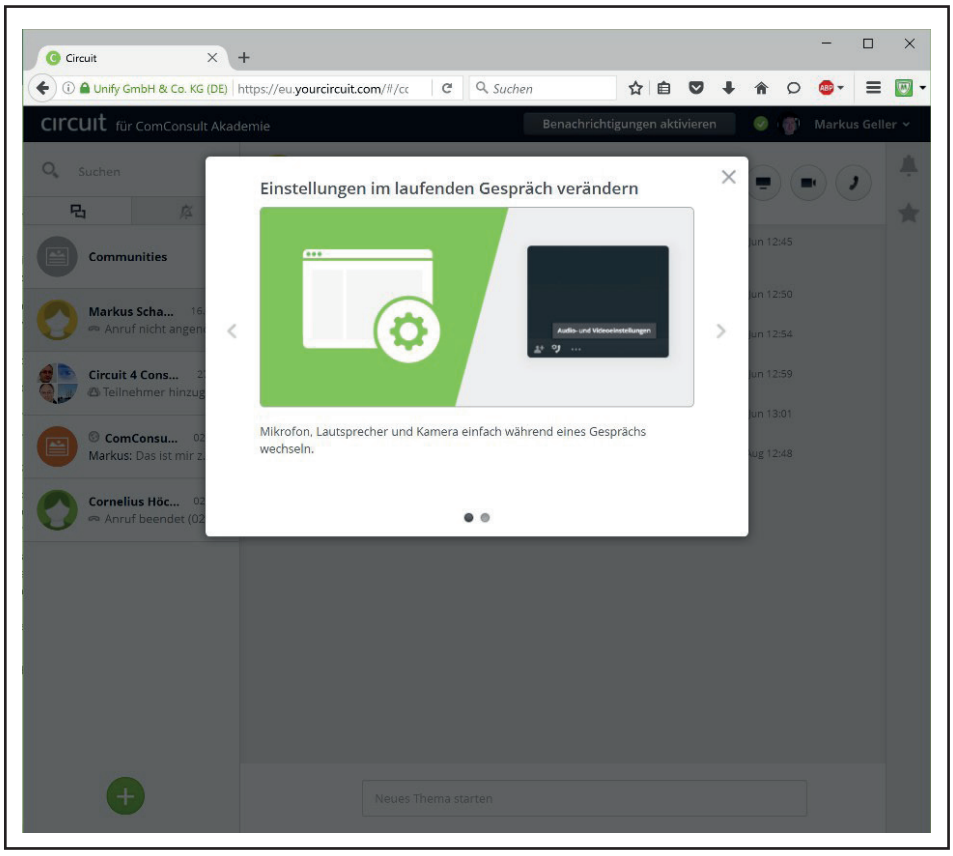

Abbildung 5: Unify Spark GUI

1. Sie verhalten sich passiv und nutzen ein Gateway, welches die digitale Vermittlung an den All-IP Anschluss anpasst und machen einfach so weiter. Aber Vorsicht: zum einen verbauen Sie sich dadurch die Teilhabe an neuen Entwicklungen, die auf All-IP beruhen. Und zum anderen sollten Sie bedenken, dass klassische Vermittlungstechnik langsam ausstirbt, was man heute schon beim Thema Ersatzteilversorgung und technischem Know-how seitens der Hersteller solcher Anlagen beobachten kann.

2. Sie ergreifen die Chance und planen die Umstellung Ihrer TK-Dienste in Richtung VoIP. Durch eine Bestandsaufnahme Ihrer Anforderungen und einem entsprechenden Vergleich der am Markt befindlichen Lösungen können Sie sich im Anschluss pro oder contra Cloud entscheiden. Dabei werden Sie nicht gezwungen eine vollständige Migration hin in Richtung UC zu vollziehen. Nutzen Sie zunächst das, was Sie wirklich benötigen (Pay what you need) und überlegen Sie dann, ob einsetzbare UC Komponenten sich in Betriebsprozesse integrieren lassen und welche Mitarbeiter davon konkret betroffen sind oder profitieren.

Die Auswirkungen sind offensichtlich. Viele unserer Kunden haben geradezu auf den entscheidenden Auslöser gewartet um ihre Alt-Systeme abzulösen.

Der zweite große Treiber ist WebRTC. Ich möchte an dieser Stelle nicht die Grundlagen dieser Technologie erläutern (wer sich hierfür interessiert den möchte ich auf einen entsprechenden Insider Artikel vom September 2013 verweisen).

Jedoch muss man feststellen, dass die Entwicklung dieser Technologie einen unglaublichen Boom im UC-Markt ausgelöst hat. Alle etablierten UC-Hersteller sind vertreten:

Cisco Spark, Unify Circuit, Alcatel Lucent Rainbow, Mitel MiCollab, Innovaphone myPBX, Google Hangouts uva. zeigen, welches Potential die Technik mit sich bringt.

Der große Vorteil jedoch, den WebRTC ausspielen kann, ist die Unabhängigkeit von einem Betriebssystem oder einer speziell auf die UC-Plattform abgestimmten Client Software.

Durch die Auslegung als reine HTML5 Implementierung wird es in naher Zukunft von allen Browsern unterstützt werden. Die aktuellen Probleme ergeben

sich aus einer gewissen Verweigerungshaltung seitens Microsoft und Apple, wer aber heute schon Chrome, Opera oder Firefox als Webbrowser einsetzt, kann vollumfänglich mit den genannten UC-Plattformen arbeiten.

Aber Vorsicht, auch hier gibt es ein paar kleine Einschränkungen. So empfiehlt Cisco für seine Spark Umgebung die Verwendung des Chrome Browsers, während Unify Circuit auf Firefox abgestimmt ist.

Diese Empfehlungen sind durchaus ernst zu nehmen, da es sonst zu Problemen bei der Wiedergabe von Sprach- und Videodaten kommen kann oder aber die Auswahl der verwendeten Hardware, wie Mikrofon, Lautsprecher oder Kamera, nicht funktioniert.

Dies sind jedoch Kinderkrankheiten, wenn man bedenkt, dass die ersten kommerziellen Produkte erst seit zwei Jahren verfügbar sind.

Die Vorteile hingegen überwiegen, mit WebRTC ist es erstmals möglich ohne großen Aufwand Kollaboration, Video und Sprache über die eigene Unternehmensgrenze hinaus einzusetzen und mit Kunden und Partner neue Wege in der Kommunikation einzuschlagen.

Dieser Artikel kann natürlich nicht alle Aspekte der aktuellen Umbrüche im VoIP und UC-Markt beleuchten, jedoch möchte ich Sie in diesem Rahmen auf unser diesjähriges ComConsult UC-Forum vom 21. bis 23.11.2016 im Van der Valk Airporthotel Düsseldorf verwiesen, wo wir die hier angesprochenen Themen vertiefen und viele weitere Aspekte beleuchten werden.

Aktueller Kongress

Frühbucherphase bis 15.09.16
ComConsult UC-Forum 2016
21.11. - 23.11.16 in Düsseldorf

Die ComConsult Akademie veranstaltet vom 21.11. bis 23.11.16 ihr "ComConsult UC-Forum" in Düsseldorf.

Das ComConsult UC-Forum 2016 analysiert die herausragenden Trends für UC und VoIP und gibt Empfehlungen für Projekte, Technologie-Auswahl und Investitionen.

Folgende Themen stehen im Mittelpunkt des UC-Forums:
- UC aus der Cloud inklusive einer Analyse der Rolle Microsofts: pro und kontra!
- All-IP und die Abschaltung von ISDN: Konsequenzen, Migration, Technologie!
- Der Arbeitsplatz der Zukunft und seine Gestaltung: die Rolle von UC in einem Gesamt-Bild!

UC aus der Cloud wird nach Einschätzung von ComConsult Research das Mega-Thema der nächsten Jahre werden. Dabei geht es sowohl um die vollständige Verlagerung der bisher lokalen UC-Anlage als auch um eine selektive Erweiterung einer weiterhin lokalen Anlage durch Cloud-Funktionen.

Wir analysieren dabei für Sie:
- Ist UC aus der Cloud funktional gleichwertig?
- Wird UC aus der Cloud langfristig die Standard-Lösung werden?
- Werden alle Endgeräte unterstützt?
- Werden alle Standorte unterstützt?
- Wie sieht der technische Zugang aus und wie abhängig ist er von einem übergreifenden WAN/Internet Konzept?
- Wie wird Video umgesetzt?
- Stehen alle typischen Erweiterungen zur Verfügung?
- Wie sind Kollaborations-Funktionen integriert?
- Wie werden Drittprodukte integriert?
- Wo liegen die wirtschaftlichen und technischen Vorteile?
- Wie weit müssen sich die UC-Betreiber mit der Cloud vergleichen lassen?
- Wo sind mögliche Nachteile?
- Wie groß wird die Abhängigkeit von einer UC-Cloud-Lösung?
- Was muss zwingend für eine hohe Verfügbarkeit getan werden?

Die Diskussion der UC-Cloud führt zwangsläufig zur Rolle Microsofts in diesem Markt. Office 365 nimmt an Bedeutung zu und die Integration von „Skype for Business“ wird unabwendbar dazu führen, dass die meisten Unternehmen diese Variante in der einen oder anderen Form evaluieren müssen. Sollte Microsoft endlich den lange erwarteten Übergang ins PSTN zu günstigen Tarifen schaffen, wird das erhebliche Konsequenzen für den Markt haben.

Wir analysieren deshalb für Sie:
- Ist Skype for Business funktional ebenbürtig zu einer traditionellen UC-Lösung?
- Wo liegen Stärken und Schwächen?
- Welche Vor- und Nachteile hat ein reines Microsoft Ökosystem am Arbeitsplatz?
- Wie stellt sich Microsoft die VideoIntegration von morgen vor?
- Was ist die Vision hinter “Surface-Hub”?
- Office Delve - wie gläsern darf Kommunikationsverhalten sein?
- Wie werden Drittprodukte integriert?
- Wie können externe Kommunikationspartner einbezogen werden?

Das dominante Thema für 2016 und 2017 ist aber weiterhin All-IP, sprich die Abschaltung der ISDN- und PSTN-Infrastruktur. Diese geht einher mit einer Welle neuer Dienste und einer Neugestaltung des Mobilfunks. Vereinfacht gesagt entsteht eine völlig neue Kommunikationswelt.

Wir analysieren für Sie:
- Wird All-IP wirklich bis 2018 umgesetzt?
- Wird All-IP die Kunden bis 2018 überhaupt betreffen?
- Was bedeutet die Abschaltung, wie sieht die neue Infrastruktur aus?
- Wie weit werden sich die Provider unterscheiden?
- Welche Technologien rücken in den Mittelpunkt und müssen zwingend beherrscht werden?
- Session Border Controller: Markt und Technik einer Schlüsseltechnologie
- SIP Connect 2.0: genügt der Standard endlich den Ansprüchen?
- Wie wirkt sich All-IP auf die Wirtschaftlichkeit der Festnetz-Anbindung aus?

Dabei darf nicht übersehen werden, dass der Markt weiterhin im Wandel ist. Die jetzige Anbieter-Struktur steht vor einer weiteren Bereinigung. Dabei setzen die verschiedenen Hersteller auch unterschiedliche Schwerpunkte.

Wir stellen uns dementsprechend auf dem UC-Forum 2016 den Fragen:
- Wo steht der Markt, wie verändert sich die Position der Hersteller, wer hat im Moment die beste Lösung?
- Migration im Enterprise und KMU Umfeld: was hat sich bewährt, was ist kritisch?
- Spezialfälle und Sonderschaltungen: wie funktioniert das? (Beispiele: E-Cash, Gefahrenmeldeanlagen)

Mit den aktuellen Änderungen der Technik ändern sich auch die Arbeitsplätze. Dies generiert neue Chancen für mehr Effizienz bei sinkenden Kosten, aber es generiert auch eine Reihe ernst zu nehmender Probleme. Gerade hier hat Microsoft in diesem Jahr eine Reihe von interessanten Ankündigungen und Produkten lanciert, die wir natürlich genauer analysieren möchten. Zudem sind jetzt auch die WebRTC-basierten Produkte Unify Circuit und Cisco Spark verfügbar, die ja eine neue Art der Kommunikation und Kollaboration mittels Browser-Technologie ermöglichen. Dieser Entwicklung tragen wir mit unserem Intensivtag Rechnung, für den wir alle relevanten Anbieter auf der Basis eines RFI zu einem Wettbewerb um die beste Lösung einladen.

Seien Sie dabei und erhalten Sie die aktuellsten Trendanalysen und Informationen von ComConsult Research mit Top-Referenten, Analysen, Projektberichten und Praxiserfahrungen.

Programmübersicht ComConsult UC-Forum 2016

Montag 21.11.2016 - UC 2016 – Cloud und Co.

9:30 - 10:15 Uhr
Keynote
- Wo steht der Markt für UC, Video und Collaboration?
- Was wurde eigentlich aus WebRTC?
- Welche Fragen wirft All-IP auf?
- Gibt es ein Leben ohne die Cloud?
- Welche Trends gestalten den Arbeitsplatz der Zukunft?

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

10:15 - 11:00 Uhr
UC goes http:
WebRTC Anwendungen im Vergleich
- Kommunikation ist mehr als telefonieren
- Warum ist Web Technik hierfür ideal
- Wie schlagen sich die Lösungen etablierter Hersteller: Cisco Spark, Unify Circuit, Alcatel Lucent Enterprise Rainbow, ...

Markus Geller, ComConsult Research GmbH

11:00 - 11:30 Uhr Kaffeepause

11:30 - 12:15 Uhr
Monitoring für Enterprise VoIP-Dienste
- Warum nicht Wireshark?
- Qualität von VoIP - Woran hakt es?
- Testing vs. Monitoring - ein integrierter Ansatz
- Übersprechen, Fax-Abbrüche - Troubleshooting-Beispiele aus der Praxis

Dr. Michael Wallbaum, VOIPFUTURE GmbH

12:15 - 12:45 Uhr
Wie reif ist Skype for Business als TK-Ersatz
- Wofür braucht man noch TK-Anlagen wenn es Skype-for-Business gibt?
- Wo liegen die Stärken und Schwächen von S4B?
- Wie stellt sich Microsoft die Video-Integration von morgen vor?
- Was ist die Vision hinter „Surface Hub“?
- Ist Skype-for-Business untrennbar mit Office365 verbunden?

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

12:45 - 13:00 Uhr
Tour Guide zur Ausstellung
- Welche Aussteller sind im Forum vertreten?
- Welche Trends lassen sich an der Ausstellung ablesen?
- Was sind die persönlichen Highlights?

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

13:00 - 14:30 Uhr Mittagspause

14:30 - 15:15 Uhr
Arbeitsplatz-Optimierung - Office Delve und Office Graph als Fitness App für das Berufsleben
- Finden Sie heraus, wie effizient Sie kommunizieren, um Ihre Leistungsfähigkeit zu steigern
- Das intelligente Werkzeug erkennt, mit wem und woran Sie arbeiten und verbindet Sie mit neuen relevanten Informationen und Kontakten
- Erkennen Sie, womit andere sich momentan beschäftigen, mit wem sie zusammenarbeiten und wo ihre Kompetenzen liegen
- Office Delve zeigt auf, womit Sie Ihren Arbeitstag verbringen (E-Mails, Besprechungen, …) und ermöglicht Ihnen eine bessere Zeiteinteilung
- Sie erfahren, mit wem Sie wie viel Zeit verbringen und wer mehr Aufmerksamkeit benötigt

Christian Sailer, Microsoft Deutschland GmbH

15:15 - 15:45 Uhra
Blick hinter die Kulissen: innovaphone Cloud
- Architekturkomponenten: PBX, Session Border Controller, Reverse Proxy, PSTN Anbindung (ISDN/SIP/Federation)
- Redundanzmöglichkeiten
- Multiservicefunktionen: Videokommunikation, Desktopsharing, WebRTC Toolbox
- Ende zu Ende Sicherheit durch DTLS Verschlüsselung

Lars Dietrichkeit, innovaphone AG

15:45 - 16:15 Uhr Kaffeepause

16:15 - 16:45 Uhr
Liefert die Cloud die bessere UC-Lösung?
- Wie sehen die UC-Angebote in der Cloud aus?
- Werden alle Funktionsbereiche abgedeckt?
- Welche Anforderungen entstehen an die Verbindung zur Cloud?
- Wie wird Video umgesetzt?
- Ist die Cloud als UC-Lösung wirklich preiswerter?
- Wie können Drittprodukte integriert werden, geht das überhaupt?
- Wie sieht der Betrieb aus, ist er mehr oder weniger aufwendig als eine lokale UC-Lösung?

Markus Geller, ComConsult Research GmbH

16:45 - 17:45 Uhr
Podiumsdiskussion:
UC aus der Public Cloud, Pro‘s und Con‘s
Mit Herstellern auf dem Podium

ab 18:00 Uhr Happy Hour

Dienstag 22.11.2016 - All-IP

9:00 - 9:45 Uhr
SIPconnect 2.0: Neuer Standard für SIP Trunking
- SIPconnect 1.1 • SIPconnect 2.0
- Architektur • Voice-LM
- Video-Unterstützung
- IPv6 • Notruf

Dipl.-Inform. Petra Borowka-Gatzweiler, UBN

9:45 - 10:30 Uhr
All-IP Migration aus Carrier- und Kundensicht
- Warum überhaupt All-IP?
- Neue Carrier-Infrastuktur, neue SIP- und VPN-Services: Was ändert sich und wann?
- Chancen durch All-IP: Neue Designansätze bei Sprach- und Datennetzen

Dipl.-Ing. Wilfried Meer, T-Systems International GmbH

10:30 - 11:00 Uhr Kaffeepause

11:00 - 11:30 Uhr
Was passiert mit Sonderanschaltungen an TK-Systemen bei der ISDN-Abschaltung

Henry Lakatos, D.I.E. Projekt GmbH

11:30 - 12:00 Uhr
Einsatzszenarien eines Avaya SBC für Enterprise – weit über SIP-Trunking hinaus!
Relevanz eines SBC an der Demarkationslinie zum Unternehmen
- 5 Gründe für einen Avaya SBCE im Unternehmen (Mehr als nur eine Firewall!, Remote-User, WebRTC, Multimedia, Recording)
- Wie sieht eine SIP Connect Zertifizierung aus?

Thomas Römer, Avaya Deutschland GmbH

12:00 - 12:30 Uhr
All-IP in Filialszenarien
- Was unterscheidet All-IP in Filialszenarien von anderen Szenarien?
- Was ist bei Filialszenarien zu beachten? Wo liegen die Fallstricke?
- Wie sehen Architekturen aus und mit welcher Technik setzt man sie um?

Markus Emde, ComConsult Beratung und Planung GmbH

12:30 - 14:00 Uhr Mittagspause

14:00 - 14:30 Uhr
Cisco Collaboration Cloud
- Neue Modelle der Zusammenarbeit unter Berücksichtigung von veränderten betrieblichen Anforderungen
- Integration von interaktiven Hilfsmitteln und Endgeräten in eine gesamtseitliche SaaS Lösung
- Einbindung von Anwendungen über offene APIs
- Wie adressiert die Lösung die Sicherheitsanforderungen und den Schutz der Privatsphäre

Tobias Neumann, Cisco Systems GmbH

14:30 - 15:15 Uhr
Datenschutz bei der Umstellung auf All-IP
- Verschlüsselungsanforderungen und Netztrennung
- SIP-Trunking und Verschlüsselung
- Anforderungen durch das IT-Sicherheitsgesetz und die Cyber-Security-Richtlinie der EU
- Anforderungen durch die EU-Datenschutzverordnung ab Mai 2018

Ulrich Emmert, esb Rechtsanwälte

15:15 - 15:45 Uhr Kaffeepause

15:45 - 16:45 Uhr
Enterprise Session Border Controller: Evaluierung
- Einsatzbereiche: UNI, NNI, E-SBC
- Funktionsbereiche
- ALE, Avaya, Cisco, Mitel, Unify

Dipl.-Inform. Petra Borowka-Gatzweiler, UBN

Programmübersicht ComConsult UC-Forum 2016

Mittwoch 23.11.2016 - Zusatztag „Arbeitsplatz der Zukunft“

9:00 - 9:45 Uhr
Einführung zum RfQ „Arbeitsplatz der Zukunft“
- Welche Anforderungen stellen sich an den Arbeitsplatz der Zukunft?
- Welche Szenarien und Use Cases wurden im RfQ angefragt?
- Welche Hersteller und Lieferanten beteiligen sich an der Live-Demo?

Dipl.-Ing. Dominik Zöller, ComConsault Beratung und Planung GmbH

9:45 - 12:00 Uhr (integrierte Kaffeepause)
Live-Demos zum RfQ „Arbeitsplatz der Zukunft“
Referenten der teilnehmenden Hersteller und Lieferanten
- Führung zu den Live-Demo-Stationen der Aussteller
- Präsentation von Use-Cases
- Anschauen und Ausprobieren von realen Arbeitsplatzszenarien

12:00 - 12:45 Uhr
Wieviel Social Collaboration braucht ein Unternehmen?
- Wie relevant ist Social Collaboration für Unternehmen?
- Wann sollte man mit Social Collaboration starten?
- Wie führt man Social Collaboration ins Unternehmen ein?

Dr. Thomas Kreye, CEO, Just Software AG

12:45 - 13:45 Uhr Mittagspause

13:45 - 15:00 Uhr
Diskussionsrunde „Arbeitsplatz der Zukunft“
- Offene Diskussionsrunde mit Ausstellern und Teilnehmern
- Anregungen und Kritik zu den gezeigten Arbeitsplatzkonzepten
- Erfüllen die gezeigten Arbeitsplätze die Teilnehmererwartungen?
- Erfahrungsaustausch

15:00 - 15:45 Uhr
Arbeitsplatztransformation und Change-Management
- Wie führt man neue Technologien am Arbeitsplatz ein?
- Wie wichtig ist Change Management für die Arbeitsplatztransformation?
- Welche CM-Maßnahmen haben sich in der Praxis bewährt?

Johanna Ahrens, avodaq AG

15:45 - 16:00 Uhr
Wrap-up des Tages
Dipl.-Ing. Dominik Zöller, ComConsult Beratung und Planung GmbH

Zusatztag "Arbeitsplatz der Zukunft"

Der dritte Tag des ComConsult UC-Forums widmet sich traditionell einem Schwerpunktthema, welches wir gemeinsam mit Ihnen intensiv beleuchten möchten. In diesem Jahr steht der „Arbeitsplatz der Zukunft“ im Fokus:

- Wie sieht die Software-Ausstattung des zukünftigen Arbeitsplatzes aus?
- Welche Anforderungen stellen Mitarbeiter an den Arbeitsplatz der Zukunft?
- Welche Visionen (und Geschäftsmodelle?) verfolgen die Hersteller und Anbieter?
- Werden sie den Anforderungen der Unternehmen gerecht?

Diese Fragen können Sie direkt an die Experten renommierter Anbieter adressieren. Und da PowerPoint bekanntermaßen ein geduldiges Medium ist, stellen sich die Anbieter diesen Fragen an ihren Live-Demo-Stationen. Hier erhalten Sie einen näheren Einblick in Lösungen und Innovationen und können sie teils selbst erproben. Natürlich sind UC- und Video-Systeme nur EIN Bestandteil des Arbeitsplatzes von morgen. Document-Sharing, Self-Service Apps und Collaboration Tools sind mindestens ebenso wichtig. Und so möchten wir Ihnen als Teil des Rahmenprogramms einen Einblick geben, wie man Social Collaboration richtig macht. Dr. Thomas Kreye, CEO der Hamburger JUST Software AG erklärt, wieviel Kollaboration ein Unternehmen wirklich braucht. Im Nachgang diskutieren wir gemeinsam die Erlebnisse des Vormittags und geben den Anbietern ein Feedback zu ihren Lösungen. Zum Abschluss des Tages widmen wir uns dann der Fragestellung, wie man die Arbeitsplatztransformation richtig angeht und welche Rolle ein solides Change Management hierbei spielt. Den zeitlichen Ablauf der Veranstaltung entnehmen Sie bitte der folgenden Agenda. Wir freuen uns auf Ihre Teilnahme!

Fax-Anmeldung an ComConsult 02408/955-399

ComConsult UC-Forum 2016

Ich buche den Kongress
ComConsult UC-Forum 2016

☐ Kongress mit Zusatztag
21.11. - 23.11.16 in Düsseldorf
€ 2.190,-- (statt € 2.390,--)*

☐ Kongress ohne Zusatztag
21.11. - 22.11.16 in Düsseldorf
€ 1.790,-- (statt € 1.990,--)*

☐ Zusatztag am 23.11.16
€ 790,-- (statt € 990,--)*

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

*Preise gültig bis zum 15.09.16. Danach gelten die regulären Preise.

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

ComConsult Veranstaltungskalender

Lokale Netze für Einsteiger, 19.09.-23.09.16 in Aachen

Garantietermin

Dieses Seminar vermittelt kompakt und intensiv innerhalb von 5 Tagen die Grundprinzipien des Aufbaus und der Arbeitsweise Lokaler Netzwerke. Dabei werden sowohl die notwendigen theoretischen Hintergrundkenntnisse vermittelt als auch der praktische Aufbau und der Betrieb eines LANs erläutert. Ausgehend von einer Darstellung von Themen der Verkabelung und der grundlegenden Übertragungsprotokolle werden die wichtigen Zusammenhänge zwischen der Arbeitsweise von Switch-Systemen, den darauf aufsetzenden Verfahren und der Anbindung von PCs und Servern systematisch erklärt.

Preis: € 2.490,-- netto

IP-Wissen für TK-Mitarbeiter, 19.09.-20.09.16 in Frankfurt

Garantietermin

Dieses Seminar vermittelt TK-Mitarbeitern ohne Vorkenntnisse im Bereich LAN und IP das erforderliche Wissen zur Planung und zum Betrieb von VoIP-Lösungen. Die Inhalte sind so gegliedert, dass Sie die Grundlagen schnell verstehen. Es werden die wichtigsten VoIP spezifischen Aspekte vorgestellt und unter Praxis-relevanten Gesichtspunkten beleuchtet. Die Themen erstrecken sich von IP und LAN Grundlagen hin zu Praxis relevanten Themen wie QoS, Jitter und Bandbreiten Fragen. Ziel ist es dem IP-Unkundigen die wichtigen Grundlagen der Netzwerk Technik kompakt und praxisnah zu vermitteln.

Preis: € 1.590,-- netto

Das PSTN stirbt: Die neue Kommunikation mit SIP/IP 21.09.16 in Frankfurt

Garantietermin

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.

Preis: € 1.090,-- netto

Die neue EU-Datenschutzgrundverordnung, 21.09.16 in Frankfurt

Garantietermin

Am 25.05.2016 ist ein neues einheitliches Datenschutzrecht in der Europäischen Union in Kraft getreten. Es gibt noch eine Übergangsfrist bis zum 25.05.2018, die Zeit ist jedoch knapp, um sich auf die tiefgreifenden Änderungen des Datenschutzrechts und vor allem die neue Haftung für Auftragsdatenverarbeiter und die Erhöhung der möglichen Bußgelder vorzubereiten. So wird es gravierende Änderungen bei der Verarbeitung von sensiblen Daten und bei der grenzüberschreitenden Datenverarbeitung geben. Informieren Sie sich frühzeitig über die geplanten Regelungen, damit Sie jetzt schon wissen, was auf Ihr Unternehmen zukommt.

Preis: € 1.090,-- netto

Trouble Shooting in vernetzten Infrastrukturen, 27.09.-30.09.16 in Aachen

Garantietermin

Dieses Seminar vermittelt, welche Methoden und Werkzeuge die Basis für eine erfolgreiche Fehlersuche sind. Es zeigt typische Fehler, erklärt deren Erscheinungsformen im laufenden Betrieb und trainiert ihre systematische Diagnose und die zielgerichtete Beseitigung. Dabei wird das für eine erfolgreiche Analyse erforderliche Hintergrundwissen vermittelt und mit praktischen Übungen und Fallbeispielen in einem Trainings-Netzwerk kombiniert. Die Teilnehmer werden durch dieses kombinierte Training in die Lage versetzt, das Gelernte sofort in der Praxis umzusetzen. Als Protokoll-Analysator-Software kommt Wireshark zum Einsatz. Einer Verwendung selbst mitgebrachter Analyse-Software, mit deren Bedienung der Teilnehmer vertraut ist, steht nichts im Wege.

Preis: € 2.290,-- netto

Crashkurs IT-Recht für Nichtjuristen, 05.10.16 in Düsseldorf

Garantietermin

Die Veranstaltung bildet eine kompakte Grundorientierung über das unübersichtliche Rechtsgebiet des IT-Rechts. Teilnehmern, die sich wiederkehrend mit rechtlichen Fragestellungen in der Informationstechnologie beschäftigen, wird vermittelt, wo Herausforderungen und Haftungsrisiken liegen, welche Probleme auch als Laie handhabbar sind und in welchen Fällen externes Know-How unerlässlich ist.

Preis: € 1.090,-- netto

Der Client der Zukunft, 05.10.-06.10.16 in Bonn

Garantietermin

Der klassische PC-Arbeitsplatz hat ausgesorgt. Längst verlässt sich eine Vielzahl der Mitarbeiter im Unternehmen tagtäglich auf ihr mobiles Arbeitsgerät. Die Gründe liegen nicht nur in der technischen Machbarkeit: auch unsere Arbeitsweise verändert sich unter den Einflüssen der Globalisierung und Digitalisierung. Doch was bedeutet das für die Software-Ausstattung der Clients und die zugehörigen IT-Infrastrukturen? In diesem Seminar entwickeln wir gemeinsam mit Ihnen Arbeitsplatzkonzepte, die den Anforderungen an den „Client der Zukunft“ gerecht werden.

Preis: € 1.590,-- netto

Netzwerk-Design für Enterprise Netzwerke, 05.10.-07.10.16 in Düsseldorf

Garantietermin

LAN-Technik wird im Moment neu erfunden. Neue Anforderungen erfordern neue Lösungen. Neue Fabric-Konzepte, ein Umdenken bei VLAN-Technik, eine Neupositionierung von QoS und neue Nutzungsformen im Rahmen von Audio-/Video-Bridging sind herausragende Beispiele. Das Seminar zum Thema Netzwerk-Design für Enterprise Netzwerke erklärt, was im Moment passiert und wie Sie sich auf die Zukunft vorbereiten. Es geht auf RZ- und Campus Design-Alternativen im Zeitalter neuer Layer-2 Technologien wie Fabrics, Multichassis-Link Aggregierung, Shortest Path Bridging und Hochgeschwindigkeits-Datenraten von 10/40/100 Gbit ein. Darüber hinaus werden Priorisierungs-Techniken wie AVB und DCB sowie der sinnfällige Einsatz von VLAN-Technik und VLAN-Overlays behandelt.

Preis: € 1.890,-- netto

Private Cloud rechtssicher auslagern - Vertragsgestaltung für Nichtjuristen, 05.10.-06.10.16 in Bonn

Garantietermin

Dieses Seminar erklärt, wie Sie die Auslagerung Ihrer Private Cloud vertraglich absichern und warum Sie das unbedingt machen sollten.

Preis: € 1.590,-- netto

Elektronische Akte, Dokumentenmanagement und Digitalisierung, 24.10.-25.10.16 in Frankfurt

Der öffentliche Dienst muss nach dem E-Government-Gesetz bis 2020 die elektronische Akte einführen, viele Unternehmen scheuen noch aus Gründen der Beweissicherheit den Umstieg auf elektronische Aktenführung und den Verzicht auf Papierdokumente, dabei sind die rechtlichen Grundlagen längst geschaffen.

Preis: € 1.590,-- netto

Zertifizierungen

ComConsult Certified Network Engineer

Lokale Netze
19.09. - 23.09.16 in Aachen
13.02. - 17.02.17 in Aachen
08.05. - 12.05.17 in Aachen

TCP/IP-Netze erfolgreich betreiben
24.10. - 26.10.16 in Bonn
13.03. - 15.03.17 in Aachen
29.05. - 31.05.17 in Aachen

Internetworking
14.11. - 18.11.16 in Aachen
03.04. - 07.04.17 in Aachen
19.06. - 23.06.17 in Göttingen

Paketpreis für zwei 5-tägige und ein 3-tägiges Intensiv-Seminar € 6.180,-- netto (Einzelpreise: € 2.490,-- netto bzw. 1.890,-- netto)

ComConsult Certified Trouble Shooter

Trouble Shooting in vernetzten Infrastrukturen
27.09. - 30.09.16 in Aachen
02.05. - 05.05.17 in Aachen

Trouble Shooting für Netzwerk-Anwendungen
15.11. - 18.11.16 in Aachen
27.06. - 30.06.17 in Aachen

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

ComConsult Certified Voice Engineer

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen
24.10. - 26.10.16 in Frankfurt
13.03. - 15.03.17 in Köln
15.05. - 17.05.17 in Düsseldorf

Session Initiation Protocol Basis-Technologie der IP-Telefonie
09.11. - 11.11.16 in Berlin
05.04. - 07.04.17 in Bonn
29.05. - 31.05.17 in Frankfurt

Umfassende Absicherung von Voice over IP und Unified Communications
28.11. - 30.11.16 in Bonn
08.05. - 10.05.17 in Frankfurt
10.07. - 12.07.17 in Düsseldorf

Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter
19.09. - 20.09.16 in Frankfurt
20.02. - 21.02.17 in Bonn
02.05. - 03.05.17 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,-- netto statt € 5.670,-- netto
Optionales Einsteigerseminar: Aufpreis € 1.190,-- netto statt € 1.590,-- netto

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: insider@comconsult-akademie.de
http://www.comconsult-research.de

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

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