ComConsult Research

Der Netzwerk Insider

Dezember 2017

Systematische Weiterbildung für Netzwerk- und IT-Professionals

IEEE 802.11ax: die neue WLAN Generation

von Dr. Franz-Joachim Kauffels

Mit IEEE 802.11ax kommt ein neuer WLAN-Standard auf uns zu. Im Mittelpunkt steht im Gegensatz zu den Vorgängern bis 11ac aber weniger eine weitere Steigerung der nominalen Zellen-Datenrate, sondern vielmehr die Verbesserung der Fairness für die Datenübertragung von Stationen. Allerdings konzentriert sich der Standard dabei auf bestimmte Anwendungsszenarien, bei denen sehr viele Nutzer auf sehr engem Raum zusammenkommen. Wir untersuchen die neuen Funktionen und stellen die Frage, ob 802.11ax wirklich nützlich für die Realisierung flächendeckender Wireless Versorgungsstrukturen in Unternehmen und Organisationen sein kann. Die Antwort ist anders, als man vielleicht vermuten könnte.

„Ja, ist das denn schon wieder nötig?“ Diese Frage ist sicherlich eine häufige Reaktion auf die neue WLAN-Generation IEEE 802.11ax. Die meisten Betreiber in Unternehmen und Organisationen verbauen grade die aktuelle Generation 11ac und betreiben sicherlich noch in hohem Maße 11n. Es ist wichtig zu verstehen, dass 802.11ax nicht zu dem Zweck entwickelt wurde, die in einer WLAN-Zelle mögliche aggregate Gesamtleistung gegenüber 802.11ac noch wesentlich zu erhöhen.

weiter ab Seite 10

IT-Sicherheitsgesetz und Kritis-Verordnung - eine „etwas andere“ Betrachtung

von Dipl.-Inform. Oliver Flüs

Das IT-Sicherheitsgesetz (IT-SiG) ist seit 2015 in Kraft. Die damit in Zusammenhang zu sehende Kritis-Verordnung, über die geprüft und entschieden werden kann, ob man die mit dem IT-SiG für Betreiber „kritischer Infrastrukturen“ einhergehenden Auflagen unmittelbar zu beachten und bearbeiten hat, ist mittlerweile für alle betroffenen „Sektoren“ verabschiedet. Für alle „Kritis-Umgebungen“ tickt im Sinne gesetzter Umsetzungsfristen damit die Uhr.

Betrachtet man aber Teilaspekte sowie (Hilfen für) strukturierte Prüfung und Nachweise, die sich zunächst an Betreiber von Kritis-Umgebungen richten, so kann „jeder“ etwas für den Umgang mit aus seiner Sicht „kritischen IT-Lösungen“ davon mitnehmen. In diesem Sinne beleuchtet der vorliegende Artikel das Thema - eine vielleicht etwas ungewöhnliche Betrachtungsweise, aber ein Versuch zu zeigen, dass IT-SiG und zugehörige Umsetzungshilfen für die Praxis wertvoller sind, als man vielleicht zunächst denkt.

weiter auf Seite 22

Geleit

IT-Infrastruktur-Trends 2018 aus der Sicht von ComConsult Research

auf Seite 2

Standpunkt

Im Fokus der Angreifer: Administration der IT-Infrastruktur

auf Seite 32

Neue Sonderveranstaltungen

Herausforderung Cloud

auf Seite 5

Office 365 in der Praxis

auf Seite 6

Kriterien und Erfolgs-Szenarien für den Einsatz von UCC-Produkten

auf Seite 7

Aktueller Kongress

ComConsult Netzwerk Forum 2018

ab Seite 8

Geleit

IT-Infrastruktur-Trends 2018 aus der Sicht von ComConsult Research

Weihnachten steht vor der Tür und es ist an der Zeit sich bewusst die Zeit zu nehmen, um mit etwas Abstand auf die nächsten Jahre zu schauen. Auf was müssen wir uns vorbereiten, was wird unsere Arbeit in den nächsten zwei oder drei Jahren prägen?

ComConsult Research war sehr aktiv in den letzten Monaten und wir haben eine ganze Reihe von Entwicklungen analysiert. Dabei haben sich erstaunlich deutliche Schwerpunkte ergeben, von denen wir glauben, dass sie in Zukunft eine große Rolle spielen werden. Die Liste ist sicher nicht vollständig. Aber wir wollen bewusst Schwerpunkte setzen, wir wollen fokussieren. Dabei konzentrieren wir uns auf Entwicklungen, die nicht zu abgehoben sind, die man anfassen kann und die schon bald im Mittelpunkt realer Projekte stehen werden.

Und hier sind unsere Kandidaten für IT-Infrastrukturen 2018:

1. IT-Infrastrukturen für das Gebäude der Zukunft

Das Gebäude der Zukunft ist geprägt von Sensoren, Aktoren, Beacons, Power over Ethernet als weitreichende Gleichstromversorgung, Funknetze der diversesten Ausprägungen und einem neuen Verständnis vom Arbeitsplatz der Zukunft.

Dies hat gravierende Konsequenzen:

a. Das Denken und Arbeiten in Gewerken kommt bezogen auf IT-Infrastrukturen zu einem Ende (begrifflich bezeichnen wir jeden abgegrenzten Planungs- und Bauauftrag als Gewerk, auch die IT-Planung). Ganz im Sinne von “es kann nur einen geben” muss es eine zentrale Planung aller IT-Infrastrukturen geben und die verschiedenen Gewerke müssen darauf aufsetzen.
b. Dabei kommt es zunehmend zu Überlagerungen zwischen den Gewerken und den genutzten IT-Infrastrukturen. Ein typisches Beispiel sind die Funknetze, die von ZigBee über WLAN bis 5G um die Frequenzen streiten.
c. Die Zeiten, in denen Mieter ihre eigenen Infrastrukturen betreiben konnten, sind vorbei. Es gibt zentrale Infrastrukturen mit Mandanten für Mieter.
d. Das Gebäude der Zukunft ist ein Sicherheits-Risiko der obersten Klasse. Immer mehr IT bedeutet immer mehr Angriffsfläche. Diese Risiken sind

sehr ernst zu nehmen. Und die einzige Lösung besteht in einem zentralen Sicherheitskonzept basierend auf Sicherheit als weisungsgebendes Gewerk gegenüber anderen Gewerken.
e. Der “Zwilling in der Cloud”, der sowohl die Planung als auch den Betrieb moderner Gebäude so vereinfachen und optimieren soll, wird immer mehr zum Thema. Hier liegen Vorteile, aber auch signifikante Sicherheits-Risiken.

Wir greifen dieses Mega-Thema in unserer Veranstaltung "IT-Infrastrukturen für das Gebäude der Zukunft" vom 28.02. bis 01.03.2018 in Bonn auf.

2. Wie kommunizieren wir in der Zeit nach ISDN, was löst Email, Sprache und Video ab?

Email und Sprache dominierten die Kommunikation der Vergangenheit. Diese Zeiten sind vorbei. Die Ablösung von ISDN ist dabei nicht die Ursache, gibt aber einen zeitlichen Trigger, um sich diesem Thema zu stellen. Die Zukunft wird geprägt von einem Mix aus Dokumenten-Kollaboration, Messaging, Video und Sprache mit abnehmender Bedeutung von Sprache und Video. Dabei produziert speziell Dokumenten-Kollaboration einen erheblichen Zugewinn an Effizienz in der Kommunikation. Dies erfordert einen neuen Ansatz für Kommunikation, der von sogenannten UCC Tools geliefert wird (Unified Communications and Collaboration). Damit beginnen denn auch die Probleme. Viele der im Markt angebotenen UCC Produkte kommen aus der Meeting-Welt und liefern zum Teil eine beeindruckende Meeting-Erfahrung. Aber die meisten Produkte haben ihre Tücken in einzelnen Funktionsbereichen. Diese Tücken sind so gravierend, dass ein Projekt daran scheitern kann. Wir haben deshalb eine Kriterienliste zur Auswahl von UCC-Produkten erarbeitet und zum ComConsult UC-Forum veröffentlicht. Diese Liste werden wir weiter vertiefen und Anfang 2018 in erweiterter Form auf den Markt bringen. Sie wird den Mittelpunkt einer UCC-Sonderveranstaltung am 21.03.18 in Bonn darstellen, auf der wir diese Entwicklungen analysieren und diskutieren. Wir sehen in UCC nur eine Übergangstechnik zu UC as a Service. Damit entsteht aber auch die Chance mit einem UCC-Projekt die Tür in eine UC-Zukunft in der Cloud offen zu halten.

3. Software as a Service erobert Unternehmen und Behörden

Die Cloud besteht aus vielen unterschiedlichen Geschmacksrichtungen. Und während Infrastructure as a Service IaaS wie von uns vorhergesagt gescheitert ist, hebt Software as a Service ab. Tatsächlich beobachten wir bei On-Premise-Software einen Technologie-Stillstand, während zeitgleich in der Cloud immer modernere und effizientere Software-Lösungen entstehen. Dies ist nicht das Ende von On-Premise, im Gegenteil, aber es bedeutet, dass sich jedes Unternehmen und jede Behörde dem Thema stellen muss. Und was ist aus IaaS geworden? IaaS wird abgelöst von Platform as a Service. Simple Rechenleistung oder einfach nur Speicher bieten in 90% aller Fälle nicht genügend Mehrwert (das kann sich mit Machine Learning wieder ändern), aber komplette Entwicklungs-Umgebungen speziell für Software-Lösungen, die DMZ-Lösungen ablösen, haben gravierende Vorteile. Das Projektziel heißt hier: dramatische Verkürzung von Entwicklungs- und Pflegezyklen. Von Jahren zu Wochen lautet hier die Devise, und dies ist kein Marketing-Spruch. Lange Rede, kurzer Sinn: Unternehmen und Behörden müssen sich der Cloud stellen. Dies betrifft die Netzwerk-Gestaltung, SSO, den Internet-Zugang, Sicherheit im weitesten Sinne des Begriffs und im Endeffekt die Gestaltung des Arbeitsplatzes der Zukunft. Wir gehen auf dieses Thema in unserer neuen Sonderveranstaltung "Herausforderung Cloud" am 19.03.18 in Bonn ein.

IT-Infrastruktur-Trends 2018 aus der Sicht von ComConsult Research

4. Der Arbeitsplatz der Zukunft

Der Begriff "Arbeitsplatz der Zukunft" ist schon mehrfach gefallen. Aber es ist offensichtlich, dass sich die Art, wie wir Arbeiten, die Technik, mit der wir das machen und die Applikationen, die wir dabei nutzen, in den nächsten fünf bis zehn Jahren deutlich verändern werden. Hier geht es um Wirtschaftlichkeit, Effizienz bis hin zu neuen Formen von Arbeiten. Der Schlüssel wird dabei in der Flexibilität liegen. Unsere Infrastrukturen müssen so ausgelegt sein, dass sie vom Arbeitsplatz in der Cloud auf der Basis von Chrome OS bis hin zum Workstation-Arbeitsplatz für hochwertigste Anwendungen alles unterstützen. Und dies an jedem Ort und auf fast beliebigen Endgeräten. Hier geht es darum, rechtzeitig die Weichen zu stellen, um das eigene Unternehmen oder die Behörde rechtzeitig in die richtige Richtung zu lenken. Wir werden uns diesem Thema mit einer Sonderveranstaltung im 1. Halbjahr 2018 stellen. Den Termin geben wir rechtzeitig bekannt.

5. Vom Sensor bis zur Cloud: das Netzwerk der Zukunft

Das Gebäude der Zukunft ist ein gutes Beispiel für eine neue Form von Netzwerk, das alles vom einfachen Sensor bis hin zu einer komplexen Mikro-Service-Architektur in der Cloud unterstützen muss. Dies hat handfeste Elemente wie die Abgrenzung und Integration von Funkdiensten, aber auch jede Menge virtuelle Bausteine, um Dienste zu berücksichtigen oder die Cloud zum Laufen zu bekommen. Und dabei muss die Kontrolle immer im Unternehmen bleiben. Ein heißes Thema, dem wir uns auf dem ComConsult Netzwerk Forum 2018 vom 16. bis 18. April 2018 in Königswinter stellen.

6. Mehr Intelligenz im Netzwerk-Betrieb: das Ende von CLI naht

Netzwerke werden komplexer, da gibt es keinen Zweifel. Und damit werden sowohl die Konfiguration als auch die Fehlersuche ebenfalls komplexer. Das ist auf Command Line Interface Ebene nicht mehr zu leisten. Und wir brauchen zunehmend Automatismen, um zum Beispiel Angriffe zu identifizieren und Teile des Netzwerks abzutrennen. Unser Netzwerk ist unsere Hauptverteidigungs-Linie gegen Angreifer. Nur hier können wir einen Angreifer wirkungsvoll komplett isolieren. Dies geht einher mit der Diskussion von Künstlicher Intelligenz und Machine Learning im Netzwerk. Wir stehen erst am Anfang dieser Entwicklung und viele der angebotenen Lösungen sind mehr Schein als Sein. Aber der Trend ist ebenso klar wie unumkehrbar. Automatismen und Intelligenz im Betrieb werden die Zukunft bestimmen. Der Netzwerk-Betreiber muss dazu umlernen. Aber keine Sorge, es bleibt noch genug Netzwerk im traditionellen Sinne übrig. Wir analysieren und diskutieren dies auf dem ComConsult Netzwerk Forum 2018 vom 16. bis 18. April 2018 in Königswinter.

Dies sind die Schwerpunkte, die wir momentan für 2018 sehen. Nicht so abgehoben wie bei einigen amerikanischen Analysten, mehr bodennah, aber trotzdem weitgehend in der Veränderung unserer IT. Wir müssen uns dem stellen. Die anstehenden Änderungen umfassen alle Ebenen der IT, vom Client-Betrieb bis zur Gebäudeplanung. Davon ist jeder Mitarbeiter unmittelbar betroffen. Wir unterstützen Sie dabei, auch weiterhin erfolgreich in Ihrem Umfeld zu arbeiten.

Es wird ein spannendes Jahr 2018. Und ComConsult Research wird Sie wie immer dabei begleiten.

In diesem Sinne
Ihr
Dr. Jürgen Suppan

Neue Sonderveranstaltungen

Herausforderung Cloud
19.03.2018 in Bonn

Cloudlösungen ergänzen zunehmend die eigene Infrastruktur. Insbesondere für das Rechenzentrum gilt, dass es sich nur für wenige Unternehmen lohnt, ausreichende Kapazitäten wie Internetzugänge oder Server vorrätig zu halten, um auch Spitzenzeiten abdecken zu können. Diese Veranstaltung richtet sich an alle, die einen gemeinsamen Betrieb von Cloud und Rechenzentrum planen und zeigt u.a. auf, wie die Anforderungen an die Datensicherheit oder die Koppelung erfüllt werden können.

Office 365 in der Praxis
20.03.2018 in Bonn

Software as a Service hat sich zum führenden Servicemodell aus der Public Cloud entwickelt. Office 365 ist in diesen Bereichen zweifellos der Marktführer. Gleichzeitig wird Office 365 gerade in der Einführungsphase maßlos unterschätzt. Viele Unternehmen versuchen mit Office 365 Ihre langjährige Microsoft-Office-Tradition möglichst ohne große Brüche fortzuführen und ignorieren die Auswirkungen, die die Einführung von Cloud-Anwendungen im Allgemeinen und von Office 365 im Besonderen hat.

Sparen Sie 390,- € bei der Buchung beider Sonderveranstaltungen

Sonderveranstaltung: Herausforderung Cloud am 19.03.18:	Preis 1.090,-- €
Sonderveranstaltung: Office 365 in der Praxis am 20.03.18:	Preis 1.090,-- €
Beide Seminare:	Preis 1.790,-- €

Bei Buchung der beiden einzelnen Sonderveranstaltungen wird Ihnen der Rabatt automatisch abgezogen

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

Aktuelles Seminar

IT-Infrastrukturen für das Gebäude der Zukunft

28.02. - 01.03.2018 in Bonn

Die ComConsult Akademie veranstaltet vom 28.02. bis 01.03.2018 ihr Seminar "IT-Infrastrukturen für das Gebäude der Zukunft" in Bonn.

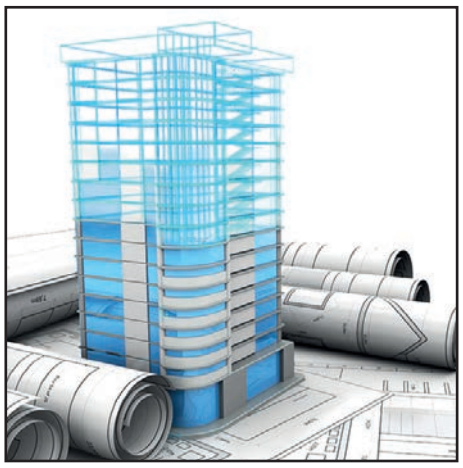
Das Gebäude der Zukunft erfordert IT-Infrastrukturen, die Gewerk-übergreifend sind, die sowohl in der Datenverarbeitung als auch in der Klimatisierung, Zugangssicherung oder allgemeiner gesprochen der Gebäude-Automatisierung eingesetzt werden können. Diese Veranstaltung wendet sich an Planer aller Gewerke und bietet den idealen Blick über den Tellerrand, um zu einer erfolgreichen und wirtschaftlichen Gewerke-übergreifenden Planung zu kommen und einen langfristig flexiblen Betrieb eines neuen Gebäudes zu erreichen.

Die IT-Infrastrukturen der Gebäude der Zukunft umfassen:

- eine Anwendungs-unabhängige Verkabelung
- eine Anwendungs-unabhängige Vorbereitung für unterschiedliche Funknetze
- flächendeckende Funknetze
- eine flächendeckende Gleichstrom-Versorgung auf der Basis Power-over-Ethernet

Auf den genannten Infrastrukturen setzen die verschiedensten Anwendungen in den unterschiedlichen Gewerken auf. Beispiele dafür sind Gebäude-Automatisierung mit Bluetooth, Zigbee, EnOcean oder Beacon-Technologien.

Damit entsteht ein hierarchisches Schichtenmodell von Infrastruktur-Diensten, das



eine Reihe von signifikanten Vorteilen hat:

- es ist wirtschaftlich, es wird nur installiert, was wirklich gebraucht wird und wesentliche Teile der Infrastruktur können von verschiedenen Gewerken gemeinsam genutzt werden
- es ist langlebig und am Nutzungszeitraum des Gebäudes ausgelegt
- es vermeidet Kollisionen oder Überlappungen zwischen Gewerken
- es ist flexibel und gestattet eine schnelle Reaktion auf Bedarfsänderungen im Betrieb des Gebäudes

Dieses Schichtenmodell steht im Einklang mit Building Information Modeling BIM. Es kann in ein BIM-Modell integriert werden, es kann aber auch autonom gesehen werden.

Diese Sonderveranstaltung diskutiert mit Ihnen:

- welchen Infrastruktur-Bedarf das Gebäude der Zukunft erzeugt
- wie eine effiziente, flexible und Gewerke-übergreifende Infrastruktur-Planung erfolgt
- wie Mehrwert-Dienste in einzelnen Gewerken auf diese Basis-Schicht von Infrastruktur aufsetzen

Wir gehen dabei auf eine Reihe von Spezialfragen ein, die helfen, den Aspekt der langfristigen Investitionssicherung abzudecken:

- wie sieht der Arbeitsplatz der Zukunft aus und welche Infrastruktur erfordert er?
- welchen Stellenwert hat eine WLAN-Infrastruktur im Gebäude der Zukunft und wie dicht wird sie geplant?
- was bedeutet Smart Building und wie kann es sauber auf eine Basis-Infrastruktur aufgesetzt werden?
- wie sieht die Anwendungs-neutrale Verkabelung eines Gebäudes aus? Bis wohin sollte sie gebracht werden und ab wann startet der Gewerke-spezifische Teil?
- wo steht Power-over-Ethernet technisch, was ist in den nächsten Jahren zu erwarten und wie kann es Gewerke-übergreifend und flexibel genutzt werden?
- wie effizient können Mehrwertdienste wie Beacon-Technologien integriert werden?
- welche Rolle wird Mobilfunk mit 5G spielen? Inwieweit muss es mit den anderen geplanten Funktechnologien als Einheit gesehen werden?

Anmeldung an kundenservice@comconsult-research.de

IT-Infrastrukturen für das Gebäude der Zukunft

Ich buche das Seminar
IT-Infrastrukturen für das Gebäude der Zukunft

☐ 28.02. - 01.03.2018 in Bonn
zum Preis von 1.690,- € 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

Neue Sonderveranstaltung

Sonderveranstaltung: Herausforderung Cloud

19.03.2018 in Bonn

Die ComConsult Akademie veranstaltet am 19.03.18 ihre neue Sonderveranstaltung "Herausforderung Cloud" in Bonn.

Cloudlösungen ergänzen zunehmend die eigene Infrastruktur. Insbesondere für das Rechenzentrum gilt, dass es sich nur für wenige Unternehmen lohnt, ausreichende Kapazitäten wie Internetzugänge oder Server vorrätig zu halten, um auch Spitzenzeiten abdecken zu können. Diese Veranstaltung richtet sich an alle, die einen gemeinsamen Betrieb von Cloud und Rechenzentrum planen und zeigt u.a. auf, wie die Anforderungen an die Datensicherheit oder die Koppelung erfüllt werden können.

Wer sein Rechenzentrum um Cloud-Lösungen ergänzen will, muss sich bereits im Vorfeld zu verschiedenen Kernthemen Gedanken machen:

- **Anbieter**
  Zunächst stellt sich die Frage, welchen Anbieter er wählen will. Bei weitem nicht alle Anbieter von Cloud-Lösungen verstehen dasselbe unter dem Begriff Cloud. Die Palette reicht von virtuellen Servern, die als „Cloud-Server“ vermarktet werden bis hin zu Anbietern wie Amazon und Microsoft, die ein unüberschaubares Portfolio von Diensten anbieten. Wir beleuchten in dieser Veranstaltung das Angebot und vergleichen die beiden Platzhirsche AWS und Azure anhand eines Projektbeispiels miteinander.

- **Kopplung**
  Reine Cloud-Lösungen sind heute eher eine Seltenheit. In der Regel ergänzen die Cloud-Dienste das eigene Rechenzentrum. Dafür ist es notwendig beides miteinander zu koppeln. Welche Zugangsverfahren werden angeboten und für welche Unternehmen eignet sich welche Technik?

- **Design**
  Wie im eigenen Rechenzentrum muss auch in der Cloud ein Netzdesign erfolgen. Dieses muss zum einen zum eigenen Rechenzentrumsnetz, zum anderen aber auch zu den in der Cloud gehosteten Anwendungen passen. Auch der globale Standort der Nutzer ist bei Cloudlösungen relevant, da diese meist weltweit Rechenzentren anbieten. Wir vergleichen die Angebote der führenden Anbieter und zeigen auf, welche Kriterien ein gutes Design erfüllen muss.

- **Sicherheit**
  Eng mit der Frage des Designs ist die Frage nach der Sicherheit verbunden. Wie muss ein Netz in der Cloud angelegt sein, um größtmögliche Sicherheit zu gewährleisten? Denn gerade Cloud-Dienste sind schnell Angriffen ausgesetzt, da sie oft als öffentliche Dienste über das Internet angeboten werden. Welche Schutzverfahren bieten Cloud-Lösungen von Hause aus an? Welche kann man von Drittanbietern hinzunehmen und was gilt es bei dem Design von Netz- und Anwendung zu beachten?

- **Datenschutz**
  Neben der Zugangssicherheit muss auch der Datenschutz beachtet werden. Welche gesetzlichen Richtlinien sind hier einzuhalten? Was muss beachtet werden? Kann man personenbezogene Daten bei jedem Cloudanbieter hosten oder behält man sie lieber in einen Rechenzentrum? Diese und weitere Fragen zu Recht und Technik werden wir exklusiv für Sie diskutieren.

Sparen Sie 390,- € bei der Buchung beider Sonderveranstaltungen
Herausforderung Cloud am 19.03.18:
Preis 1.090,-- €
Office 365 in der Praxis am 20.03.18:
Preis 1.090,-- €
Beide Sonderveranstaltungen:
Preis 1.790,-- €
Bei Buchung der beiden einzelnen Sonderveranstaltungen wird Ihnen der Rabatt automatisch abgezogen

Anmeldung an kundenservice@comconsult-research.de

Sonderveranstaltung: Herausforderung Cloud

Ich buche die Sonderveranstaltung
Herausforderung Cloud

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

☐ Bitte buchen Sie mir ein Hotelzimmer

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

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

Neue Sonderveranstaltung

Sonderveranstaltung: Office 365 in der Praxis

20.03.2018 in Bonn

Die ComConsult Akademie veranstaltet am 20.03.18 ihre neue Sonderveranstaltung "Office 365 in der Praxis" in Bonn.

Software as a Service hat sich zum führenden Servicemodell aus der Public Cloud entwickelt und bei gut der Hälfte der deutschen Unternehmen, die Anwendungen aus der Cloud nutzen, handelt es sich hierbei um Office-Anwendungen aus der Cloud, bei jeweils über einem Drittel um Groupware oder Kollaborationsanwendungen.

Office 365 ist in diesen Bereichen zweifellos der Marktführer. Gleichzeitig wird Office 365 gerade in der Einführungsphase maßlos unterschätzt. Viele Unternehmen versuchen mit Office 365 ihre langjährige Microsoft-Office-Tradition möglichst ohne große Brüche fortzuführen und ignorieren die Auswirkungen, die die Einführung von Cloud-Anwendungen im Allgemeinen und von Office 365 im Besonderen hat.

Wir sprechen mit Ihnen über:

- Anforderungen und Konsequenzen für die IT
  - Grundlagen und Lizenzmodelle
  - Anbindung und Zugang an die bzw. zur Microsoft Cloud
  - Integration des Active Directory
  - Single Sign-On
- Konsequenzen für Geschäftsprozesse und Unternehmensabläufe:
  - Wo unterscheiden sich Cloud-Anwendungen von klassischen Anwendungen?
  - Die Bedeutung von "User Experience"
- Anforderungen an die Netzinfrastruktur
  - WAN-Anbindung
  - Tools zur Überprüfung der Netzqualität
  - Netzdesigns zur Anbindung von Niederlassungen
  - Tuning Möglichkeiten
- Erfahrungen aus Kundenprojekten

Die Veranstaltung richtet sich an alle Personen, die die Einführung von Office 365 oder wesentlicher Funktionsbereiche wie Datenhaltung, Kollaboration oder Telefonie über Skype for Business in ihrem Unternehmen diskutieren oder bereits strategisch planen und vorbereiten.

Durch die Veranstaltung führt Sie Dipl.-Math. Cornelius Höchel-Winter. Er ist Leiter des Technologie-Labors und des Bereichs Systemintegration bei der ComConsult Research GmbH. In dem Labor werden regelmäßig Messungen und Evaluierungen neuester Hard- und Softwareprodukte durchgeführt und ausgewertet. Herr Höchel-Winter besitzt langjährige Erfahrung in der Konzeptionierung, im Aufbau und Betrieb von RZ- und Campusnetzen und von Windows- und Linux-Umgebungen. So hat er als verantwortlicher Projektmanager die Rechenzentren und Netzwerke auf dem Gelände der EXPO2000 in Hannover aufgebaut und während der Weltausstellung betrieben. Für die ComConsult Akademie ist er außerdem seit 2001 als Autor, Trainer und Referent auf Seminaren und Kongressen schwerpunktmäßig in den Bereichen Data Center, Virtualisierung, Storage, Netzwerke und Cloud Computing tätig.

Sparen Sie 390,- € bei der Buchung beider Sonderveranstaltungen
Herausforderung Cloud am 19.03.18:
Preis 1.090,-- €
Office 365 in der Praxis am 20.03.18:
Preis 1.090,-- €
Beide Sonderveranstaltungen:
Preis 1.790,-- €
Bei Buchung der beiden einzelnen Sonderveranstaltungen wird Ihnen der Rabatt automatisch abgezogen

Anmeldung an kundenservice@comconsult-research.de

Sonderveranstaltung: Office 365 in der Praxis

Ich buche die Sonderveranstaltung
Office 365 in der Praxis

☐ 20.03.2018 in Bonn
zum Preis von 1.090,- € netto

☐ Bitte buchen Sie mir ein Hotelzimmer

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

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

Neue Sonderveranstaltung

Kriterien und Erfolgs-Szenarien für den Einsatz von UCC-Produkten

Cisco Spark, Microsoft Teams und Unify Circuit in der Analyse

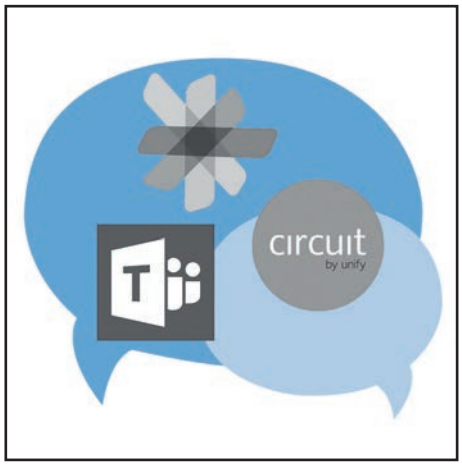
21.03.2018 in Bonn

Die ComConsult Akademie veranstaltet am 21.03.18 ihre neue Sonderveranstaltung "Kriterien und Erfolgs-Szenarien für den Einsatz von UCC-Produkten: Cisco Spark, Microsoft Teams und Unify Circuit in der Analyse" in Bonn.

Die Positionierung von Unified Communications und Collaboration UCC hat sich in den letzten Monaten gewandelt. Bis dahin war es eher ein Spezial-Produkt für kleinere Teams. Der erste Wechsel kam mit dem Einstieg von Microsoft in den Markt und der Entwicklung von Microsoft Teams als Teil von Office 365. Und der große Knall kam im Oktober mit der Ankündigung von Microsoft, dass Teams den bisherigen UC-Client in Skype for Business ablösen wird. Parallel bauen Cisco und Unify ihre Produkte immer weiter aus und auch die anderen traditionellen TK-Anbieter wie Alcatel und Avaya steigen in diesen Markt ein.

Bei der Bewertung von UCC für den praktischen Einsatz müssen die verschiedenen Funktionsbereiche von UCC sauber abgegrenzt und im Projekt positioniert werden:

- Team-Bildung und Schaffung von Themen-bezogenen Kommunikations-Kanälen
- Sprach- und Video-Meetings auf Team-Niveau



- Dokumenten-Kollaboration
- Persistent Chat

Damit muss auch aus der Sicht des Planers eine Neupositionierung von UCC erfolgen. Jedes UC-Projekt muss sich damit den folgenden Fragen stellen:

- Ist UCC funktional die Zukunft in der Zeit nach ISDN?
- Welche Rolle werden Persistent-Chat und Dokumenten-Kollaboration in Zukunft haben?
- Wie offen muss eine UCC-Lösung sein?
- Wann sind solche Projekte erfolgreich und woran können sie scheitern?

Mit der Ablösung von ISDN wird die Dominanz Sprache und Email enden. Dieser Trend existiert seit einigen Jahren und wir nähern uns der kritischen Masse. Die Frage ist entsprechend, was danach kommt. Und mit UCC werfen die Hersteller einen funktionalen Hut in den Ring, der in der Tat die wichtigsten technologischen Entwicklungen der letzten Jahre integriert.

Hier setzt diese Sonderveranstaltung an:

- Wir stellen unsere Bewertungs-Kriterien für den Einsatz von UCC-Produkten vor
- Wir sagen, warum Projekte erfolgreich sind und woran sie scheitern können
- Wir gehen in Form von Beispielen auf die bestehenden Produkte ein und zeigen, wo sie stehen
- Wir setzen UCC in den Zusammenhang mit der Zukunft von UC

Vereinfacht gesagt zeigen wir, wie man mit UCC einen stufenweisen Einstieg in das UC der Zukunft aufbauen kann. Und wir werden dabei auch zeigen, dass dies nicht automatisch die Zukunft des heute bei Ihnen im Einsatz befindlichen Produktes sein muss. Mit UCC und der Zukunft von UC werden die Karten neu gemischt. Es entsteht ein neuer Markt und die Frage, wie gut ein Hersteller oder Produkt bisher war, spielt dabei keine Rolle.

Anmeldung an kundenservice@comconsult-research.de

Kriterien und Erfolgs-Szenarien für den Einsatz von UCC-Produkten

Ich buche die Sonderveranstaltung
Kriterien und Erfolgs-Szenarien für den Einsatz von UCC-Produkten

☐ 21.03.2018 in Bonn
zum Preis von 1.090,- € netto

☐ Bitte buchen Sie mir ein Hotelzimmer

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

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

Aktueller Kongress

ComConsult Netzwerk Forum 2018

16.04. - 19.04.2018 in Königswinter

Frühbucherphase bis zum 31.12.17

Die ComConsult Akademie veranstaltet vom 16.04. bis zum 19.04.2018 ihren Kongress "ComConsult Netzwerk Forum" in Königswinter.

Wir sehen folgende Mega-Trends, die unsere IT-Architekturen und Infrastrukturen in den nächsten Jahren bestimmen werden:

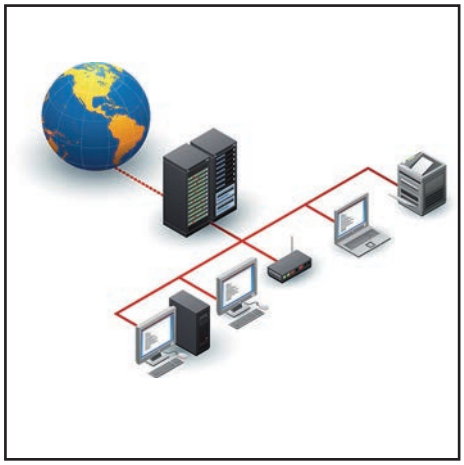
- Ein neues Verständnis vom Endgerät mit veränderten Anforderungen, vor allem bezogen auf die Frage, welche und wie viele Endgeräte wir wo im Netzwerk haben und was wir an Dienstqualität dafür zu leisten haben
- Der Umbau der IT-Architekturen zu Cloud-basierten Architekturen, sei es eine Private oder eine Public Cloud. Dies umfasst auch die Veränderungen auf der Seite genutzter Applikationen mit einem klaren Trend zu Software as a Service
- Eine zunehmende Integration aus Cloud und Data Center mit dem Data Center im Kern und der Cloud als Ergänzung
- Der Entwicklung des Netzwerks zum zentralen und wichtigsten Verteidigungs-Instrument gegen Angriffe

Typische Projektbeispiele, in denen diese Trends zum tragen kommen, sind:

- Smart-Building: IT-Infrastrukturen für das Gebäude der Zukunft - vom Sensor bis zum Mainframe, von der Beleuchtung bis zum High Performance-Computing.
- Team-Kollaboration über Unternehmensgrenzen hinaus im Rahmen einer UC-Zukunft in der Cloud.
- Internet-Zugang: mehr Sicherheit, mehr Bandbreite, geringe Latenz, dezentral
- Verkürzung von Projektlaufzeiten in der IT: von Jahren zu Wochen
- Sicherheits-Infrastrukturen im Campus-Netzwerk: Erkennung und Isolierung des Angreifers

Unsere traditionellen Netzwerke kommen dabei in mehreren Bereichen an ihre Grenzen:

- Sensorik, mobile Endgeräte, High Performance Workstations: wir brauchen



ein Gesamtkonzept, das Wireless und Wired über alle Formen von Kommunikation abdeckt.
- Zugang zu Software as a Service, Kombination von Cloud-Anwendungen mit dem lokalen Data Center: Kommunikation macht nicht mehr an der Unternehmensgrenze halt, wir müssen unser Verständnis weiter fassen und die Kontrolle für das Gesamtgebilde übernehmen.
- Netzwerke sind Verbindungs- aber nicht dienstorientiert. Traditionell sind sie dienstneutral und auf Bandbreite optimiert. Schnelle Bereitstellung geht so nicht.
- Data Center, Campus, WAN und Access haben sich in verschiedene Richtungen entwickelt. Wir müssen die Frage stellen, wo wir welche Protokolle übergreifend sinnvoll zum Einsatz bringen können.
- Die Verzettelung in verschiedene Anforderungen und Protokolle im Data Center, im Campus, im Access und im WAN führt zu mehr Betriebs-Komplexität. Es muss immer mehr konfiguriert werden. Mehr Komplexität bedeutet ein höheres Risiko von Fehlern und höhere Betriebskosten.

Daraus leiten wir folgende Trends auf der Netzwerkseite ab, auf die Netzwerk-Planer und Betreiber reagieren sollten:

- Netzwerk-Infrastrukturen für den Arbeitsplatz und das Gebäude der Zukunft
- Konsistentes Netzwerk Design: wie kommen WAN, Campus, Data Center, Access in einer integrierten Architektur mit durchgehenden Verfahren zusammen?
- Optimierter Netzwerk-Betrieb, das Ende des Command Line Interfaces: gezielter Einsatz von Automatisierung, Analytics und Machine Learning. Ist die Zukunft besser, verfügbarer, weniger komplex, wirtschaftlicher? Welche Auswirkungen hat das auf den Betreiber, was muss der können oder lernen?
- Wireless Unlimited: Bluetooth, IEEE 802.11ax + 5G, Harmonisierung und Neuausrichtung einer neuen Generation von Wireless Netzwerken. Mehr Leistung, mehr Varianten aber auch mehr Überlappung und mehr Störungen: wie kommen wir zu einer schlüssigen Gesamt-Lösung?
- Sicherheit im Campus: wie sicher sind unsere Netzwerke wirklich? Wie können wir eine korrekte und unbeeinflusste Konfiguration sicherstellen? Wie können wir den Erfolg eines Angreifers eingrenzen?

Dies sind die Themen, denen sich das ComConsult Netzwerk-Forum 2018 stellt!

Am ersten Tag startet die Keynote von Dr. Jürgen Suppan mit der Analyse des Infrastruktur-Bedarfs des Arbeitsplatzes der Zukunft. Wir vertiefen dies mit der Diskussion der aktuellsten Entwicklungen im Bereich der IT-Architekturen.

Dabei analysieren und diskutieren wir u.a. folgende Fragen:

- Wie schätzen wir den Trend zur Cloud ein und was bedeutet die zunehmende Nutzung von Cloud-Diensten für das Design des Netzwerks?
- Wie wichtig wird die Virtualisierung des Netzwerks? Brauchen wir wirklich Overlays?
- Wie können extrem unterschiedliche Anforderungen von sehr einfachen hochgradig standardisierten bis hin zu sehr speziell ausgelegten High Performance Arbeitsplätzen in einem kohärenten Design verheiratet werden? Wird 10 Gigabit am Arbeitsplatz ein Thema? Wie passt das wirtschaftlich zusammen mit einem Cloud-Arbeitsplatz?
- Schnelle Bereitstellung bei gleichzeitig

ComConsult Netzwerk Forum 2018

dynamisch schwankenden Kapazitäts-Anforderungen: wie geht das?

Daraus leiten wir in eine vertiefte Analyse der aktuellsten Trends im Netzwerk-Design über. Hier stellt sich vor allem die Frage, wie wir die verschiedenen Trends der letzten Jahren vom WAN bis zum Access in ein schlüssiges Gesamtkonzept mit möglichst wenigen, aber einheitlichen Technologien überführen können.

Wir analysieren für Sie:

- Data Center Verfahren dominieren den High-End-Bereich: wie relevant ist das für den Campus? Welche Elemente aus dem RZ.-Design verbessern das Campus-Design und bringen einen signifikanten Mehrwert?
- Wie bringen wir WAN, Campus, Data Center und Access zusammen?
- Internet-Zugang im Wandel: wie werden wir den immer kritischeren Anforderungen an einen Internet-Zugang gerecht? Was sind die führenden Planungs-Parameter?
- Netzwerk-Design in der Cloud: was müssen wir leisten? Wie kombinieren wir Cloud und lokales Data Center zu einer Einheit?

Netzwerke waren und sind der Lebensnerv unserer IT. Niemals war das so klar wie heute. Dabei verschwimmen die Grenzen zur Cloud, die eingesetzten Verfahren werden weiterhin komplexer und die Risiken im Bereich von Sicherheit nehmen zu. Haben wir hier die Grenze eines normalen Betriebs erreicht? Brauchen wir einen frischen Ansatz, um den Anforderungen noch gerecht zu werden?

Wir analysieren für Sie und diskutieren mit Ihnen:

- Ist das Command-Line-Interface tot? Erfordern die modernen Netzwerk-Architekturen einen frischen Konfigurations-Ansatz, der effizienter und weniger fehleranfällig ist?
- Analytics und Automatisierung: ist das die Zukunft?
- Das Berufsbild des Netzwerk-Betreibers: was muss der Betreiber in Zukunft können? Wie erfolgt der Übergang zu einer neuen Form von Betrieb?

2018 und 2019 werden Wireless-Jahre sein. Die Zahl der Endpunkte mit Wireless-Technik wird explodieren. Gleichzeitig kommen neue Technologien in den Markt, die mehr können, aber auch komplexer sind. In 2018 wird das Thema WLAN durch den neuen Standard 802.11ax bestimmt werden. Und zum ersten Mal ist dies wirklich ein neuer Standard, der das Nutzungsspektrum von WLANs in eine völlig neue Dimension bringen wird. Vom garantierten Zugang für einen Sensor mit zu einer Vervielfachung der spektralen Nutzung werden die unterschiedlichsten Szenarien durch eine neue Art der Steuerung möglich gemacht.

Wir analysieren und diskutieren die folgenden Fragen:

- IEEE 802.11ax - der Wunder-Standard: die erste wirklich professionelle WLAN-Technologie? Was wird möglich, was bisher nicht möglich war? Wo liegen Risiken?
- Immer mehr und immer neuere Technologien in einem Gebäude oder Gelände. Und alle benutzen die gleichen Frequenzen. Wird das Eis, auf dem wir wandern, immer dünner? Wie gehen wir damit um, wie vermeiden wir den Mega-GAU?
- 5G: die erste Modem-Welle steht vor der Tür. Die nächste oder übernächste Welle von Mobilgeräten wird die 5G-Fähigkeit haben. Die ersten kommerziell interessanten Netzwerke werden 2019 kommen, die große Welle kommt 2020. Was bringt diese Technik eigentlich, wie verträgt sie sich mit WLAN und wie kommen wir zu einem schlüssigen Gesamtkonzept?

Ein Angriff auf unsere Netzwerke ist der größte anzunehmende Unfall für unsere IT. Mit einem Schlag geht nichts mehr. Überlegen Sie, was das für Ihr Unternehmen bedeuten würde: das Netzwerk ist unter der Kontrolle von Hackern. Endlich lernen Sie den Vorstand persönlich kennen. Gleichzeitig ist das Netzwerk der einzige IT-Bereich, in dem wir Angreifer komplett blockieren und eingrenzen können. Wie real ist dieses Risiko und was können wir im Bereich des wirtschaftlich vertretbaren tun?

Wir analysieren und diskutieren mit Ihnen:

- Wie kommt der Angreifer rein? Müssen wir bei mobilen Endgeräten einen Zahn zulegen?
- Wie kann das Netzwerk Angreifer erkennen und isolieren?
- Das Campus-Netzwerk ist unser Kern. Von hier aus kommt der Angreifer überall hin. Damit ist es unsere Haupt-Verteidigungslinie. Wie gehe ich vor, wie sichere ich den Campus ab? Wie bereite ich mich auf den Tag x vor? Kann ich sicherstellen, dass der Angreifer nicht die gesamte Infrastruktur übernimmt?
- Wie kann ein Audit aussehen, das mehr wert ist als das Papier, auf dem es beschrieben wird?

Wie in jedem Jahr so wird auch 2018 das ComConsult Netzwerk Forum der Treffpunkt der Branche sein. Top-Referenten, die Analyse der neuesten Entwicklungen, praxisnahe Empfehlungen, mehr Sicherheit für Ihre Entscheidungen und viele, viele Diskussionen prägen diese Veranstaltung. Versäumen Sie nicht sich rechtzeitig einen Platz zu sichern.

Anmeldung an kundenservice@comconsult-research.de

ComConsult Netzwerk Forum 2018

Ich buche den Kongress
ComConsult Netzwerk Forum 2018

☐ 16.04. - 19.04.2018 in Königswinter
zum Preis von 2.590,-- € netto*

*gültig bis zum 31.12.2017 -
danach regulärer Preis 2.790,-- € 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

IEEE 802.11ax: die neue WLAN Generation

Fortsetzung von Seite 1

Dr. Franz-Joachim Kauffels ist Technologie- und Industrie-Analyst und Autor. Seit über 30 Jahren unabhängiger, kritischer und oft unbequemer Bestandteil der Netzwerkszene. Verfasser von über 20 Büchern in über 70 Ausgaben sowie über 2000 Artikeln, Videos und Reports.

Vielmehr geht es darum, die Fairness zwischen den Teilnehmern zu verbessern und ihnen auch unter eigentlich ungünstigen Bedingungen jederzeit eine hinreichende Datenrate zu liefern. Kern des neuen Standards ist zumindest in einem der drei möglichen Arbeitsmodi ein anderes Steuerungsverfahren für den Zugriff auf das gemeinsam genutzte Übertragungsmedium. Es basiert zum ersten Mal in der WLAN-Geschichte auf einer weitest gehend zentralen Steuerung. Natürlich wurde bei dieser Gelegenheit auch die gesamte Übertragungstechnik auf den neuesten Stand gebracht und dadurch die mögliche aggregate Gesamtleistung am Ende doch erhöht. Kern ist aber die Eignung des Systems für neue Anwendungsbereiche, bei denen die Versorgung sehr vieler Nutzer auf einem engen Bereich im Vordergrund steht. (siehe Abbildung 1)

Nach Quantenna, die ja schon 2016 mit einem Muster vorpreschten, hat der bekannte Chip-Hersteller Qualcomm (Nasdaq: QCOM) schon Mitte Februar 2017 die ersten 11ax-Chips, jeweils einen für Access Points oder Router und einen für Smartphones vorgestellt. Der bei WLANs ebenfalls sehr erfolgreiche Hersteller Broadcom (Nasdaq: AVGO) hat Mitte August 2017 mir einer Reihe von Chips für die erste Generation von Geräten nach dem neuen Standard nachgezogen. Dabei handelt es sich jeweils um einen Chip für Access Points in Haushalte und professionellen Anwendungsumgebungen und einen Combo-Chip für Smartphones. Das reicht eigentlich schon für den Start, denn QCOM und AVGO dominieren zusammen den Markt.

Von den einschlägigen Herstellern von professionellen Lösungen für Unternehmen und Organisationen hat Extreme Networks bereits für Mitte 2018 Produkte angekündigt. Das zeigt deutlich, dass die Hersteller die Zeit zwischen dem Eintreffen einer neuen Chip-Generation bis zu fertigen Produkten von früher 2 Jahren deutlich verkürzen können.

Abbildung 1: Umgebung mit dichter Population Quelle: Oishi Restaurant Aaachen

Über die nächsten 5 Jahre werden nach Angaben von Marktforschern 20 Mrd. Wi-Fi-Chips verkauft, 2021 wird 11ax daran einen Anteil von 57 Prozent haben. Auf Endgeräte brauchen wir nicht mehr zu warten: das neue Samsung Galaxy S8 beherrscht das neue WLAN mit dem QCA 6290 Chip von Samsung, die neuen iPhones bleiben zumindest in Europa mit 11ac-Support unterhalb der Funktionalität von Samsung. Den ersten Access Point von Quantenna gibt es ja schon seit über einem Jahr, die anderen üblichen Verdächtigen für den Heimmarkt liefern, wenn sie der Ansicht sind, dass es sich lohnt.

In diesem Artikel sehen wir uns zunächst diese Anwendungsbereiche genauer an, nehmen dann die Probleme mit den bisherigen Verfahren unter die Lupe, und kommen dann zu den Änderungen in MAC und PHY, die die gewünschten Verbesserungen realisieren sollen. Schließlich werfen wir einen Blick auf mögliche Probleme und die Bedeutung des neuen WLAN-Standards für die flächendeckende Versorgung in modernen Gebäuden bei Unternehmen und Organisationen.

1. Ein neues System für neue, anspruchsvolle Anwendungsbereiche

Einen ersten Hinweis auf die Andersartigkeit von 11ax gibt der ursprüngliche Name der Arbeitsgruppe, die den Standard angestoßen hat: High Efficiency Wireless, kurz: HEW. Und ein Blick in die Realität.

Der Autor gibt zu, sich im Zuge seiner mittlerweile schon weit über 20 Jahre zurückliegenden Midlife Crisis einen gebrauchten Sportwagen gekauft zu haben. Damals war es durchaus möglich, mit etwas Glück ein Stück Autobahn oder eine leere gewundene Landstraße zu fin-

den, an dem man das Auto wirklich nutzen konnte. Das gibt es heute kaum mehr und wenn man sich heute durch den dichten Innenstadtverkehr schleppen oder an einer „Stau“ genannten unpolitischen Versammlung auf der Autobahn teilnehmen muss, werden die 300 PS zahnlos und man fragt sich, ob nicht ein kleineres billigeres Auto mit bequemeren Sitzen für die Situation besser wäre. Porsche hat das Auto natürlich weiterentwickelt, es hat jetzt rund 500 PS, die aber in der Praxis kaum nützlicher sind. Also ist der Carrera mit den Jahren breiter geworden und wurde mit diesem ganzen elektronischen Kleinkram vollgestopft, den heute auch jeder Kleinwagen hat. Vielleicht soll das den Fahrer nur von seiner eigentlich unglücklichen Situation ablenken.

Was hat das alles mit WLANs zu tun? Nun, aus der Perspektive eines Benutzers ist doch eigentlich nur interessant, wie schnell seine Daten laufen können. Und so sind auch alle bisherigen Entwicklungen zu werten. Mit 802.11n von 2009 konnte man zum ersten Mal mit einem Single Stream mehr als 100 Mbps erreichen. Durch MIMO-Antennentechnik kann man bis zu vier Single Streams bündeln und rein theoretisch fast 600 Mbps aggregate Gesamtleistung in der WLAN-Zelle erzielen. 802.11ac von 2013 kam dann durch dichtere Modulation (256-QAM) und die Nutzung breiterer Kanäle (max. 160 MHz) theoretisch auf 866 Mbps auf einem einzelnen Stream. MIMO wurde auf maximal 8 Kanäle erweitert und im Vollausbau könnte man in einer idealen Welt der Wunder eine aggregate Gesamtleistung von 6,97 Gbps in einer Zelle erreichen.

In der realen Welt wurden diese theoretischen Gesamtleistungen nie erreicht. Das lag weniger an der Übertragungstechnik, die funktioniert ja durchaus wie gewünscht, sondern an einer Mischung aus Tücken der Realität und geerbter Beulen-Pest. Die Tücken der Realität sind vielfältig und liegen vor allem in der Natur des Übertragungsmediums Luft. Die Dämpfung ist nicht nur hoch, sondern auch launisch und man kann sie eigentlich immer nur näherungsweise betrachten. Viel schlimmer ist aber der Wettbewerb unter den Stationen um das gemeinsam wechselseitig ausgeschlossen zu nutzende Übertragungsmedium. Gefühlt seit Abraham verwenden WLANs das Steuerungsverfahren DCF, Distributed Controlling Funktion, wie der Name schon sagt, ein Verfahren, welches den Verkehr in der WLAN-Zelle regelt ohne eine zentrale Station zu benötigen. Das Verfahren ist eine Version von CSMA/CD, dem Steuerungsverfahren für Ethernet vor über 30 Jahren, für Funknetze. DCF schwächelt, wenn es zu viele Stationen gibt (mehr als eine Hand voll), die durchschnittliche Paketlänge zu lang ist, die mittlere Paket-Ankunftsrate ungünstig ist und noch aus vielen anderen Gründen. Die statistische Hauptanwendung von WLANs ist aber heute die DSL-Verlängerung für Triple Play in Haushalten, und dafür ist es prima, wenn es nicht zu viele Kinder oder Haustiere mit eigenen Endgeräten gibt. Deshalb wurde es seit dem ersten WLAN nach IEEE 802.11b von System zu System mitgenommen.

In einer anspruchsvollen Umgebung offenbaren sich die Schwächen von DCF aber deutlicher. Vor allem gibt es bei DCF-WLANs keinerlei verläßlichen Durchsatz, weil es nicht deterministisch ist.

In Unternehmen und Organisationen begegnet man solchen Problemen gerne und erfolgreich durch sehr sorgfältige Planung und spezielle Controller-Architekturen.

Neuerdings gibt es aber Anforderungen und Umgebungen, für die und in denen das alles nicht mehr reicht. Das sind Umgebungen mit hoher Teilnehmerdichte, wie z.B.

- Stadien
- Flughafenterminals, Bahnhöfe oder Gaststätten mit public WiFi
- Öffentliche Bereiche wie Innenstädte mit flächendeckendem free WiFi
- WiFi in Small Cells im Rahmen von Mobilfunk-Infrastrukturen in LTE Advanced/5G-Versorgungsbereichen

Hier haben wir nämlich das gleiche Problem wie auf der Autobahn oder in der Rush Hour: zu viele Teilnehmer auf relativ geringem Raum. In diesen Umgebungen versagt DCF vollends, aber wir wollen zur Ehrenrettung sagen, dass es auch nicht dafür gemacht wurde. (siehe Abbildung 2)

802.11ax hat schlicht und ergreifend das konstruktive Ziel, den mittleren Durchsatz pro Benutzer in dichten Umgebungen zu erhöhen, und zwar um den Faktor 4.

Es geht also nicht mehr um die weitere Steigerung der aggregaten Zellen-Leistung in einer WLAN-Zelle, sondern um eine Verbesserung des individuellen Benutzer-Erlebnisses in dichten Umgebungen, kurz gesagt um mehr Fairness.

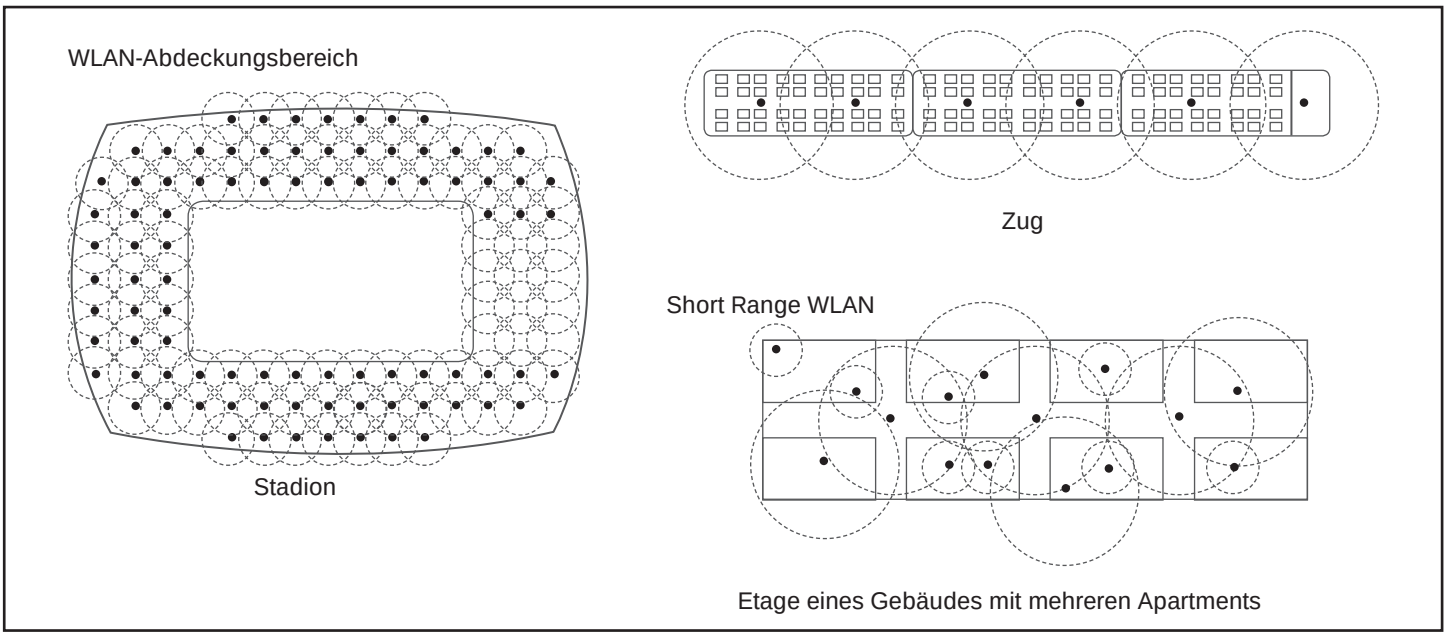


Abbildung 2: Hochdichte WLAN-Szenarien Grafik: Bellalta

Natürlich werden in diesem Zusammenhang die technischen Parameter der Übertragungssysteme auf den allerneuesten Stand gebracht, die wirkliche Neuheit ist aber ein fairer Zugriffsmechanismus. 802.11ax hat sich dabei für OFDMA entschieden, das ist das Verfahren, mit dem LTE-Basisstationen den Verkehr der bei ihnen gemeldeten Nutzer steuert. OFDMA benötigt technisch eine kleine Zentrale.

In der vielfältigen Literatur zu IEEE 802.11ax wird gerne übersehen, dass es noch einen anderen wichtigen Punkt gibt, nämlich die Möglichkeit, eine Kommunikations-Bandbreite für einen Nutzer auch zu garantieren und diese Garantie durchzusetzen. Das braucht man, wenn man LTE Advanced oder 5G-Netze ernsthaft mit vielen Small Cells betreiben möchte, wie ich das ja schon mehrfach in anderen Artikeln dargestellt habe. Jeder Benutzer hat einen Contract mit einem Provider, für den er auch bezahlt. In diesem Contract wird u.a. eine minimale Bandbreite für seine Verbindung und eine Grundqualität festgelegt. In dichteren Umgebungen kooperieren die Mobilfunk-Zellen mittels LTE-U oder LAA mit WLANs, um die Gesamt-Bandbreite zu erhöhen. Dazu gibt es meist eine schmalbandige Mobilfunk-Verbindung zwischen Nutzer und Basis-Station auf einer lizensierten Frequenz, die die Kommunikation steuert und eine zweite Verbindung zwischen Nutzer und WLAN, über die die eigentlichen Daten geschickt werden. Hört sich kompliziert an, ist es auch, funktioniert aber gut. Wermutstropfen heute: mit WLANs bis 11ac gibt es keine Garantien für die Leistung, die einen individuellen Benutzer erreicht. Das widerspricht dem Contract und muss technisch abgestellt werden. Dazu benötigt man ein deutlich verbessertes Steuerungsverfahren für die WLAN-Zellen.

Wir fassen zusammen:

Es gibt vier Schwerpunkte bei Anwendungsbereichen für das neue 11ax WLAN:

- Offloading Zellularer Daten: Prognosen von Cisco gehen davon aus, dass 2020 jeden Monat 38,1 Exabytes Wi-Fi Offload Traffic erzeugt werden. Dies setzt die Tendenz fort, dass das Offloading den gesamten mobilen/zellularen Mobilfunkverkehr (im klassischen Sinne) übersteigt, der in 2020 für 30,6 Exabytes sorgen soll. Das ist äquivalent dazu, mehr als 6000 Blu Ray Filme pro Minute auf diesen Netzen zu bewegen.

- Versorgung von Umgebungen mit vielen Access Points und einer hohen Konzentration von Nutzern mit heterogenen Geräten. Airport WiFi ist eben etwas anderes als Heim-WiFi.

- Verbesserung der Indoor-Versorgung in Apartment-Häusern mit einer hohen dreidimensionalen Dichte von Bewohnern.

- Gemischte Outdoor Umgebungen. Hier sind vor allem Dinge wie U-Bahn Wagen spannend, in denen jeder Fahrgast seine persönliche Unterhaltung oder Information aus dem Internet ziehen können soll, auch wenn der Waggon grenzwertig gefüllt ist.

Das neue 11ax WLAN hat folgende Schlüssel-Eigenschaften, die wir in den weiteren Abschnitten noch genauer unter die Lupe nehmen werden:

- Rückwärtskompatibilität mit 802.11 a, b, g, n, ac

- Steigerung des durchschnittlichen Durchsatzes pro Benutzer in hochdichten Umgebungen (Bahnhöfe, Flugplätze, Stadien) um den Faktor vier

- Datenraten und Kanalbreiten ähnlich zu IEEE 802.11ac mit der Ausnahme der Einführung neuer Sets für Modulation und Codierung mit 1024 QAM

- Spezifiziert für Multi-User Betrieb mit Uplink und Downlink mit MU-MIMO und OFDMA (Orthogonal Frequency Division Multiple Access). Dies bedingt die Einführung einer zentralen Steuerung mit erheblich mehr Einfluss und Funktionen als bei einem traditionellen Access Point.

- Breitere FFT-Größen in OFDM (4X), schmalere Abstände zwischen den Unterträgern (4 X enger) und längere Symbolzeit (4X) für erhöhte Robustheit und Leistung in Umgebungen mit Multipath Fading und Outdoor.

- Verbesserter Verkehrsfluss und Kanalzugriff

2. Probleme mit dem WiFi-Durchsatz in dichten Umgebungen

Das 802.11 Protokoll nutzt mit DCF eine Carrier Sense Multiple Access (CSMA)-

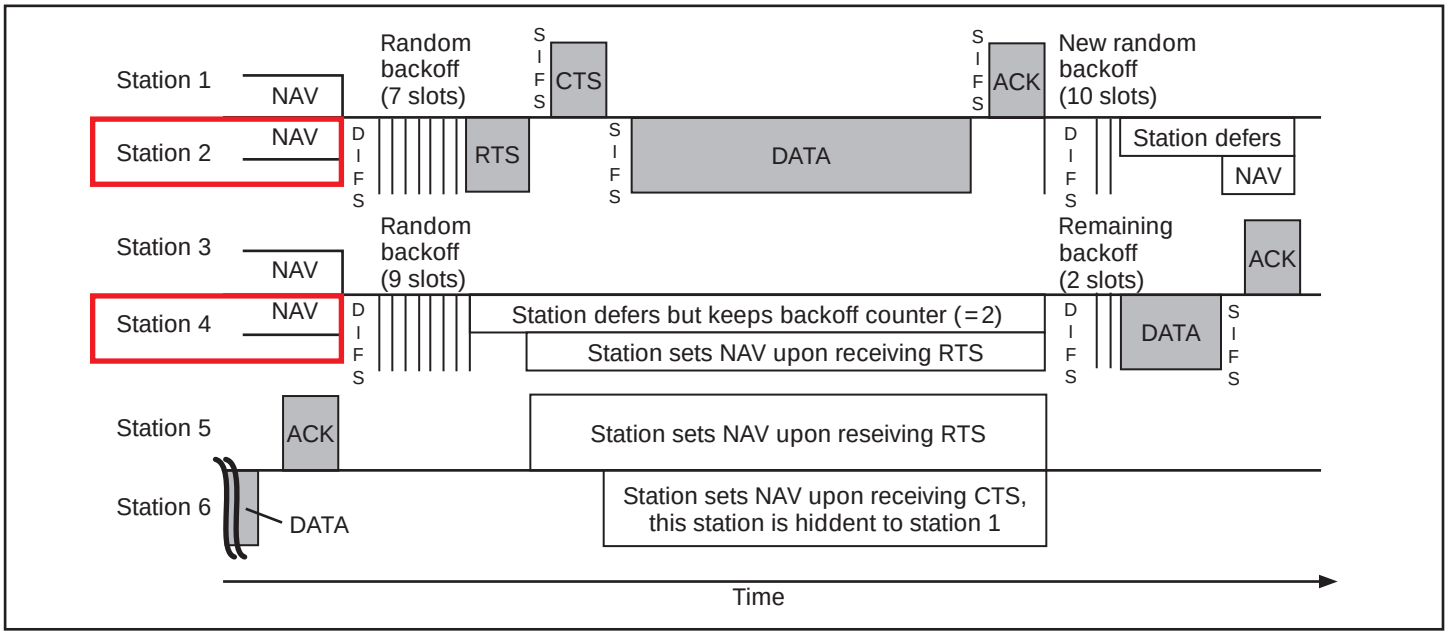


Abbildung 3: Clear Channel Assessment Protocol

Quelle: IEEE

Steuerungstechnik, bei der die Stationen zunächst in den Kanal hineingehören und versuchen, Kollisionen zu vermeiden, indem sie nur dann senden, wenn sie den Kanal für freihalten. Das ist dann der Fall, wenn sie keine andern 802.11 Signale erkennen. Hört eine Station ein Signal von einer anderen, wartet sie eine aus einem Intervall zufällig gewählte Verzögerungszeit ab, in der Hoffnung, dass die andere Station in diesem Intervall ihre Sendung beenden kann. Dann horcht sie wieder auf den Kanal. Hat sie wieder keinen Erfolg, muss sie wieder eine Verzögerungszeit abwarten, die dieses Mal aber aus einem doppelt so langen Intervall gewürfelt wird (Binary Exponential Backoff BEB). Wenn frei ist, senden Stationen ihre gesamten Pakete. WiFi Stationen können Request to Send / Clear to Send (RTS/CTS) dazu nutzen, den Zugriff zum gemeinsam benutzten Medium zu steuern. Dabei sendet der Access Point zu einer Zeit nur ein CTS Paket zu einer Station, die daraufhin im Gegenzug ihren ganzen Frame an den AP schickt. Die Station wartet dann auf ein Acknowledgement Paket (ACK) vom AP, welches anzeigt, ob das Paket korrekt empfangen wurde. Wenn die Station das ACK nicht innerhalb einer gewissen Zeit bekommt, muss sie davon ausgehen, dass ihr Paket mit einer anderen Sendung kollidiert ist, und fällt wieder in den BEB-Modus. Sie startet erst dann wieder einen Versuch, wenn die Backoff-Zeit abgelaufen ist. (siehe Abbildung 3)

Zusammenfassend wird diese Arbeitsweise auch als Clear Channel Assessment Protocol bezeichnet. Dieses Verfahren und die Kollisionsvermeidung sorgen seit Jahrzehnten für eine halbwegs faire Aufteilung des Kommunikationsmediums unter allen Teilnehmern innerhalb der Kollisions-Domäne, seine Effizienz nimmt aber mit der Anzahl der Stationen deutlich ab.

Es gibt aber noch einen anderen Faktor, der sich negativ auf die Effizienz der Netzwerk-Effizienz auswirkt, und zwar dann, wenn man viele APs mit überlappenden Versorgungsbereichen hat. Die Abbildung 4 zeigt einen Nutzer (User 1), der zum linken Basic Service Set BSS (der Menge von Wireless Clients, die mit einem AP assoziiert sind) gehört. Normalerweise steht User 1 im Wettbewerb mit allen anderen Nutzern in seinem eigenen BSS um seinem AP Daten schicken zu können. Dieser Nutzer ist aber leider auch in der Lage, Verkehr vom überlappenden rechten BSS zu hören. Und genau dieser Verkehr triggert dann die Backoff Prozedur von User 1. Das Resultat solcher Situationen ist, dass alle Nutzer länger darauf warten müssen, senden zu können und somit der durchschnittliche Datendurchsatz sinkt.

Nun wird es eine große Anzahl von Lesern geben, die entgegenhalten, dass genau das bei einer ordentlichen Planung von Reichweite und Kanälen mit unterschiedlichen Frequenzen bei einer flächendeckenden Versorgung nicht auftreten kann. Recht haben sie, aber eben nur unter der Voraussetzung, dass der gesamte zu versorgende Bereich in einer planerischen und betrieblichen Hand ist.

Und es gibt heute schon einen sehr lästigen Fall, in dem genau dieses Problem sehr heftig zuschlägt, nämlich die WLAN-Versorgung von Wohnungen in Mehrfamilienhäusern. Ich habe das immer wieder mal in Vorträgen und Artikeln angesprochen und bis heute gibt es keine wirklich verbreitete Lösung. Der WLAN-DSL-Router wird irgendwo in einer Wohnung aufgestellt und versorgt sie dann ganz ordentlich, wenn sie nicht zu groß ist. Sollte die Leistung für eine Wohnung nicht ausreichen, gibt es „WLAN-Verlängerungen“, die mehrere Access Points meist mit Power Line Verbindungen über das Stromnetz synchronisieren können. In der Zukunft könnten hier auch Mesh-Systeme eine Rolle spielen, momentan statistisch eher nicht. Das macht jetzt jeder in seiner Wohnung und dann haben wir den interessanten Fall, dass z.B. bei der WLAN-Konfiguration eines neuen Endgerätes nicht nur das eigene, sondern auch noch mehr als ein ganzes Dutzend fremder WLANs auf dem Bildschirm erschient. Die kann man zwar normalerweise nicht nutzen, weil sie mittlerweile doch meist verschlüsselt sind, das ändert aber rein gar nichts an der Tatsache, dass sich die Kollisions-Domänen dieser Netze massiv überschneiden können. Eine geeignete Vorgehensweise wäre nun die Erstellung eines Frequenzplans für das Mehrfamilienhaus.

Ich glaube, der Verwalter des Hauses, in dem der Autor wohnt, hat immer noch nicht aufgehört, über diesen Vorschlag zu lachen. Der Versuch, das Problem einer gemischten Eigentümerversammlung mit dem üblichen Anteil von Rentnern klar zu machen, endete in der langsamen Auflösung der Versammlung.

Ohne das näher auszuführen: Funktionen wie Dynamic Frequency Selection DFS helfen in dieser Situation genau deshalb nicht, weil alle APs das machen. DSL-Router kommen von den Providern mit Voreinstellungen in die Wohnungen. Erst in letzter Zeit ist das Bewusstsein dafür gestiegen, dass man wenigstens den voreingestellten WPA2-Schlüssel ab und an ändert. Änderungen der Frequenzen habe ich in diesem Umfeld noch nicht gesehen und das ist auch nichts für ganz normale durchschnittliche Benutzer.

Kommen wir jetzt zu hochdichten Umgebungen, meist in öffentlichen Bereichen. Sicher hier sind der planerischen Hand deutliche Grenzen gesetzt.

Betrachten wir ein Stadion. Wie breit ist so ein Schalensitz? Vielleicht 50 cm. Wie viel Platz ist zwischen Rückgrat und Kniescheibe? Mit Glück 80 cm. Die meisten Sitze in einem Stadion sind bestenfalls Economy. Selbst das einfachste WLAN kann rund 100 qm abdecken. Ein Sitzplatz ist 0,4 qm. Also passen rund 250 Fans unter ein WLAN. Viel zu viele für normale DCF-Steuerung. Natürlich kann ein Stadion-Besitzer eine vernünftige Zellplanung machen. Aber auch das hat Grenzen. Streng genommen gibt es nur drei

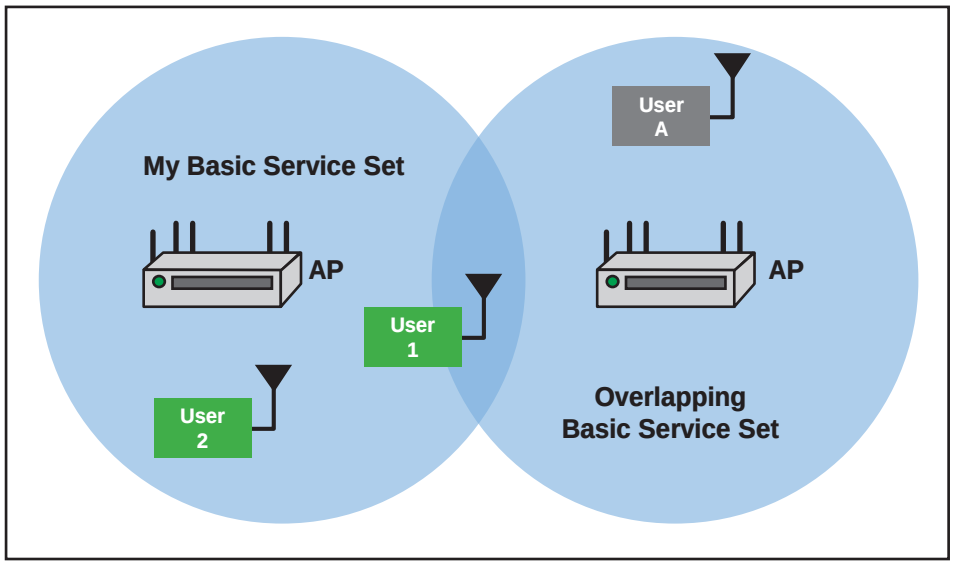


Abbildung 4: Ineffizienz des Medium-Zugriffs bei überlappenden BSS Quelle: NI

oder vier wirklich überlappungsfreie Frequenzbänder in herkömmlicher Technik. Ein UEFA-Stadion hat so um die 60.000 Plätze. Das ergibt ungefähr 240 notwendige Access Points. Viel Spaß bei der Planung.

Noch dramatischer sind aber die Verhältnisse in öffentlichen Verkehrsmitteln. In Stoßzeiten können sich hier durchaus auch 5 oder mehr Nutzer pro qm versammeln. Im Gegensatz zum Stadion bewegen sie sich aber zum Teil. Selbst ein einfacher S-Bahn Waggon kann mit Hunderten gefüllt sein. In Japan das Doppelte.

Ein weiterer Faktor, den es zu berücksichtigen gilt, ist die gemeinsame Benutzung breiterer Kanäle. Wir erinnern uns: in einen Kanal kann man nicht beliebig viele Bits pro Sekunde stecken, sondern seine Übertragungsleistung hängt maßgeblich von seiner Breite ab. Begonnen haben wir mit 20 MHz breiten Kanälen bei 802.11b. Mit 11ac können rein theoretisch 160 MHz breite Kanäle definiert werden, in Nord Amerika nur einer, in Europa zwei. Mit zwei Kanälen kann man keine flächendeckenden überlappungsfreien Infrastrukturen definieren. Je weniger Kanäle es gibt, desto mehr werden Netzwerk-Manager dazu gezwungen, Kanäle in benachbarten Zellen wiederzuverwenden. Ohne sorgfältiges und empfindsames Power Management kommt es zu Co-Channel Interferenz bei den Nutzern. Sie degradiert die Leistung und zerstört so mögliche Vorteile, die man sich von den breiteren Kanälen erhofft hatte. Das trifft besonders auf die durch dichtere Vorcodierung erzielten höheren Datenraten, die umso empfindlicher gegenüber schlechtem Signal/Rauschverhältnis sind, desto mehr sie theoretisch leisten.

Außerdem kennen die Kanäle keine Gnade. Ein 20 MHz-Kanal, der mit einem 80 MHz-Kanal interferiert, macht den 80 MHz Kanal insgesamt unbrauchbar, wenn auch nur ein einziger Nutzer auf dem 20 MHz-Kanal sendet. Die Implementierung der Kanalaufteilung von 802.11ac mit breiten Kanälen in hochdichten Umgebungen zerstört die möglichen Gewinne des breiteren Kanals.

3. Änderungen und funktionale Erweiterungen in der PHY

Die 802.11ax Spezifikation bringt eine Menge von Änderungen und funktionalen Erweiterungen in die PHY. Dennoch gibt es Rückwärts-Kompatibilität mit 802.11 a/b/g/n und ac/ Geräten. Eine 802.11ax Station kann Daten von Stationen nach allen bisherigen Standards senden und empfangen. Die Stationen, die nach älteren Standards arbeiten, können 11ax Paketköpfe demodulieren und decodieren und so auch einen Backoff durchführen, wenn eine 11ax Station sendet. Ganze 802.11ax-Pakete können sie jedoch nicht demodulieren und decodieren.

Tabelle 1 fasst die wichtigsten Änderungen von 11ax gegenüber 11ac zusammen. Es fällt sofort auf, dass 11ax auch die Nutzung des 2,4 GHz-Bandes ermöglicht, was man ja eigentlich eher mit den älteren Standards in Verbindung bringt. Die Kanal-Bandbreiten bleiben gleich, es ist aber auch keine sinnvolle Erweiterung mehr denkbar. Die OFDM-Unterträger sitzen bei 11ax näher zusammen als bei 11ac und 11ax kann als höchste Modulation im Rahmen der OFDM-Signalsynthetisierung 1024 QAM verwenden. Das war ja ursprünglich für 11ac auch angedacht, in der Praxis aber nicht wirklich zu implementieren. Die OFDM-Symboldauer ist bei 11ax deutlich höher. Bei den Datenraten gibt es keine großen Überraschungen, in der Tabelle 1 stehen die Werte für die theoretische Maximalleistung auf einem Kanal von 80 MHz ohne Nutzung von MIMO (mit einem Spatial Stream SS) und auf einem Kanal von 160 MHz mit der Nutzung von acht parallelen Wegen mit MIMO.

Die Spezifikation definiert eine vierfach größere FFT und multipliziert die Anzahl der Unterträger. Eine kritische Änderung gegenüber 11ax ist, dass der Abstand zwischen den Unterträgern auf ein Viertel des Wertes früherer Standards heruntergesetzt wurde, ohne die bisherigen Kanalbandbreiten zu verändern.

Die OFDM Symboldauer und das zyklische Präfix sind ebenfalls um den Faktor vier gewachsen und halten so die Rohdatenrate zunächst im Bereich von 11ac. Nur mit 1024 QAM und kleineren zyklischen Präfixen für Indoor Anwendungen kann die maximale Datenrate erhöht werden.

Wie ist das in der Praxis zu bewerten? Die engeren Zwischenräume zwischen den Unterträgern lassen sich nur mit einer insgesamt deutlich verbesserten Transceivertechnik implementieren. Um es populär auszudrücken: würden sich die Unterträger näherkommen und unter ungünstigen Bedingungen sogar überlappen, würde das gesamte OFDM nicht mehr funktionieren. Eine verbesserte Transceivertechnik mit steileren Filtern, möglichst linearen Verstärkern, Moderatoren und Antennen-Switches ist dafür absolut notwendig, aber auch nicht unrealistisch. Der erste WLAN-Standard mit OFDM war 802.11a und ist schon rund zwanzig Jahre alt. In dieser Zeit hat die Transceivertechnik erhebliche Fortschritte gemacht. Alleine Moore´s Law hat sozusagen zehnmal hintereinander zugeschlagen und die Möglichkeiten für komplexe, stabile Signalprozessoren deutlich verbessert. Kritisch ist vor allem die Temperaturabhängigkeit der Schaltungen, die aber ebenfalls nachhaltig verbessert wurde. Also wird es Zeit, dass auch in der Praxis zu nutzen.

802.11ax implementiert eine explizite Beamforming Prozedur, die der von 802.11ac ähnlich ist. Der Beamformer (Trainer) initiiert eine Prozedur zur Kanalprüfung mit einem Nulldaten-Paket. Der Partner (Trainee) misst den Kanal und antwortet mit einem Beamforming Feedback Frame, der eine komprimierte Feedback Matrix enthält. Der Beamformer nutzt diese Information zur Berechnung der Kanalmatrix H. Anschließend kann der Beamformer diese Kanalmatrix dazu nutzen, die RF-Energie gezielt auf jeden Nutzer zu richten. Das ist eine verkürzte Darstellung. Es gibt auch die Möglichkeit von längeren Beamforming Training Prozeduren und kürzeren Beamforming „Nachbesserungs“-Prozeduren. (siehe Abbildung 5)

	802.11ac	802.11ax
Bänder	5 GHz	2,4 GHz und 5 GHz
Kanal-Bandbreiten	20, 40, 80, 80 + 80, 160 MHz	20, 40, 80, 80 + 80, 160 MHz
FFT-Größen	64, 128, 256, 512	256, 512, 1024, 2048
Subcarrier Spacing	312,5 kHz	78,125 kHz
OFDM-Symboldauer	3,2 µs + 0,8/0,4 µs CP	12,8 µs + 0,8/1,6/3,2 µs CP
Höchste Modulation	256 QAM	1024 QAM
Datenraten	433 Mbps (80 MHz, 1 SS) 6933 Mbps (160 MHz, 8 SS)	600,4 Mbps (80 MHz, 1 SS) 9607,8 Mbps (160 MHz, 8 SS)

Tabelle 1: 802.11ac vs. 802.11ax PHY

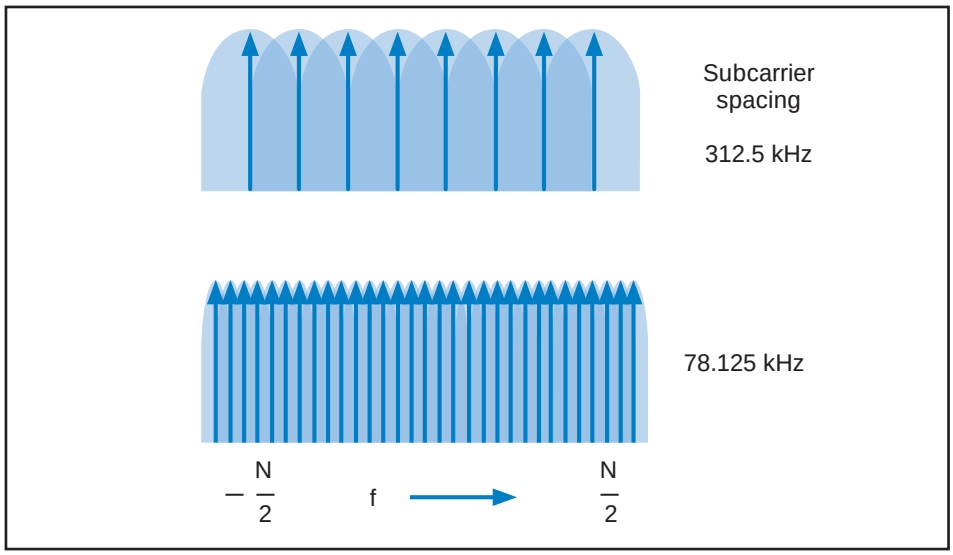


Abbildung 5: Engeres Subcarrier Spacing Quelle: NI

4. Multi-User Betrieb: MU-MIMO und OFDMA

Es gibt im Standard 802.11ax unterschiedliche Betriebsmodi, die auf den ersten Blick etwas verwirrend wirken. Grundsätzlich gibt es die Unterscheidung zwischen Single User und Multi User.

Der **Single User Modus** ist ein sequentieller Modus. Die Stationen senden und empfangen ihre Daten, sobald sie sicheren Zugriff auf das Medium haben wie weiter oben beschrieben. Man könnte auch sagen, dass der Single User Modus ein einfacher DCF-Modus ohne Zusatzfunktionen wie etwa bei 802.11a ist.

Der **Multi-User Modus** erlaubt den simultanen Betrieb mehrerer Teilnehmer-Stationen, die nicht Access Point sind. Der Standard unterteilt diesen Modus in Downlink- und Uplink Multi-User Betrieb.

Downlink Multi User bezieht sich auf Daten, die ein AP zur gleichen Zeit simultan an mehrere Nutzer-Stationen schickt. Der existierende 11ac-Standard spezifiziert diese Funktion als MU-MIMO.

Uplink Multi User beschreibt eine simultane Daten-Übertragung von multiplen Nutzer Stationen zum AP. Das ist eine neue Funktionalität des 802.11ax-Standards, die es bisher in keinem WiFi Standard gab.

Im Rahmen der zwei Multi User Modi spezifiziert der Standard zwei verschiedene Arten für den Multiplex mehrere Benutzer innerhalb eines begrenzten Bereiches: Multi-User MIMO und Orthogonal Frequency Division Multiple Access OFDMA. Bei beiden Verfahren arbeitet der AP als zentraler Controller für alle Aspekte des Multi-User Betriebs ähnlich einer Base Station bei LTE, die das Multiplexen der Subscriber steuert. Ein 802.11ax Access Point kann MU-MIMO mit OFDMA kombinieren. Wegen der zu einer Base Station ähnlichen Arbeitsweise wird ein 11ax-AP in der neueren Literatur auch gerne als 11ax-Base bezeichnet.

Genau wie in der 802.11ac Spezifikation nutzen die 802.11ax-Geräte für **MU-MIMO** Beamforming, um Pakete an räumlich getrennte Nutzer zu schicken. Der AP berechnet eine Kanalmatrix für jeden Nutzer und richtet gleichzeitig verschiedene „Strahlen“ zu den unterschiedlichen Nutzern, wobei jeder gerichtete Strahl die Information für den angepeilten Nutzer enthält. Im Gegensatz zu 802.11ac, wo vier unterschiedliche Ziele unterstützt werden, kann 802.11ax bis zu acht unterschiedliche Ziele bedienen. Jede MU-MIMO-Übertragung kann ihre eigene Modulations- und Codierungsmenge (MCS) und eine eigene Anzahl von Spital Streams haben. Man könnte für MU-MIMO eine Analogie zu einem Ethernet Switch bilden, der die Kollisions-Domäne von einem großen Netz auf einen einzelnen Port reduziert.

Als neue Eigenschaft beim MU-MIMO Uplink initiiert der AP mittels eines Träger Frames eine simultane Uplink-Übertragung von jeder der Stationen zum Access Point. Antworten die angesprochenen Stationen unisono mit ihren eigenen Paketen, wendet der AP die Kanal-Matrix auf die eingegangenen Strahlen an und extrahiert die Information, die jeder Uplink Beam enthält. Der AP kann auch Uplink Multi User Übertragungen initiieren, um von allen Stationen Beamforming Feedback Information zu erhalten. (siehe Abbildung 6)

Um mehrere Nutzer auf dem gleichen Kanal zu multiplexen, leiht sich 802.11ax eine bewährte technische Verbesserung aus der 4G Mobilfunktechnik: **OFDMA**. Man baut hier auf dem bereits für 802.11ac existierenden digitalen OFDM Modulationsschema auf. Prinzipiell gibt es die auf orthogonalen Unterträgern basierende sehr stabile Übertragungstechnik mit Signalsynthetisierung schon seit 802.11a. Bisher werden von einer Station zur Übertragung alle zur Verfügung stehenden OFDM-Unterkanäle gleichzeitig benutzt, wenn sie ihr Paket losschickt. **Die wesentliche Neuheit ist, dass der Standard 802.11ax unterschiedlichen Nutzern unterschiedliche Mengen von Unterkanälen zuordnet**. Das bedeutet, dass die existierenden 802.11-Kanäle (von 20, 40, 80 oder 160 MHz Breite) in kleinere Unter-Kanäle mit einer vordefinierten Anzahl von Unter-Trägern aufgeteilt werden. Genau wie in der modernen LTE Terminologie heißt der kleinste Unterkanal im

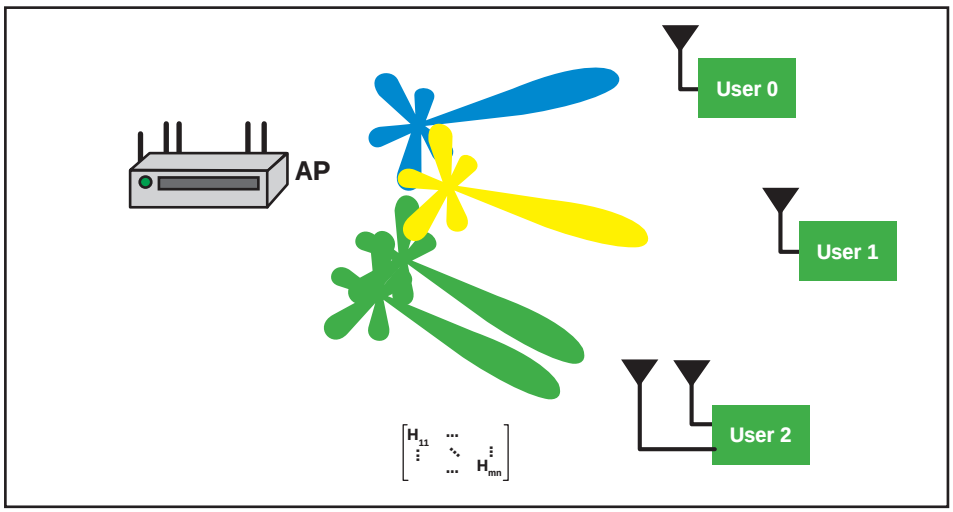


Abbildung 6: AP mit MU-MIMO sendet gerichtet an Teilnehmer Quelle: NI

IEEE 802.11ax: die neue WLAN Generation

802.11ax-Standard Ressource Unit (RU) und hat eine minimale Größe von 26 Unterträgern. Der AP entscheidet aufgrund der allgemeinen Verkehrssituation und dem Bedarf, wie der Kanal im Einzelnen zugeordnet wird. Es werden aber immer alle verfügbaren RUs auf dem Downlink benutzt. So kann der AP einem einzelnen Nutzer den gesamten Kanal geben, wie das 11ac aktuell macht, oder den Kanal partitionieren, um mehrere Nutzer parallel zu bedienen. Die Abbildung 7 zeigt eigentlich auf einen Blick, worum es geht.

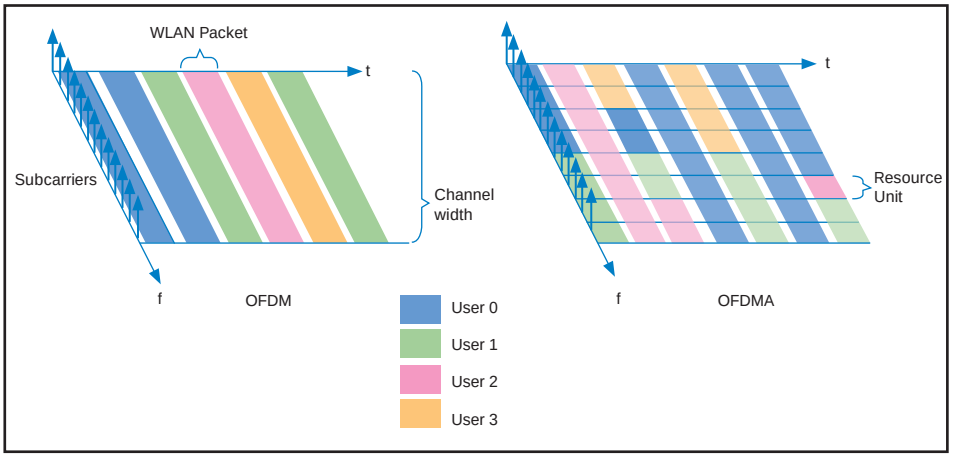


Abbildung 7: OFDM: ein Nutzer pro Zeiteinheit pro Kanal
OFDMA: mehrere Nutzer pro Zeiteinheit pro Kanal

In dichten Umgebungen, in denen viele Nutzer normalerweise ineffizient darum kämpfen würden, den Kanal Benutzer zu können, hilft der OFDMA-Mechanismus, sie simultan zu bedienen, zwar mit einem schmaleren Kanal, der dafür aber der Station eindeutig zugeordnet ist. So wird der mittlere Durchsatz pro Benutzer deutlich verbessert.

In Abbildung 8 sieht man, wie ein 802.11ax System Kanäle unter Nutzung verschiedener RU-Größen multiplexen kann. Die kleinste Unterteilung des Kanals ermöglicht bis zu 9 gleichzeitige Nutzer für jede 20 MHz Bandbreite. Danach haben wir noch die Tabelle 2, auf der man sieht, wie viele Nutzer Frequenz-multiplexten Kanalzugang bei unterschiedlichen RU-Größen und Kanalbandbreiten (CBW) bekommen können.

Zur Koordination von Uplink MU-MIMO oder Uplink OFDMA-Übertragungen sen-

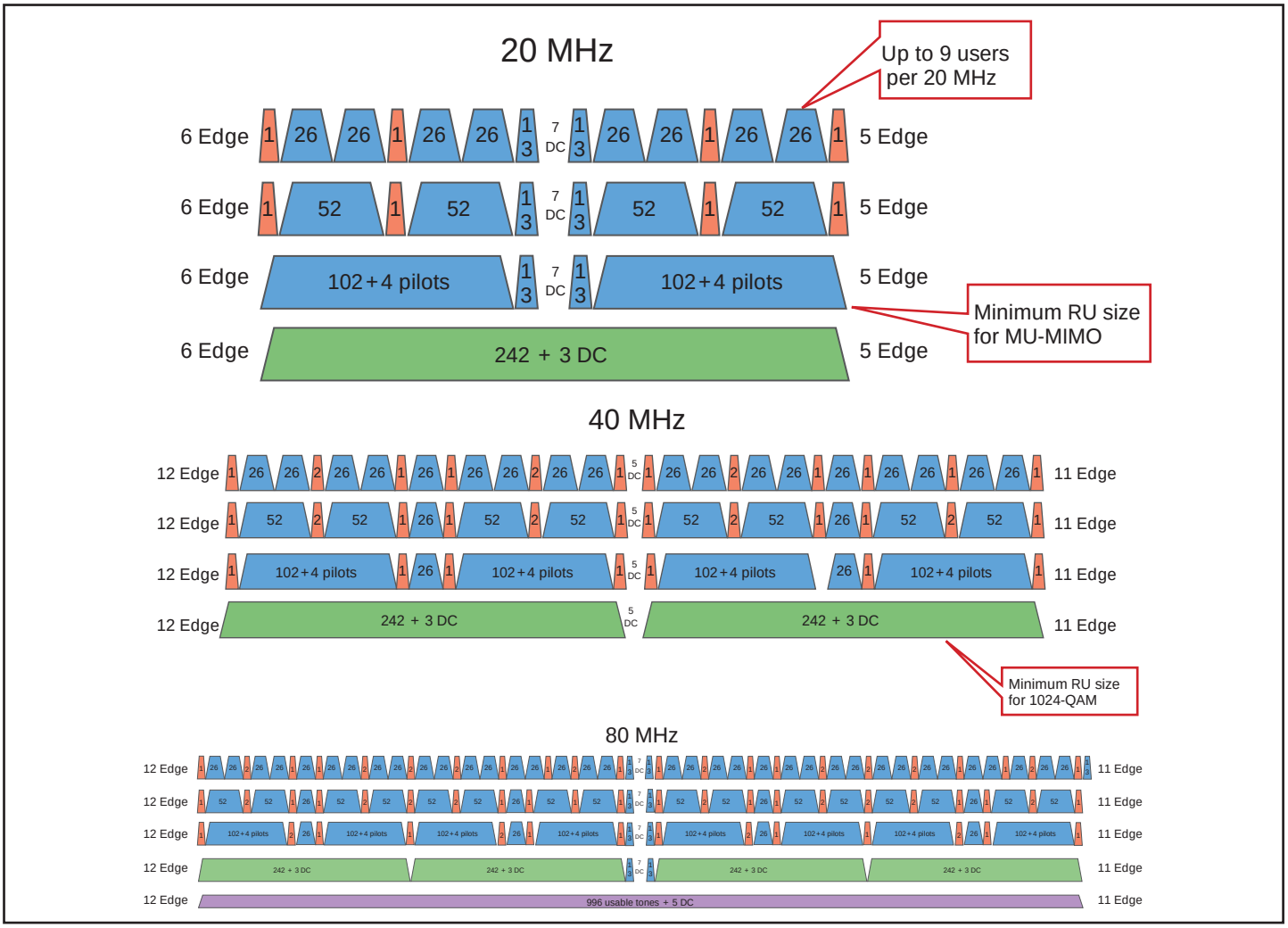


Abbildung 8: Unterteilung von WiFi-Kanälen mit unterschiedlichen RU-Größen Quelle: IEEE

RU-Typ	CBW20	CBW40	CBW80	CBW160
26 subcarrier	9	18	37	74
52 subcarrier	4	8	16	32
106 subcarrier	2	4	8	16
242 subcarrier	1-SU/MU-MIMO	2	4	8
484 subcarrier	N/A	1-SU/MU-MIMO	2	4

Tabelle 2: Anzahl möglicher Benutzer in Abhängigkeit von der Anzahl der Unterträger und der Gesamtbandbreite

det der AP einen Trigger-Frame an alle Nutzer. Dieser Frame indiziert die Anzahl der Spital Streams und/oder die OFDMA-Zuordnungen (Frequenz und RU Größen) für jeden Nutzer. Er enthält auch Informationen zur Power Control, so dass individuelle Nutzer ihre Übertragungsleistung herauf- oder herausstellen können. Das Ziel dabei ist es nicht, Energie zu sparen, sondern dafür zu sorgen, dass die Leistung, die der AP von den Stationen erhält, für alle Stationen möglichst gleich ist, egal ob die Station nun in der Nähe des APs ist oder weiter weg. Der AP teilt allen Stationen mit, wann sie mit der Sendung beginnen und diese beenden sollen. Der AP sendet einen Multi-User Uplink Trigger Frame, der den genauen Moment, an dem sie alle anfangen sollen zu senden, und die genaue Länge ihres Frames anzeigt, damit sie auch alle gleichzeitig mit dem Senden wieder aufhören. Sobald der AP die Frames von allen Stationen empfangen hat, schickt der ein Block ACK an alle. (siehe Abbildung 9)

Eines der Hauptziele von 802.11ax ist die Unterstützung eines viermal höheren durchschnittlichen Durchsatzes pro Nutzer in dichten Umgebungen. Mit diesem Ziel im Kopf haben die Designer spezifiziert, dass 802.11ax Geräte Downlink und Uplink MU-MIMO, MU-OFDMA oder beides unterstützen. Aber damit sind wir noch nicht fertig.

5. MAC-Mechanismen für hohe Effizienz

Neben den Verbesserungen in der PHY gibt es noch zwei zusätzliche MAC-Mechanismen.

5.1 Spatial Reuse mit Color Codes

Um die Leistung auf dem System-Level zu verbessern und die spektrale Ressourcen in dichten Umgebungen effektiv zu nutzen, definiert der 11ax Standard eine Technik zur räumlichen Mehrfachnutzung von Frequenzen.

Das ist für denjenigen, der mit Funktechnik nicht erfahren ist, unverständlich und für den Funk-Profi zunächst haarsträubend, wenn man es nicht mit Analogien erklärt.

Bei WLANs und anderen Funksystem ist es ja ein eisernes Gesetz, dass eine Frequenz auf einem bestimmten räumlichen Gebiet nur einmal benutzt werden soll, weil es sonst wüstes Durcheinander gibt. Das beginnt ja schon bei den Steuerungsverfahren für WLAN-Zellen, die ja grade dafür sorgen, dass auf einer Frequenz nicht zwei oder mehr Stationen gleichzeitig senden und setzt sich bei der Planung für flächendeckende Versorgungsbereiche fort, die dafür sorgt, dass Systeme mit gleichen Frequenzen nicht direkt nebeneinanderliegen. Beim Rundfunk hat jeder schon einmal erlebt, was passiert, wenn man mit dem Auto von einem Funkbereich zum nächsten fährt. Das Autoradio ist auf eine Frequenz eingestellt und irgendwann verlässt man den Wirkungsbereich eines Senders und tritt in den einer anderen Station ein. Häufig funktioniert das problemlos mit einer kleinen Pause. Bei bestimmten Wetterlagen und in Grenznähe gibt es aber stärkere Überlappungen, die dafür sorgen, dass man beide Sender zugleich hört, was unangenehm ist. Also auch hier haben wir gute Gründe, Frequenzen in gleichen Gebiet nicht mehrfach zu verwenden.

Jetzt verlassen wir den Funk mal kurz und gehen auf eine Party oder einen Empfang. Da stehen Dutzende oder Hunderte Leute herum und der Raum ist objektiv gesehen von massivem Durcheinander gesprochener Wörter aus vielen Stimmen erfüllt. Es gibt nur einen einzigen Frequenzbereich, nämlich den der menschlichen Stimme. Allerdings sprechen Personen mit bestimmten Charakteristika über diesen Frequenzbereich und auch mit sehr unterschiedlichen Lautstärken. Nach kurzer Zeit passiert aber Folgendes: wir verstehen ziemlich gut, was die Personen, die in unserer unmittelbaren Nähe sind, sprechen und filtern dabei die anderen Stimmen automatisch als Hintergrundrauschen aus. Das heißt, dass ein Mensch um sich herum eine Zone erschafft, in der er weitestgehend ungestörte Kommunikation hat, obwohl er sich mitten in einem fürchterlichen Durcheinander befindet. Diese Fähigkeit lässt leider meist mit dem Alter und einem schlechter werdenden Hörvermögen immer mehr nach. Aber wäre es nicht schön, wenn wir WLAN-Stationen diese Fähigkeit irgendwie beibringen könnten?

Die räumliche Mehrfachnutzung von Frequenzen in 802.11ax basiert darauf, dass Stationen Signale von überlappenden Basic Service Sets BSS identifizieren können und Entscheidungen über Wettbewerb für das Medium und Interferenz-Management basierend auf dieser Information treffen können. Und das geschieht auf Basis von Bitmustern, die im Standard als „Farben“ bezeichnet werden.

Wenn eine Station aktiv ins Medium hineinhört und einen 802.11ax Frame detektiert, prüft sie das BSS-Farb-Bit oder die MAC-Adresse im MAC-Header. Ist die BSS-Farbe in der empfangenen PPDU die gleiche Farbe, die der dazu gehörige AP schon veröffentlicht hat, betrachtet die Station diesen Frame als Intra-BSS-Frame. Hat der empfangene Frame aber eine andere Farbe als die eigene, fasst die Station diesen Frame als Inter-BSS Frame von einem überlappenden BSS auf. Die Station betrachtet dann das Medium nur so lange als BUSY, wie es dauert, festzustellen, dass der detektierte Frame zu einem überlappenden, fremden BSS gehört. Das ist in jedem Fall kürzer als die

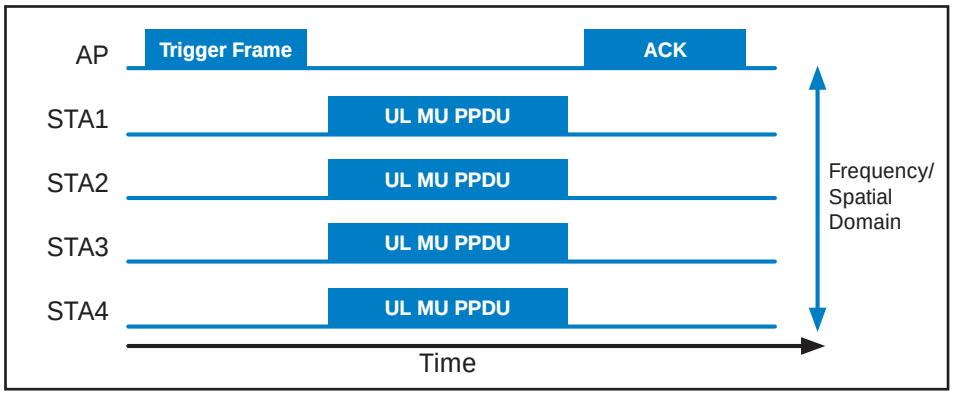


Abbildung 9: Koordination des Multi-User Betriebs im Uplink

Zeit, die als Länge der Payload dieses Frames angegeben wurde. (siehe Abbildung 10)

Der Standard muss die Mechanismen, mit denen Stationen Pakete von benachbarten überlappenden BSS ignorieren können, noch genauer definieren, aber eine Implementierung könnte eine Clear Channel Aassessment Signal Detection mit einem höheren Schwellwert für Inter-BSS Frames und einem geringeren für Intra-BSS-Verkehr enthalten, sozusagen wie im richtigen Leben. Auf diese Weise würde Verkehr von benachbarten BSS auf der gleichen Frequenz nicht unnötigen Wettbewerb um den Kanalzugang auslösen.

Wenn die 802.11ax Stationen die Clear Channel Assessment CCA Prozedur auf Grundlage der Farben nutzen, dürfen sie auch den Schwellwert für die Signal Detection eines überlappenden BSS zusammen mit der Transmit Power Control verstellen. Diese Verstellmöglichkeit verbessert die Leistung auf dem System-Level und die Nutzung der spektralen Ressourcen. Die 802.11ax Stationen können auch weitere CCA Parameter wie den Energy Desertion Level und den Signal Desertion Level nachstellen.

Neben der Nutzung der CCA zur Bestimmung, ob das Medium für den aktuellen Frame frei oder belegt ist, gibt es im 802.11-Standard auch den Network Allocation Vector NAV. Das ist ein Timer-Mechanismus, der eine Vorhersage des zukünftigen Verkehrs ermöglichen soll. Er zeigt den Stationen die Zeit an, die für die Pakete, die unmittelbar auch das aktuelle folgen, benötigt wird. Der NAV ist ein virtueller Carrier Sense Mechanismus, der Medium-Reservierungen für Frames vornimmt, die für den Betrieb eines 802.11 Protokolls wichtig sind, wie Control Frames oder Daten und ACKs nach einem RTS/CTS-Wechsel.

Im Standard gibt es wahrscheinlich am Ende nicht nur ein NAV-Feld, sondern zwei verschiedene. Ein Intra-BSS-NAV und ein Inter-BSS-NAV könnten einer Station dabei helfen, den Verkehr im eigenen BSS vorherzusehen und zu senden, wenn sie den Status im überlappenden BSS kennen.

5.2 Stromsparen mit Target Wake Time

Ein 802.11ax AP kann mit den teilnehmenden Stationen über die Nutzung der Target Wake Time TWT-Funktion für die Definition einer oder mehrerer spezifischen Zeiten, zu denen bestimmte Stationen das Medium nutzen können, verhandeln. Die Stationen und der AP tauschen Informationen aus, die auch die erwartete Dauer einer Aktivität umfassen. Auf diese Weise kann der AP den Grad des Wettbewerbs und die Überlappung von Stationen, die Zugriff auf das Medium haben möchten, kontrollieren. 802.11ax Stationen können TWT zur Senkung ihres Energieverbrauchs nutzen, indem sie einen Schlafzustand einnehmen, bis sie dran sind, also ihr TWT ankommt. Weiterhin kann ein AP eine Art Scheduling über verschiedene Stationen ausüben und einfach TW-Werte an Stationen schicken, ohne dass vorher mit ihnen zu verhandeln. Im Standard nennt man das **Broadcast-TWT-Betrieb**.

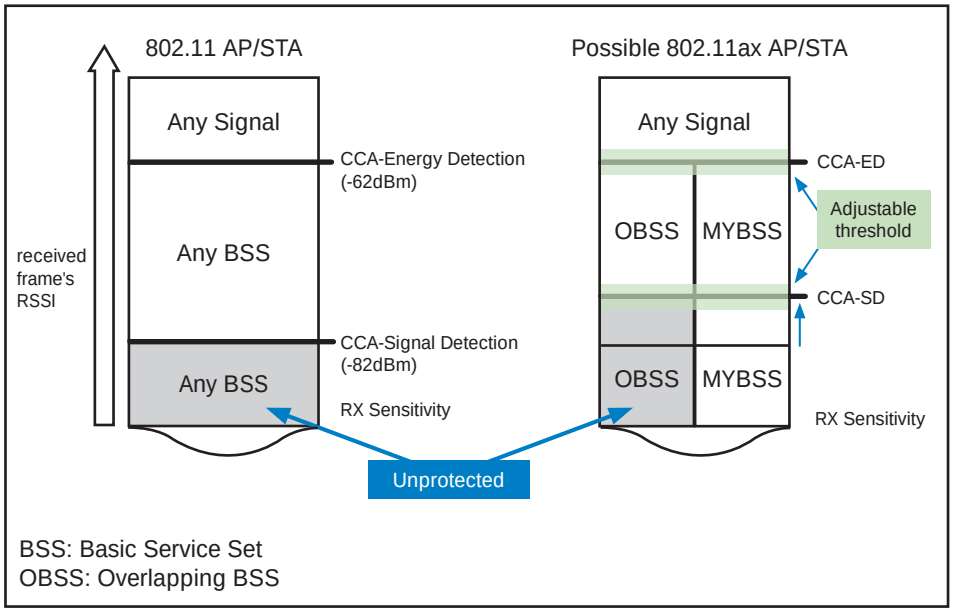


Abbildung 10: Nutzung von Farbcodes für Clear Channel Assessment Quelle: NI

6. Besondere technische Herausforderungen

Wie praktisch jeder seiner Vorgänger betritt der Standard 11ax ausgehend von einer sicheren übertragungstechnischen Position auch Neuland. Aus der Vergangenheit wissen wir, dass das nicht immer erfolgreich ist. So wurden z.B. für 802.11n lange 600 Mbps als maximale Zellenleistung angepriesen, in der Praxis aber nie erreicht. Bei 802.11ac gibt es auch schon die 1024-QAM Vorcodierung. Sie führt aber zu einem Signal, welches so empfindlich ist, dass seine tatsächliche Nutzung auch in Zukunft fraglich ist. Letztlich hoffen die Väter und Mütter der Standards, dass sich die Nachrichten-Übertragungstechnik im Zeitraum zwischen Standard und Implementierung grade so weit verbessert, wie es für die erfolgreiche Implementierung des Standards hilfreich und notwendig ist. Wie gesagt klappt das aber nicht immer. Höhere Anforderungen an die Übertragungstechnik führen natürlich auch dazu, dass die Hersteller von Meß- und Prüfgeräten immer neue Wege beschreiten müssen. Sehen wir uns die schlimmsten Baustellen einmal an.

6.1 Engere EVM Anforderungen

EVM steht für Error Vector Magnitude und ist ein Maß zur Quantifizierung der Leistung eines Senders oder Empfängers eines digitalen Radios. Ein Signal, was von einem idealen Sender gesendet oder einem idealen Empfänger empfangen wurde, wäre alle QAM Konstellationspunkte an der präzise richtigen Stelle haben. Verschiedene Unzulänglichkeiten in der Fertigung (Carrier-Überlappung, Phasenrauschen …) führen aber dazu, dass die realen Konstellationspunkte von den idealen Positionen abweichen. Informell gesehen ist EVM ein Maß für den Grad dieser Abweichung. Kanalrauschen, Störungen, verzerrte Signale und Phasenrauschen setzen der digitalen Signalqualität zu. Bei Multi-Carrier Modulation korreliert EVM mit dem Modulations-Fehler-Verhältnis, das ist das Verhältnis zwischen mittlerer Signal-Leistung zu mittlerer Fehler-Leistung.

Der 802.11ax Standard unterstützt 1024 QAM. Außerdem sind die Unterträger nur 78,125 kHz voneinander entfernt. Das bedeutet, dass 802.11ax Geräte Oszillatoren mit einer deutlich verbesserten Leistung hinsichtlich des Phasenrauschens und RF Front Ends mit besserer Linearität benötigen. Die Tabelle 3 zeigt, welche EVM-Level 802.11ax-fähige Geräte wahrscheinlich haben müssen.

6.2 Absoluter und relativer Frequenzfehler

OFDMA-Systeme sind sehr empfindlich gegenüber Frequenz- und Taktungs-Abweichungen. Daher hängt die Leistung im OFDMA Multi-User Betriebsmodus von

	16-QAM	64-QAM	256-QAM	1024-QAM
802.11ax EVM Anforderung	-19 dB	-27 dB	-32 dB	-35 dB

Tabelle 3: Anforderungen an EVM

einer extrem engen Korrektur von Frequenz- und Taktungsfehlern ab. Dazu müssen ALLE Stationen exakt innerhalb der ihnen zugewiesenen Unterkanäle arbeiten und es darf nur ganz minimale spektrale „Undichtigkeiten“ geben. Die strikten Anforderungen an das Timing garantieren u.A., dass alle Stationen gleichzeitig auf die MU Träger Frames des Access Points antworten.

Im Fall von 4G LTE haben die Basis-Stationen den Vorteil, dass die Clocks aller teilnehmenden Stationen über GPS reguliert werden. Für 802.11ax APs wird es einen derartigen Luxus nicht geben und sie müssen die gesamte System-Synchronisierung auf Basis ihrer eigenen eingebauten Oszillatoren vornehmen. Stationen können ihre internen Clock- und Frequenz-Referenzen durch Extraktion der Offset-Information aus den Trigger Frames, die sie vom AP bekommen, nachstellen. Die Toleranzen für absolute Frequenzabweichungen liegen im Bereich derer von 11ac. Die Toleranzen für relative Frequenzabweichungen betreffen die Fähigkeit einer Station, sich im Rahmen der Uplink Multi-User Übertragung auf die Arbeitsfrequenz des APs einzustellen. Sie sind sehr eng, denn die Abweichungen müssen weniger als 350 Hz und +/- 0,4 µs relativ zum Trigger Frame des APs sein.

6.3 Transmit Power Control der Station

Ähnlich der Anforderung nach geringen Abweichungen in Frequenz und Taktung sollte die Leistung, die ein AP während der Multi-User Übertragungen empfängt, über alle teilnehmenden Stationen hinweg keine größeren Abweichungen haben. Daher muss der AP die Sendeleistung jeder teilnehmenden Station kontrollieren. Dazu kann der AP einen Trigger-Frame benutzen, der die Information über die richtige Sendeleistung für jede Station enthält. Entwickler können diese Funktion zusammen mit den Frequenz- und Taktungsabweichungen testen. Die Empfindlichkeit des Empfängers im AP ist ebenfalls ein wesentlicher Punkt. Es muss ja sichergestellt werden, dass er in einem Multi-User Betrieb auch dann ordentlich arbeitet, wenn sich manche oder alle teilnehmenden Nutzer entfernen, so dass in einem konventionellen WLAN und nur einem Nutzer pro Zeiteinheit die nächst höhere Empfindlichkeitsstufe eingestellt würde.

Der Kommentar des Autors ist an dieser Stelle, dass grade die Anforderungen an enge Taktung, Frequenztreue und Empfindlichkeitskontrolle, die wir in konventionellen WLANs, wo es ja zu jedem Zeitpunkt nur die Kommunikation zwischen einem AP und einem einzigen Nutzer gibt, sehr gut im Griff haben, in der Multi-User-Umgebung dann zu großen Problemen führen kann, wenn die Nutzer nicht „still sitzen“ bleiben, sondern sich stochastisch bewegen. Ich bin aus der Erfahrung davon überzeugt, dass die 11ax-Systeme hier sehr schnell an ihre Grenzen stoßen werden. Was machen sie in einem solchen Fall? Naja, sie schalten einfach auf den Single User Modus zurück und dann haben wir ein leicht veredeltes 11ac-Netz und nichts weiter.

7. Konsequenzen für flächendeckende WLANs in Unternehmen und Organisationen

Der Standard IEEE 802.11ax verspricht eine Verbesserung des mittleren Durchsatzes pro Benutzer in dichten Umgebungen um den Faktor 4. Nicht mehr und nicht weniger. Dazu werden folgende Technologien und/oder Parameteränderungen herangezogen:

- Neue Modulations- und Codierungsmengen mit 1024-QAM
- Spezifikation von Multi-User Modi für Uplink und Downlink mit MU-MIMO und OFDMA
- Erweiterte OFDM FFT-Größen, 4 Mal engeres Spacing für die Unterträger und längere Symboldauer
- Spatial Reuse

In der Einleitung haben wir mögliche Einsatzszenarien und auch die Probleme mit bestehenden WLANs in diesen Szenarien besprochen. Die Kernfrage ist aber:

- Gibt es in herkömmlichen Unternehmen und Organisationen wirklich „hochdichte“ Umgebungen in der Art, wie sie im Standard gemeint sind in statistisch spürbarer Größenordnung?

Der Autor ist der Ansicht, dass Unternehmen in den meisten Fällen weder ein Stadion noch eine U-Bahn sind und im Rahmen der professionellen neuen Arbeitsplatzmodelle mit mobiler Anbindung eine Dichte wie in Stadien, U-Bahnen oder Hotspots nicht erreicht wird, mit Ausnahme vielleicht der Kantine. Also ist der Einsatz von Systemen nach dem Standard 802.11ax zunächst eher weniger erforderlich.

In der Werbung arbeitet der Hersteller Broadcom mit der nachdrücklichen Behauptung, dass „die Steuerungstechnik von 802.11ax die gleiche wie bei LTE sei … und daher das System „deterministisch“ ist“.

Was bedeutet das? Wie in der Einleitung schon dargestellt, ist einer der wesentlichen traditionellen Mängel von WLANs bis 802.11ac, dass man für einen Nutzer keine Datenrate garantieren kann, je höher die Gesamtlast in einer Zelle wird, desto höher wird die Wahrscheinlichkeit, dass man eigentlich gar keine Übertragung mehr für ihn garantieren kann. Außerdem ist es so wie im richtigen Leben, dass sich manche Nutzer einen ziemlich großen Teil der zur Verfügung stehenden Bandbreite unter den Nagel reißen können, während andere fast leer ausgehen, um es mal populär zu formulieren.

Mit der Einführung von OFDMA, dem bewährten Steuerungsverfahren aus LTE soll Fairness zwischen den Stationen gewährleistet werden, aber klappt das wirklich?

Zur Verwirrung der Interessenten werden zwei grundsätzliche Betriebsarten vorgestellt: Single User SU und Multi User MU. SU ist nichts weiter als ein 11ac-Modus, also damit ist eigentlich nichts gewonnen. MU zerfällt dann in die zwei Alternativen MU-MIMO und OFDMA.

MU-MIMO kennen wir schon aus 11ac und wenn es überhaupt funktioniert, ist seine Wirkung doch beschränkt. Der Laie in der Funktechnik kann sich MU-MIMO leicht vorstellen, wenn man eine Analogie zur Übertragung von Licht im Freiraum findet, nämlich Lichtmorsen mit der Taschenlampe. Normalerweise hat ein AP im SU-Modus nur eine Taschenlampe, die alle sehen können. Im MU-MIMO-Modus bekommt er jetzt z.B. vier Taschenlampen, die er in verschiedene Richtungen hält (wo er jeweils den Empfänger vermutet) und auf jeder Taschenlampe gibt es andere Signale. Jetzt nehmen wir einmal an, die Empfänger räumlich sind weit genug voneinander getrennt. Dann hat das gute Chancen. In einer hochdichten Umgebung sind die Empfänger aber grade sehr eng beieinander und die Chancen, dass jeder Empfänger noch genau das zu ihm passende Signal gut „sehen“ kann, sinken erheblich. Je enger die Empfänger benachbart sind, desto schwieriger wird es, die für den jeweiligen Empfänger bestimmte Information aus den interferieren-

den Sendungen zu extrahieren. Also ist im Umkehrschluss MU-MIMO umso ungeeigneter, desto dichter die räumliche Population mit Nutzern ist.

Nun dann, bliebe noch OFDMA. OFDMA ist nach Konstruktion deterministisch und damit fair. Weltweit funktionieren Milliarden Mobiltelefone und andere mobile Endgeräte prima mit LTE-OFDMA. Es fallen aber sofort folgende Probleme auf:

- OFDMA ist nur einer von drei Betriebsmodi. **Auch wenn OFDMA deterministisch ist, kann man daraus keineswegs ableiten, dass das gesamte 802.11ax-System deterministisch ist**, wie der Chip-Hersteller Broadcom das macht. Die anderen zwei Betriebsmodi sind nämlich definitiv **nicht deterministisch**.

- Für OFDMA werden die üblichen OFDM-Kanäle noch weiter in Ressource Units aufgeteilt, was aber eigentlich nur ein anderer Name für sehr schmale Kanäle ist. Diese sehr schmalen Kanäle liegen sehr eng beieinander, für die reibungslose Funktion von OFDMA ist es aber nötig, dass sie sich keinesfalls überlappen. Die Anforderungen an Frequenzstabilität und Synchronisierung werden dadurch viel höher als bei „normalen“ WLANs. WLANs sind traditionell eine Billig-Technologie. Können die Hersteller hier tatsächlich Produkte liefern, die diesen erhöhten Anforderungen wirklich gerecht werden? Das müssen wir schon abwarten. Noch spannender ist es, wie diese Dinge bei Consumer-Produkten realisiert werden.

- Um am OFDMA Multi-User Modus teilnehmen zu können, müssen **ALLE** Stationen in der Zelle die kleinen RUs verarbeiten können und für sie auf bestimmten Frequenzen liegende Informationen aus den Trigger-Frames richtig verarbeiten können. **Das bedeutet, dass ALLE Stationen 802.11ax können müssen! Schon eine einzige 802.11ac oder gar 802.11n-Station in der Zelle verdirbt den Spaß** und alle müssen im Zweifel auf den SU-Modus zurückschalten. So, jetzt stellt sich die Frage: wie wahrscheinlich ist es denn, dass wir in den nächsten Jahren „reine“ 11ax-Nutzerumgebungen bekommen? Sehr unwahrscheinlich.

Für mich ist diese Frage wirklich zentral, denn OFDMA ist das Bonbon am 802.11ax-Standard. Wie lange leben Mobilgeräte? Hersteller sind gerne davon überzeugt, dass die Besitzer ihrer Geräte nur auf das nächste, bessere, Gerät warten. So rechnen Apple und auch viele der Analysten tatsächlich damit, dass Nutzer spätestens alle zwei Jahre ihr Gerät wechseln. Die Realität sieht anders aus. Die Geräte haben immer mehr Möglichkeiten, von denen praktisch immer weniger benutzt werden, und es gibt immer weniger Anreize, das Gerät zu wechseln. Die Handy-Kameras sind schärfer als jedes Auge das nutzen kann und Funktionen wie dreidimensionale Gesichtserkennung sind ganz nett, es geht aber auch für viele Nutzer ohne. Die Geräte werden immer teurer, Apple reißt locker die 1000 US$-Marke und dafür muss ein Jugendlicher viele Autos waschen. Realistischer ist eher eine Nutzungsdauer von 4 oder mehr Jahren.

Ein Bereich, der wirklich von 802.11ax mit fairem OFDMA profitieren könnte, ist die industrielle Fertigung. Kompetente Kollegen, die in diesem Bereich arbeiten, sagen mir aber immer wieder, dass hier die Lebensdauer älterer Standard-Varianten noch deutlich höher ist. Also wieder nichts.

Letztlich ist die Frage: **wann werden hoch dichte Umgebungen so aussehen, dass wirklich alle Nutzer 802.11ax-fähige Handys (oder besser) haben und dann OFDMA sinnfällig eingesetzt werden kann?**

Und selbst wenn das tatsächlich einmal so sein sollte, enden die Probleme damit nicht.

Ein verbreitetes Problem bestehender flächendeckender WLAN-Installationen ist das **„Kleben“** einer Station an einem Access Point. Die Station arbeitet mit diesem AP, entfernt sich aber von ihm. Dadurch wird die Signalqualität immer schlechter und die Station muss die Datenübertragungsgeschwindigkeit immer weiter herabsetzen. „Kleben“ bedeutet, dass sie das auch macht, wenn eigentlich schon ein für die Kommunikation besser geeigneter AP ganz in ihrer Nähe ist und sie dorthin Roamen sollte. Aber nein, macht sie nicht, sondern klebt an ihrem alten Kommunikationspartner. Natürlich gibt es bei WLANs für professionelle Anwendungen Hilfsmittel, mit denen man genau das abstellen kann, aber das ist nicht der Allgemeinfall.

Die Multi-User Modi von 802.11ax (MU-MIMO und OFDMA) fördern aber grade das „Kleben“, denn die Versammlung der mit ihnen arbeitenden Stationen ist genau ihre Arbeitsgrundlage. Wenn da Stationen verschwinden und wiederkommen, wie es grade passt, sinkt die Gesamtleistung wegen der notwendigen Umkonfigurierungen. Das pingelige Nachstellen von Sende- und Empfangsleistungen ist hier nicht wirklich hilfreich.

Die erweiterten OFDM-FFT-Größen wollen wir hier nicht weiter kommentieren.

Der Spatial Reuse widerspricht massiv dem, was wir in den vergangenen Jahren im Rahmen einer verantwortungsvollen Frequenzplanung gemacht haben. Das Ganze hört sich sinnvoll an, mag im Labor praktisch funktionieren, Beweise für

die Sinnfälligkeit unter harten praktischen Bedingungen stehen aber noch aus.

Fassen wir nochmal zusammen:

- die für den Standard angenommenen „hochdichten“ Nutzerumgebungen kommen in normalen Unternehmen und Organisationen eher selten vor.
- das von Chip-Herstellern versprochene deterministische Verhalten kann sich nur dann einstellen, wenn alle Stationen 802.11ax beherrschen. Das ist für die nächsten Jahre eher unwahrscheinlich.
- die für Datenraten jenseits der Leistung von 11ac notwendige Präzision in der Übertragungstechnik ist mit einem erhöhten Aufwand in den Schaltungen verbunden. Dieser sollte aber durchaus geleistet werden können, da Endgeräte ja mit Multi-Normen Radios arbeiten, die auch die neuen LTE- und 5G-Übertragungstechniken enthalten werden. Hier gibt es viele nutzbare Synergien.

Der Standard und zu ihm passende Produkte werden in 2018 kommen. Es ist aber fraglich, ob die unmittelbare Notwendigkeit besteht, Planungen jetzt panisch danach auszurichten.

Nach einer gewissen Einführungsphase mit den üblichen Rückschlägen wird der Standard die Versprechungen für die eingangs dargestellten speziellen Anwendungsbereiche durchaus halten und hier zu Verbesserungen führen. Lediglich im Sektor der Nutzung von Small Cells im Zusammenhang mit LTE Advanced oder 5G fehlen mir zum heutigen Zeitpunkt noch Bausteine um zu entscheiden, ob das wirklich am Ende nützlich funktioniert.

Der Betreiber normaler flächendeckender Infrastrukturen in Unternehmen und Organisationen wird oberflächlich gesehen in nächster Zeit nicht so stark von 802.11ax profitieren können.

Aber, man darf nicht vergessen, dass mit 11ax eine deutlich verbesserte Transceivertechnologie mit erhöhter Trennschärfe (wegen der engeren Abstände der OFDM-Unterkanäle) und somit deutlich optimiertem Signalverhalten kommt. Installiert man 11ax auch schon bei nur wenigen 11ax-fähigen Endgeräten, so ist man für die nächsten Jahre auf der sicheren Seite, was die eigentliche Übertragungstechnik anbetrifft. Das wird vor allem dann entscheidend, wenn sich mit LTE Advanced und 5G die Mobilfunknetze auch auf den lizenzfreien WLAN-Frequenzen breitmachen. Aus der Erfahrung kann man sagen, dass gute Access Points für eine neue WLAN-Generation nach kurzer Zeit nicht mehr kosten als die der Vorgänger-Generation. Das wird auch bezüglich 11ax vs. 11ac so sein.

Deshalb ist das überraschende Fazit, dass 11ax für flächendeckende Infrastrukturen in Unternehmen und Organisationen alleine wegen der besseren Übertragungstechnik sehr interessant ist, auch wenn die unmittelbaren Auswirkungen auf durchschnittliche Anwendungsszenarien zunächst eher gering sind.

IT-Sicherheits-gesetz und Kritis-Verordnung - eine „etwas andere“ Betrachtung

Fortsetzung von Seite 1

Oliver Flüs ist seit mehr als 20 Jahren Senior Consultant der ComConsult Beratung und Planung GmbH. Er verfügt über tiefgehende IT-Kenntnisse und langjährige Projekterfahrung. Als Leiter des Competence Center IT-Service und Senior Consultant für IT-Sicherheit ist er praxiserfahren in der Anwendung anerkannter Standards in den Bereichen IT-Service-Management und Informationssicherheitsmanagement. Ein wesentlicher Schwerpunkt seiner Arbeit ist die Begleitung der systematischen Vorbereitung von IT-Bereichen bei Kunden auf verschiedene Arten von Audits und Zertifizierungen. Dazu wirkt er in den Competence Centern IT-Sicherheit, Netze sowie Tests und Analysen mit, etwa bei der Erstellung von Konzepten, Ausschreibungsunterlagen inklusive Testspezifikationen, sowie Dokumentation zu technischen Lösungen und deren Betrieb.

IT-Sicherheitsgesetz - ein paar Fakten als Einstieg

Das IT-Sicherheitsgesetz vom 17. Juli 2015 umfasst Änderungen zu verschiedenen Gesetzen, um damit wichtigem Sicherheitsbedarf erhöhten Nachdruck zu verleihen.

Betreibern von Web-Angeboten (z.B.: Online-Shops oder ähnliche „E-Business-Präsenzen“) wird abverlangt, erhöhte Anforderungen an den Schutz der Kundendaten und der verwendeten Systeme zu erfüllen. Telekommunikationsunternehmen wird gezielt die Pflicht auferlegt, Sicherheitsmaßnahmen nicht nur zum Schutz personenbezogener Daten, sondern auch zur Vermeidung unerlaubter Zugriffe auf die von ihnen betriebenen Infrastrukturen zu treffen. Darüber hinaus werden verstärkte Meldepflichten von Telekommunikationsunternehmen gegenüber den Kunden sowie gegenüber der Bundesnetzagentur eingeführt.

Des Weiteren sieht das IT-SiG umfangreiche Änderungen des BSI-Gesetzes von 2009 vor.

Insbesondere werden Betreiber kritischer Infrastrukturen im Sinne des Gesetzes verpflichtet, „angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen maßgeblich sind.“

Maßnahmen der geforderten Art und Angemessenheit muss der Betreiber einer kritischen Infrastruktur spätestens zwei Jahre nach Inkrafttreten einer Rechtsverordnung treffen, über deren Festlegungen diese Infrastruktur als „kritisch“ im Sinne des IT-SiG/ der entsprechenden Änderungen des BSI-Gesetzes anzusehen ist. Die in 2016 verabschiedete erste Version der entsprechenden „Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz“ (BSI-Kritis-Verordnung“, BSI-KritisV) nennt entsprechende Kriterien und Schwellwerte für Einrichtungen der Sektoren Energie, Wasser, Ernährung sowie Informationstechnik und Telekommunikation.

Im Mai 2017 wurde nun die „Erste Verordnung zur Änderung der BSI-Kritis-Verordnung“ verabschiedet. Diese ist inhaltlich der „2. Teil der Festlegung von Kriterien zur Identifikation kritischer Infrastrukturen“, jetzt für die Sektoren Gesundheit, Finanz- und Versicherungswesen sowie Transport und Verkehr. (siehe Abbildung 1)

Der Betreiber einer so durch Schwellwertüberschreitung identifizierbaren Kritischen Infrastruktur (eigentlich genauer: einer entsprechenden typischen Anlage wie in der Kritis-Verordnung je nach Sektor benannt) hat gemäß den Inhalten des IT-SiG unter anderem mindestens alle zwei Jahre das geforderte Ergreifen angemessener störungsvermeidender organisatorischer und technischer Vorkehrungen gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) nachzuweisen. Der Nachweis wird geführt über (Dokumentation zu) Sicherheitsaudits, Prüfungen oder Zertifizierungen.

Dies bedeutet gemäß entsprechender Fristenregelung im IT-SiG in der Praxis: Gemessen ab dem Erscheinen der Fassung der Kritis-Verordnung, der die eigene Anlage „sektorentechnisch“ zu-

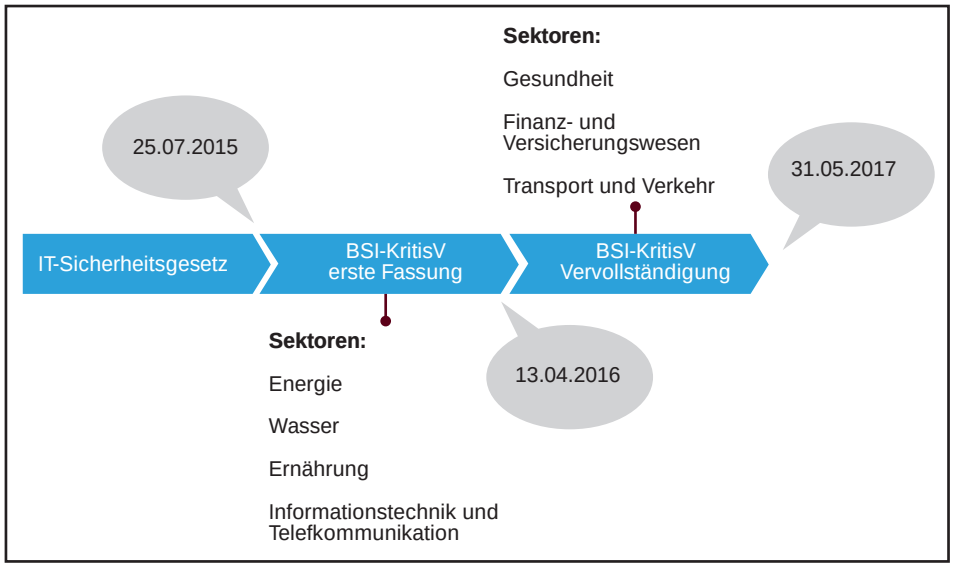


Abbildung 1: „Startpunkte" IT-SiG / Kritis-Verordnung zur Identifikation kritischer Infrastrukturen

zuordnen ist, hat man ca. 2 Jahre Zeit, um festzustellen, dass man eine Anlage mit Größenordnung / Bedeutung „für das Gemeinwesen“ betreibt, deretwegen man als Kritis-Umgebung einzustufen ist, Maßnahmen zur Ausfallsicherheit der zugehörigen „kritischen Dienstleistung“ und Vorkehrungen und interne Regelungen für Vorfallerkennung und Einhaltung von Meldepflichten nötigenfalls zu schärfen bzw. zu ergänzen, entsprechende Dokumentation zu ergänzen bzw. aufzubauen und eine zugehörige Prüfung zu durchlaufen, so dass man einen Version 1.0 eines nach IT-SiG vorzulegenden Nachweises vorlegen kann.

Hier ein erster dringender Hinweis für die Praxis - zwei Jahre sind schnell um, angesichts des Katalogs an Pflichtthemen, der abzudecken ist! Potenzielle Kandidaten sollten keine Zeit verlieren, ihren Kritis-Status zu verifizieren. Hat man entsprechende Gewissheit, sollte man sich unverzüglich (!) entsprechend über Pflichten kundig machen und aktiv werden, am besten in Projektform, um ausreichend Ressourcen und Tempo sicher zu stellen. Selbst wenn man glaubt, Maßnahmen-technisch mit Blick auf Störungsvermeidung und -behandlung gut dazustehen, ist da immer noch die Dokumentenlage und die durchzuführende Prüfung als Arbeitspunkt - und bei allen im weiteren beleuchteten Freiheitsgraden zur Wahl der Schwerpunkte und der Strategie des „Konzentrierens auf im Sinne der Kritikalität Wesentliches“ sind Mindest-Themenfelder von Tagesgeschäft bis zu Sonderfallbetrachtung zu „Business Continuity“ mit Blick auf die kritische Anlage und die damit erbrachte kritische Dienstleistung schon dokumentationstechnisch keine Kleinigkeit. Die Praxiserfahrung des Autors des vorliegenden Artikels mit Dokumentation zu derartigen Themen lässt erwarten, dass in jedem Fall Arbeit ansteht, die sich nicht „nebenbei“ innerhalb von zwei Jahren erledigt.

IT-SiG-Anwendung in der Praxis - Denk- und Arbeitshilfen für jedermann

Nun gibt es ausführlichere Informationen zum IT-Sicherheitsgesetz samt Kritis-Verordnung. Wer einen direkten Einstieg sucht, kann etwa die Startseite der Web-Präsenz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) besuchen und findet dort direkten Zugang zu erläuternden Texten (Broschüren, FAQs, sowie Weiterleitungen zu weiteren Informationen). Wer bereits festgestellt hat, dass er unmittelbar betroffen ist bzw. zumindest innerhalb der fraglichen Branche eine Größenordnung hat, dass er Betreiber einer kritischen Infrastruktur sein könnte, wird sich mit solchen Informationen bereits beschäftigt haben bzw. dies gerade tun.

Warum also (noch) ein Artikel, der auf das IT-SiG und die Kritis-Verordnung hinweist? Außerdem ist das doch nur ein Thema für ein Fachblatt, das sich gezielt an Umgebungen entsprechender Größe richtet?

Nein!

Sollte eine betrachtete Infrastruktur gemäß BSI-KritisV nicht sofort als Kritische Infrastruktur im Sinne des IT-SiG zu betrachten sein, aber einem maßgeblichen Schwellwert zumindest nahe kommen, ist es natürlich sinnvoll, sich bereits jetzt gezielt an den Kritis-Anforderungen zu orientieren.

Insbesondere bei anstehenden größeren Veränderungen im Bereich IT-Ausstattung bzw. IT-Infrastruktur kann man hier ohne erschreckenden Mehraufwand im Rahmen von Planung und Entscheidungsfindung zumindest die Weichen stellen, um nicht später „im laufenden Betrieb“ unter Zeitdruck bei Lösungsdetails oder Dokumentation nachlegen zu müssen. Wer möchte schon „Opfer des eigenen Erfolgs“ werden, wenn er durch Wachstum später „Kritis-Größenordnung“ erreicht?

Auch für kleine bis mittlere Umgebungen ohne realistische Prognose zum zukünftigen Wachstum in Richtung „Kritis-Bedeutung“ bieten IT-SiG zusammen mit dem Kritis-Thema Denkhilfen, die man nicht übersehen sollte - man muss nur das Stichwort „kritisch“ sinnvoll auf die eigene Situation anwenden. Kann man sich wirklich allein auf die erfolgreiche Umsetzung des IT-SiG durch Versorger und Dienstleister mit Kritis-Status stützen, deren Leistungen man dann in Anspruch nimmt?

Die tägliche Praxis zeigt doch: Niemand ist in der Lage, eine Garantie für absolute Ausfallsicherheit zu geben - und dann? Wenn man in so einer Situation kalt erwischt wird, kann das fatal sein.

Wie groß ist also die eigene Abhängigkeit von im Normalfall als „gegeben“ betrachteten Fremdleistungen, unmittelbar bei Ausfällen bzw. mit Blick auf Folgeschäden, wenn es situationsbedingt trotz aller Anstrengungen der „großen Versorger und Dienstleister“ nicht bei einer kurzen Störung bleibt?

Wer sich anschaut, was nach IT-SiG und Kritis-Verordnung getan werden soll, und dies auf seine eigene Situation „übersetzt“, bekommt in jedem Fall (Denk-)Hilfen für die eigene Praxis.

- Im Weiteren erwähnte Erläuterungs- und Hilfsdokumente mit Orientierungshilfen für den Umgang mit Inhalten des IT-Sicherheitsgesetzes enthalten Themenlisten (abzudeckende Themengebiete, konkrete Themen der technischen Informationssicherheit). Solche Listen kann man auch als „nicht-Kritis“-Umgebung nutzen, etwa um Schwerpunkte oder Struktur für eigene interne Prüfungen oder Anforderungspunkte zu größeren Planungen abzuleiten.

- Grundlegende Ansatzpunkte und zugehörige Hilfen im Sinne branchenspezifischer Schwerpunktsetzungen und -Maßnahmenwahl nach „Stand der Technik“ können auch von nicht-Kritis-Umgebungen als Vergleichsmöglichkeit und Ideenquelle verwendet werden.

  Das IT-SiG erlaubt und motiviert dabei „branchenspezifische“ Eigeninitiative.

  Wenn sich „Insider“ zusammenfinden, ihr spezielles Verständnis ihrer Branche und Techniknutzung sowie Anekdotenwissen aus dem „eigenen Alltag“ zusammenwerfen, ist dies eine große Chance. Kleinere Unternehmen einer Branche haben oft gar nicht die Kapazitäten, um eine solche (Selbst-)Analyse strukturiert und umfassend anzugehen. Getrieben durch IT-SiG und Kritis-Verordnung kann über Ergebnisdokumente, die sich zunächst an Betreiber von Infrastrukturen wenden, die Dienstleistungen mit kritischer Größenordnung bei Ausfällen stützen, ein wertvoller brancheninterner Wissenstransfer zustande kommen.

- Der Ansatz einer Fokussierung auf „Kritisches“ kann für jede Umgebungsgröße geschickt auf die eigene Situation übertragen werden.

  Insbesondere bei eigenen Überlegungen, wo und inwieweit besonderer Aufwand sinnvoll nach „Stand der Technik“ aussehen kann, erhält man (Argumentations-)Hilfe dafür, sich bei solchem erhöhtem Aufwand auf die wesentlichen Teile der eigenen Infrastruktur und IT-Ausstattung zu konzentrieren - man ersetze „kritische Dienstleistung“ in den entsprechenden Texten vom BSI oder in Branchendokumenten durch „im eigenen Hause Verfügbarkeitskritisches“. Dafür muss man dann im Sinne von „was passiert, wenn dies länger nicht zur Verfügung steht, wann wird ein solcher Zustand kritisch und warum“ denken.

IT-Sicherheitsgesetz und Kritis-Verordnung - eine „etwas andere“ Betrachtung

Versetzt man sich dabei versuchsweise in die Lage des Betreibers der Infrastruktur für eine kritische Versorgungsleistung, nur eben jetzt mit Blick auf die eigene Infrastruktur, fallen einem Fragestellungen und Szenarien ein, die man evtl. sonst übersehen hätte - und die doch im eigenen, kleineren Rahmen auch eine wichtige Rolle spielen können.

Natürlich kann und soll die nachfolgend punktuelle Beleuchtung von Arbeitspunkten und zugehörigen vorhandenen oder absehbaren Hilfsdokumenten einem Kritis-Betreiber, der am Anfang der notwendigen Aktivitäten steht, ein paar „Lesehilfen“ und erste Eindrücke bieten und so eine Einstiegshilfe sein. Die Wahl der im Folgenden beleuchteten Aspekte, Interpretationen und Denkanstöße ist aber bewusst so getroffen, dass es einer beliebigen „Organisation“ möglich sein soll, davon Nützliches mitzunehmen.

Also hier nun der Versuch eines auszugsweisen Blicks aus der Erfahrung und Praxis eines Umgangs mit „Kritikalität“ und für die Praxis verschiedener Umgebungsgrößen, anstelle einer „vollständigen Abhandlung der Pflichten in Kritis-Umgebungen“.

Unmittelbar betroffen vom IT-SiG sind natürlich Betreiber von Infrastrukturen, die im Sinne der erwähnten Kritis-Verordnung als „kritisch“ einzustufen sind. Diese haben nicht zuletzt gemäß Inhalten des IT-SiG besondere Nachweis- und Meldepflichten mit Blick auf (die Vermeidung) von Störungen.

Der Betreiber einer so identifizierbaren kritischen Infrastruktur hat gemäß den Inhalten des IT-SiG insbesondere mindestens alle zwei Jahre den Nachweis zu erbringen, dass er wie gefordert in angemessener Weise störungsvermeidende organisatorische und technische Vorkehrungen getroffen hat. Der Nachweis ist gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zu führen, das auf dieser Basis nötigenfalls Verbesserungen fordern kann.

Das ist ja nun kein neuer Gedanke: Störungen vermeiden bzw. frühzeitig erkennen und prompt melden und darauf reagieren, hierzu Vorkehrungen treffen und diese - auf Grundlage entsprechender Dokumentation und Prüfung der praktischen Umsetzung - nachweisen. Auch die formalen Details wie „Durchführung einer Prüfung, Erstellung eines Prüfberichts, Vorlage bei einer abschließend prüfenden Stelle“ - im Wirkbereich des IT-SiG: dem BSI - erkennt manch einer aus Revisionsvorgängen oder Zertifizierungen wieder.

Ein paar erste Überraschungen warten aber doch bei der Beschäftigung mit dem IT-SiG. Man kann sich z.B. ein entsprechendes Erläuterungsdokument des BSI, die **„Orientierungshilfe zu Nachweisen gemäß § 8a (3) BSIG“**, anschauen. Als interessanten Punkt stellt man darin fest: Es wird anders als oft üblich kein fester Prüfkatalog an Anforderungen im Detail oder eine verbindliche Liste von „Pflichtdokumenten“ angegeben, nach denen die Prüfung zu erfolgen hat, dass angemessene „störungsvermeidende Maßnahmen“ getroffen wurden.

Vielmehr werden verschiedene Wege zugelassen, strukturiert eine Selbstanalyse durchzuführen und nach entsprechender Maßnahmenwahl und Umsetzungen einen zugehörigen Nachweis zu führen und sich prüfen zu lassen:

- Es kann ein **„BranchenSpezifischer Sicherheitsstandard“ (B3S)** als Prüfbasis verwendet und angegeben werden.

  Solche branchenspezifischen Standards können von Betreibern kritischer Infrastrukturen oder ihren Fachverbänden selbst erarbeitet und dem BSI zur Eignungsprüfung vorgelegt werden. War eine solche Eignungsprüfung positiv, ist eine Prüfung und zugehörige Dokumentation entlang eines solchen Standards ein akzeptierter Ansatz und erspart einem die Erarbeitung und Abstimmung einer entsprechenden Prüfstruktur und Festlegung relevanter Themen als Vorbereitung.

  Wichtig und äußerst nützlich ist hier insbesondere der Branchenbezug solcher Hilfen, sobald sie zur Verfügung stehen.

  Allgemeine Kriterien- oder Anforderungskataloge haben in der Praxis den Nachteil, dass man sie auf die Besonderheiten der eigenen Umgebung „übersetzen“ muss. Spätestens da, wo man für sich selbst erhöhten Sicherheitsbedarf / erhöhtes Risiko festgestellt hat, muss man selbst entscheiden, wann gewählte Maßnahmen die besonderen Risiken vollständig und geeignet abdecken.

  Ein typischer Versuch hierzu in der Praxis ist, sich mit anderen in ähnlicher Lage zu vergleichen, z.B. eben Unternehmen aus der eigenen Branche. Ein branchenspezifischer Sicherheitsstandard nimmt dies ein stückweit vorweg und ist dabei - Zielgruppe Anbieter „kritischer Dienstleistungen“ - angesichts des möglichen enormen Wirkbereichs schon auf erhöhten Bedarf an Vermeidung bzw. zügiger Entschärfung schädlicher Vorfälle ausgelegt.

  Noch gibt es nur einen einzigen B3S, zu dem die Eignung vom BSI festgestellt wurde, zu einer Branche, die bereits Gegenstand der ersten Fassung der Kritis-Verordnung war (Branchenstandard IT-Sicherheit Wasser / Abwasser). Erste weitere B3S zu verschiedenen Branchen und Dienstleistungen/ Anlagen zu solchen Branchen sind aber in Arbeit (siehe z.B. entsprechende „Übersicht über Branchenspezifische Sicherheitsstandards (B3S)“ auf der Web-Site des BSI).

- Vorhandene, ausreichend aktuelle Prüfungen zu anderen Prüfschwerpunkten („einschlägige Standards“) können in der Prüfung nach § 8a (3) BSI-G berücksichtigt werden.

  Beispielsweise ist eine ISO-27001-Zertifizierung eine solche mögliche Grundlage. Derartige Zertifizierungen können unmittelbar als Teil-Nachweis dienen, es muss nur sichergestellt werden, dass die „kritische Infrastruktur“ durch den Geltungsbereich der Zertifizierung vollständig abgedeckt ist. (Sofern dies nicht der Fall ist, muss die „Lücke“ separat in den Prüfplan zur „Kritis-Prüfung“ aufgenommen werden.)

- Es werden keine Prüfthemen im Detail vorgegeben, sondern „Themenfelder“.

  Auch hier erfolgt ein klares Signal, dass die konkrete Situation und damit verbundene Risikolage, die sich aus der Art der über die betrachtete Infrastruktur erbrachten Dienstleistungen ergibt, im Fokus steht, kein „akademisch im Detail vollständiger, generischer Katalog“, der durchzukämpfen wäre: Für eine angemessene Prüfthemenliste im Detail wird wiederum auf einen branchenspezifischen B3S als mögliche Basis zur Orientierung verwiesen.

  Ist (noch) kein inhaltlich passender B3S verfügbar oder man hält die verfügbaren im eigenen Fall für nicht genau genug zutreffend, um die eigene Situation systematisch und ohne „Blindleistung“ anzugehen, kann man etwa die vom BSI herausgegebene „Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a (2) BSIG“ **(Orientierungshilfe B3S)** heranziehen und für den eigenen Fall selbst eine Themenliste festlegen. Die Orientierungshilfe B3S nennt mindestens abzudeckende Themenfelder, denen man „eigene“ spezifische Themen hinzufügen kann, mit denen man sich in seiner Umgebung gezielt mit Blick auf Störungsrisiken und Maßnahmenfindung auseinandergesetzt hat. (siehe Abbildung 2)

IT-Sicherheitsgesetz und Kritis-Verordnung - eine „etwas andere“ Betrachtung

Bezüglich des geeigneten Detaillierungsgrads der Behandlung eines Themengebiets wird z.B. auf ISO-Standards verwiesen. Wer bereits erwogen oder begonnen hat, mit Hilfe der Inhalte solcher Standards vorzugehen, ist auf einem richtigen Weg auch im Sinne der IT-SiG-Umsetzung und kann damit fortfahren, bei Erscheinen dann ergänzend einen passenden B3S als zusätzliche Hilfe verwenden.

Allgemein wird ein Detaillierungsgrad in Anlehnung an den in ISO 27002 ersichtlichen vorgesehen.

Bei Themen, die man für eine konkrete Infrastruktur als Schwerpunktthemen ansieht, wird auf entsprechend vertiefende ISO-Standards, technische Richtlinien u.Ä. verwiesen - der Detaillierungsgrad soll hier entsprechend der Wichtigkeit höher sein. Beispielhaft benannte, branchennahe vertiefende ISO-Standards sind ISO/IEC TR 27019 (Energiebranche) und ISO/IEC TR 27015 (Finanzdienstleistungen). Wer etwa danach vorgegangen ist und entsprechend dokumentiert hat, kann sich hierauf unmittelbar als Teil der Prüfbasis abstützen.

- Maßnahmenbereiche und „Stand der Technik“ werden als Basis für die Maßnahmenwahl genannt, statt allgemein verbindlich abzuarbeitender Detailkataloge an denkbaren Maßnahmen.

  Es werden im Anhang der B3S-Orientierungshilfe keine detaillierten Maßnahmenvorgaben als umfängliche und von jedem durchzuarbeitende kleinteilige Arbeitsliste, Prüf- oder Vorgabestruktur angegeben. Vielmehr wird im Anhang unter A3 „Technische Informationssicherheit“ eine Liste von Maßnahmenbereichen zur „technischen Informationssicherheit“ benannt, 10 unter „Informationssicherheit“, 12 unter „Ordnungsgemäßer IT-Betrieb mit Bezug zur Informationssicherheit“.

  Natürlich wird von einer Kritis-Umgebung erwartet, die IT-Ausstattung zu einer kritischen Dienstleistung/ der entsprechenden Anlage zu diesen Punkten so auszulegen und zu betreiben, dass mit Blick auf diese 22 Maßnahmenbereichen auch Überdurchschnittliches getan wird: Auch kleine Versäumnisse oder Lücken in der Wirksamkeit getroffener Maßnahmen können angesichts der vielen Nutznießer einer kritischen Dienstleistung schwere Folgen haben. Auch ist man aufgefordert, sich selbst gemäß Grundanforderung des IT-SiG über den „Stand der Technik“ zum jeweiligen Thema kundig zu machen. Man kann sich also nicht auf einer einmal getroffenen Maßnahmenwahl und -auslegung ungeprüft ausruhen.

  Die Konzentration auf 22 Maßnahmenbereiche als „Kern der Maßnahmenfindung“, je nach Anlagentyp und Sektor/ Art der Dienstleistung dann flexibel ergänzbar bzgl. Maßnahmen zu spezifisch zu beachtenden Themenbereichen, ist aber doch mal übersichtlich und eine klare Hilfe im Sinne einer „Konzentration auf das Wesentliche“. Was man als Input zum „Stand der Technik“ verwendet, kann man zudem je nach „Knackpunkten“ und Sektor gegebenenfalls „individuell“ bestimmen und die Schwerpunkte damit selbst entsprechend eigener Risikoeinschätzung wählen.

Insgesamt erkennt man den Ansatz, einen höheren Freiheitsgrad bzgl. Gestaltung des Nachweises und Setzung der Schwerpunkte von Maßnahmen im Sinne der Vermeidung von „Störungen“ zu geben und damit insbesondere zu ermöglichen, sich auf die konkrete Situation einer betrachteten Umgebung und deren „Knackpunkte“ zu konzentrieren.

Auch diese guten Ideen zur Vorgehensweise helfen aber nicht, wenn man sie nicht umsetzen kann. Kann also die Orientierungshilfe B3S doch nur für Kritis-Betreiber nützlich sein?
Gerade kleine und mittlere „Organisationen“ haben oft das Problem „eines unguten Gefühls“ zur eigenen Situation, aber eines Mangels an Ressourcen und eigenen Kenntnissen für eine baldige und umfassende Klärung und nötigenfalls Maßnahmenfindung zur Schließung bislang übersehener oder schleichend entstandener Lücken im Vergleich zum „Stand der Technik“ und zur heutigen (!) Bedeutung von (IT-)Ausstattung für Funktionieren und Handlungsfähigkeit der Umgebung. Wie kann man aber trotzdem feststellen, wo man dringend herangehen muss, nötigenfalls auch unter Hinzuziehung von Know-how und Kapazität Dritter? Wie kann man eine Reihenfolge in solche Aktivitäten bringen, dass das mit seiner Umgebungskenntnis zwingend einzubindende eigene Personal nicht überlastet wird?

Und hier schlummern **Nutzungsmöglichkeiten etwa der Orientierungshilfe B3S oder auf ihrer Basis entstandener B3S-Veröffentlichungen auch für nicht Kritis-Umgebungen.**

- Themengebiete gemäß Orientierungshilfe B3S für GAP-Analysen oder Priorisierung kommender „Optimierungsprojekte“ heranziehen

  Wer sich bei einem der nach B3S Orientierungshilfe, Abschnitt 5 abzudeckende Pflicht-Themenbereiche für Kritis-Umgebungen eingestehen muss, dazu gar nicht oder nur bruchstückhaft erklären zu können, wie er in seiner eigenen Umgebung mit dem Themenbereich umgeht und wer „zuständig“ bzw. „sachkundig“ ist, hat ein mögliches Problemfeld identifiziert.

  Hier sollte man zumindest Klarheit schaffen. Meist ergeben sich dabei erste gute Ideen, wo man mit überschau-

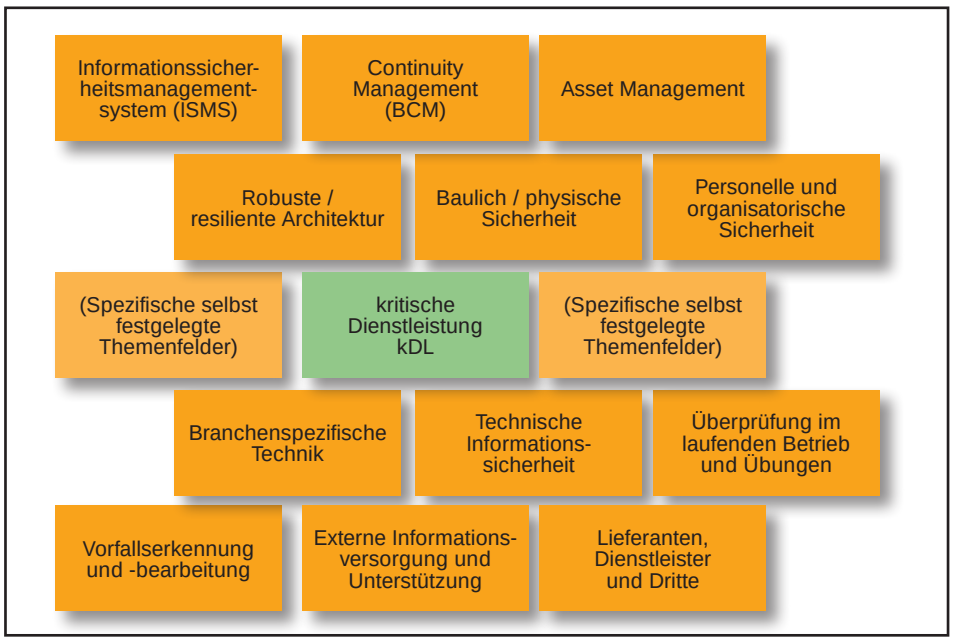


Abbildung 2: Themenfelder nach Orientierungshilfe B3S

barem Aufwand deutlich besser gerüstet sein kann als bisher.

- Liste der Maßnahmenbereiche im Anhang der Orientierungshilfe B3S als Basis für ein fokussiertes Analyseraster „Sicherheitsanalyse light“ verwenden

  Ja, es gibt umfassende Hilfen für Sicherheitsanalysen, zur Erarbeitung von Sicherheitskonzepten, zur strukturierten Vorgehensweise dabei im Rahmen eines „Sicherheitsmanagements“, und diese sind natürlich nicht durch eine „22 Punkte-Liste“ ersetzbar. Wer sich aber akut nicht die Kapazitäten bzw. das Know-how zutraut, um das Thema Sicherheit umfassend und mit durchgängiger Detailtiefe für sich zu analysieren, kann etwa die Liste von Maßnahmenbereichen gemäß Orientierungshilfe B3S als eine Art „Top 22“ interpretieren.

  Auch hier hilft dann eine Prüfung gemäß Fragen wie:

  Kann man aufzählen und zumindest kurz erklären, was man in diesen Maßnahmenbereichen tut?

  Kann man die zuständigen Personen und Wissensträger im eigenen Haus benennen?

  Können diese ohne zu zögern bestätigen, dass die derzeitigen Lösungswege und Lösungen noch aktuell sind? Wann wurde das zu einem Maßnahmenbereich der „Top 22“ zuletzt angeschaut/durchdacht bzw. sogar technisch aktualisiert (hier kann man z.B. das Zwei-Jahres-Nachweisintervall aus dem IT-SiG als groben Maßstab nehmen)?

  Wo immer man sich selbst zu einem Maßnahmenbereich gem. Orientierungshilfe B3S in diesem Sinne unsicher oder gar „erwischt“ fühlt, hat man einen Kandidaten für eingehendere Sichtung gefunden, zunächst in Sachen Grobklärung und Entscheidung auf (besonders dringenden) Handlungsbedarf, je nach Ergebnis dann bzgl. genauerer Maßnahmensichtung und Optimierung, mit oder ohne Unterstützung Dritter.

  (Bei der genaueren Betrachtung der eigenen Situation zu einem Maßnahmenbereich helfen dann wieder gängige strukturierte Vorgehensweisen, Standards und zugehörige Kataloge, Normen, technische Richtlinien usw., die man zu Rate gezogen hätte, wenn man sich eine umfassende Analyse zugetraut hätte. Man muss nicht improvisieren, hat aber über ein sinnvolles Vorgehen „vorgefiltert“.)

  Schon die erste Selbstbefragung zu einem wichtigen Maßnahmenbereich ist gemäß Praxiserfahrung des Autors dieses Artikels ein wichtiger erster Schritt.

  In vielen im Kundenauftrag durchgeführten „Audits“ und Checkups, begleiteten Projekten zu IT-Themen usw. war erkennbar, dass in der Kundenumgebung zunächst gar nicht klar war oder schleichend das Wissen wieder verloren gegangen war, ob man alle mittlerweile anerkannt wichtigen Themenbereiche abdeckte und dies zumindest für durchschnittlichen Sicherheitsbedarf nach „Stand der Technik“.

  Wer kann und will aber auf einem solchen „Kenntnisstand“ die Verantwortung dafür übernehmen, sich auf seine (IT-basierte) Arbeitsausstattung wenigstens zum Kerngeschäft so verlassen zu können, dass er nicht plötzlich in eine vermeidbare Situation geraten kann, in der er an für sich und andere wichtigen Stellen seinen Aufgaben und Pflichten nicht mehr nachkommen kann?

- Maßnahmenvorschläge aus B3S-Veröffentlichungen als Ideengeber für eigene Modernisierungsaktivitäten bzw. Analysen nutzen, ob man eine bislang übersehene gefährliche Schutz- oder Vorsorgelücke gezielt schließen kann

  Man muss nicht selbst in jedes besondere Risikofeld der eigenen Branche oder des eigenen Anlagentyps schon hineingeraten sein, und dies ist ja auch nicht wünschenswert. Wenn aber in einer B3S-Veröffentlichung auf bestimmte Gefahren hingewiesen und mit entsprechenden Maßnahmenhinweisen reagiert wird, hat da offenbar jemand eigene unangenehme Erfahrungen in das B3S-Dokument einfließen lassen oder ein erst in letzter Zeit, etwa durch Änderungen beim Technikeinsatz akut gewordenes Problemfeld herausgearbeitet.

  Hier kann man vom Wissen anderer profitieren, entweder durch Feststellung, dass man selbst nicht wesentlich betroffen ist, oder dass man neue Maßnahmen kennenlernt, die man als Neuerung für sich sinnvoll findet und in die Planung für anstehende Modernisierungen oder Verbesserungen aufnimmt.

Natürlich kann auch ein Kritis-Betreiber oder zukünftiger Kritis-Kandidat so vorgehen, der nicht auf einen genau auf seinen Anlagen- oder Dienstleistungstyp passenden B3S-Standard warten kann bzw. will, oder aber der rechtzeitig eine Reihenfolgenfestlegung zur Erkennung und Schließung von Lücken oder Schwächen bei Maßnahmen bzw. Dokumentation treffen will, um nicht in einer ersten Pflichtprüfung im Sinne des IT-SiG wegen Zeitmangels bei Maßnahmenänderungen „durchzufallen“.

Und übrigens - die beschriebenen Vorgehensweisen und Fragen zur ersten groben Standortbestimmung haben sich in der Projekt- und Beratungspraxis des Autors des vorliegenden Artikels für Vorsortierungen in Ist-Aufnahmephasen bewährt, wenn auch bislang ohne Bezugnahme zum IT-SiG und zugehörigen Veröffentlichungen wie der Orientierungshilfe B3S. Wir sind also mitten in der Praxis angekommen, mit einer zusätzlichen Quelle für Arbeits- und Denkhilfen ...

Damit könnte es für jetzt genug sein, und man könnte erst einmal die nächste Zeit mit ersten Erfahrungen aus der Anwendung von IT-SiG und (Hilfen zur) Kritis-Verordnung abwarten und beobachten.

Eine wesentlicher Aspekt, der im Sinne der Denk- und Zielrichtung des IT-SiG zu sehen ist, darf aber nicht fehlen: der individuelle, auf die eigene Situation und Risikobereitschaft zugeschnittene Umgang mit dem Begriff „kritisch“ - bezogen auf kritische Ausnahmesituationen.

Jeder berücksichtigt bei Entscheidungen bzgl. Einführung oder Modernisierung von (Teilen der) IT-Ausstattung das Thema „Verfügbarkeit“, bei entsprechend eingeschätzter Abhängigkeit von funktionierender IT auch im Sinne von „Hochverfügbarkeit“. Natürlich sollte man dabei (auch) den Fall vor Augen haben, dass trotz umfangreicher präventiver Vorkehrungen ein größerer „Störfall“ eintreten könnte und man auch in solchen Situationen arbeits- und handlungsfähig bleiben will. Genau in dieser Richtung kann man das IT-SiG und die Kritis-Thematik auch und insbesondere „lesen“ - dabei lernen und einüben, „zusätzliche Denkmuster“ zu berücksichtigen.

„Kritisch = existenziell wichtig“ - was wäre wenn doch ...? Ein wichtiger Gedanke!

Man betrachte folgende Situation:
Die Pflichtaufgaben „Vermeidung unnötiger Ausfallrisiken“ und „Prävention von Totalausfällen mit Maßnahmen nach Stand der Technik“ sind im Rahmen des für eine betrachtete Organisation gemäß ihrem Kerngeschäft, etwa durch sie erbrachter (für das Gemeinwohl kritischer) Dienstleistungen und zugehöriger Anlagen und IT-Ausstattung ausgereizt. Man könnte denken, damit sei man mit Blick auf Verfügbarkeit wichtiger IT fertig.

IT-Sicherheitsgesetz und Kritis-Verordnung - eine „etwas andere“ Betrachtung

Aber halt - angenommen, trotz aller getroffenen Vorkehrungen, eigenen bzw. über gezielte Wahl von Dienstleistern und vertraglicher Absicherung zur Dienstleistungs-Verfügbarkeit, kommt es zu einer massiven Störung, die einen Totalausfall darstellt oder diesem nahe kommt. Ausgeschlossen ist das nicht. Betreiber von Kritis-Infrastrukturen müssen sich gemäß Pflichtthemen auch mit solchen Ausnahmesituationen beschäftigen (BCM als Pflichthema). Mindestens wer sehr stark von einer bestimmten Ausstattung abhängig ist und nicht verkraften könnte, eine längere Zeit seine Tätigkeiten und Leistungen einzustellen, sollte es dringend ebenfalls tun, Kritis-Betreiber oder nicht!

Problematisch:
Da man das Thema Ausfallsicherheit präventiv eigentlich schon ausgeschöpft hat, ist die Frage, was denn jetzt noch möglich ist. Was immer einem noch einfällt, wird entweder aufwändig und teuer sein, oder es werden eigentlich schon getroffene Einschätzungen, alles richtig gemacht und bedacht zu haben, wieder in Frage gestellt. Schon aus Machbarkeitsgründen muss man da maßhalten und sich auf wirklich „schwerwiegende oder existenzbedrohende“ Folgeschäden für eine betrachtete Umgebung konzentrieren.

Auch dies ist eigentlich kein neuer Analyseansatz, Folgeschadenanalyse oder Business Impact Analyse sind entsprechende Stichworte. Auch hier findet man bereits existente Veröffentlichungen zur systematischen Vorgehensweise, als Teilkapitel in Dokumenten zur strukturierten Vorgehensweise bei Optimierungen zum Business Continuity Management, z.B. spezifischen Standards wie EN ISO 22301 (Business Continuity Management). Der Zusammenhang zu IT-SiG und zur aktiven Beschäftigung mit diesem ist unmittelbar gegeben. Nicht umsonst ist etwa der Titel der deutschen Fassung DIN EN ISO 22301 „Sicherheit und Schutz des Gemeinwesens“ - genau in diesem Sinne will das IT-SiG in Verbindung mit der Kritis-Verordnung schwerpunktmäßig wirken. Aber auch hier kann die umfassende Arbeit gemäß einem derartigen Standard abschrecken bzw. zunächst überfordern.

Wer die Feinheiten des IT-SIG zu verstehen bemüht ist und dabei genau liest bzw. über genaue Deutungen für die Praxis nachdenkt, kann als Erkenntnisse weiter verwenden:

- „kritische Dienstleistungen“ und zugehörige Anlagen stehen im Fokus der Kritis-Verordnung, nicht die Gesamtausstattung einer Organisation, die „Dienstleistungen“ erbringt

  Typisch wird es sich um das Kerngeschäft einer betrachteten Organisation handeln. Hierauf kann und sollte man sich also konzentrieren, wenn man sich mit „kritisch“ und Ausnahmesituationen beschäftigt, schon wegen der angesprochenen Machbarkeit von Zusatzmaßnahmen oder nochmaliger Revision schon getroffener strategischer Entscheidungen zu hoher Verfügbarkeit.

- Zielstellung ist genau genommen die möglichst durchgängige Verfügbarkeit einer „kritischen Dienstleistung“

  Nicht die Verfügbarkeit von IT bzw. einer IT-basierenden Anlage ist der Aufhänger, sondern die Leistung einer Umgebung. Dies kann je nach Sektor / Branche unmittelbar mit IT-Verfügbarkeit gleichzusetzen sein, muss es aber nicht. Soweit zeitweilig zumindest bedingt auf bestimmte IT-Ausstattung bzw. auf eine bestimmte, im Normalzustand erfolgende Nutzungsweise von IT verzichtet werden kann, ohne dass die „Dienstleistung“ zum Erliegen kommt, ist das Ziel des Schutzes dieser Dienstleistung nicht völlig verfehlt.

- Meldepflichten zu besonderen Vorfällen - Voraussetzung: Kommunikationsfähigkeit!

  Wie kommen Erkenntnisse über eine akut drohende oder eintretende Störung an die richtigen Stellen? Wie kann man eingegangene oder über Gesetze und sonstige Auflagen maßgebliche Verpflichtungen zur Information Dritter („Melde- und Informationspflichten“) erfüllen, wenn eine Störung (auch) die im Normalfall genutzten Lösungen zur Kommunikation betrifft? Wie will man koordiniert mit einer solchen Lage so umgehen, dass möglichst geringer Schaden entsteht und Schritte eingeleitet sowie erfolgreich zu Ende gebracht werden, die für eine Rückkehr zum Normalzustand im akuten Fall passend und notwendig sind?

  Kommunikationsfähigkeit sicherstellen ist also nicht nur (aber natürlich insbesondere auch) für Kritis-Betreiber notwendig, die ihren Meldepflichten gemäß IT-SiG nachkommen müssen. Es ist ein Maßnahmenziel, das in der konkreten Praxis wesentlich dazu beiträgt, dass andere Maßnahmen zum schadensminimierenden Umgang mit trotz allem eingetretenen Problem- und Störungssituationen wie geplant wirken können.

Legt man diese unter anderem mit dem IT-SiG einhergehenden Gesichtspunkte den eigenen Überlegungen zugrunde, ob man für „den Störungsfall“, der trotz Prävention ausnahmsweise eingetreten ist, gut gerüstet ist oder etwas Wichtiges übersehen hat, so stellt man sich ein weiteres Mal „richtige“ Fragen, unabhängig vom Status eines Kritis-Betreibers. Wichtige Fragen dieser Art sind

IT-Sicherheitsgesetz und Kritis-Verordnung - eine „etwas andere“ Betrachtung

- Was / wer gehört in meiner Umgebung „zum Kerngeschäft“, das nicht zum Erliegen kommen sollte? Welche Aufgaben müssen „in jedem Fall“ wahrgenommen werden können?

  (Bestimmung „kritischer Prozesse und Bereiche, bzw. unterstützender Vorgänge und Leistungen, die für derartige Prozesse und Bereich besonders wichtig sind“)

- Was muss dazu bzw. zur Vermeidung von Schäden an Personen und Ausstattung möglichst zur Verfügung stehen, funktionieren, ...?

  Inwieweit sind dafür Informationen bzw. Informationsflüsse dringend und „jederzeit“ erforderlich?

  (im Fokus: kritische „Ressourcen“, inklusive Informationen und IT-Ausstattung, die für deren Nutzbarkeit besonders wichtig sind)

- Wie will oder muss ich insbesondere reagieren können, wenn eine Situation eingetreten ist, in der kritische Ressourcen nicht geeignet zugänglich sind bzw. dieses unmittelbar droht? Was wird dazu benötigt und sollte nicht auch vollständig ausfallen bzw. unzugänglich sein?

  Wie kann man zugehörige Ausfälle oder zumindest massive Probleme mit solcher Ausstattung zumindest so „überbrücken“, dass der (Folge-)Schaden möglichst gering bleibt, also kritische Prozesse (wenn überhaupt) möglichst kurz zum Stillstand kommen und die Rückkehr zum Normalzustand nicht unnötig schwierig ist?

  (Fokus hier: schadensbegrenzende Sofortmaßnahmen, Überbrückungslösungen, Ausstattung für schnellen Wiederanlauf und erfolgreiche Rückkehr zum Normalzustand über vorbereitete oder ausnahmsweise kurzfristig zu beschließende Maßnahmen)

Auch dies sind keine Gesichts- und Klärungspunkte, die mit dem IT-SiG erfunden wurden. Wie vorgeführt wurde, kann man aber (auch) durch Beschäftigung mit Intentionen und Sichtweisen zum IT-SiG zu solchen Punkten gelangen.

Beschäftigung mit dem IT-SiG und der Begriff „kritisch“ als Ausgangspunkt können also helfen, sich nicht zu einseitig auf Prävention zu verlassen, sondern auch den Fall der „Ausnahmesituation“ konsequenter zu Ende zu denken, und dies „individuell und bedarfsgerecht“ für sich und die eigene konkrete Umgebung.

Ergebnisse können dabei je nach Umgebung völlig unterschiedlich ausfallen, wie die nachfolgenden „Streiflichter“ aus der Praxis des Autors dieses Artikels kurz vorführen sollen:

- In einem Fall wurde die Ausstattung mit Mobiltelefonen als ausreichende Basis für Kommunikationsfähigkeit in Sondersituationen eingeschätzt. Die gezielte Beschäftigung mit der Nutzbarkeit solcher Ausstattung im Ernstfall führte im Detail aber zu ergänzenden Überlegungen in Richtung eines „Notfallpakets“ zur Ausstattung eines Krisenstabs, unter anderem mit Netzteilen für eingesetzte Handy-Typen sowie Mehrfachsteckdosen und Verlängerungskabeln zum Anschluss solcher Dosen.

  Man wollte sichergehen, bei länger notwendiger Aktivität eines solchen Krisenstabs tatsächlich sinnvoll ohne permanent mit Strom versorgte „Tischtelefone“ auszukommen. Man wollte sich dabei nicht darauf verlassen, dass jeder im akuten Störungsfall stets entsprechende Ausstattung vollständig bei sich führt und der genutzte Raum ideale Voraussetzungen bietet.

- In einem anderen Fall wurde ergänzend zur anstehenden Einführung einer modernen, im Normalfall für alle nutzbaren Telefonie- und Unified Communications-Gesamtlösung zusätzlich beschlossen, für Kommunikationsfähigkeit bestimmter „kritischer Nutzerkreise“ auch bei größeren Störungsfällen ein ganzes Bündel von Maßnahmen zu schnüren.

  Dieses reichte von gezielter Ausstattung mit Endgeräten, die wahlweise und möglichst einfach LAN- oder WLAN-basiert (auch) zum Telefonieren verwendet werden konnten bis zur Vorbereitung und Bereitstellung einer kleinen „Notfallanlage“ für IP-basierte Telefonie.

- Im Falle verschiedener Krankenhäuser wurde unter anderem das Thema der Verfügbarkeit von Anwendungen und Daten im Rechenzentrum gezielt mit Blick auf Ausnahmesituationen betrachtet. Ein besonders betrachteter Aspekt war dabei die Abhängigkeit von der netzbasierten Erreichbarkeit des RZ.

  Die Frage, ob und welche Patientendaten möglichst in keinem Fall unzugänglich sein sollten, führte zur Betrachtung von Szenarien wie „Versorgung von Patienten auch bei längerem Ausfall der RZ-Erreichbarkeit“ bis zu „möglichst mit zu übergebende Patientendaten im Falle der Notwendigkeit, wegen Ausnahmesituationen auf dem eigenen Campus Patienten in ein anderes Krankenhaus zu verlegen“.

  In der Folge wurden sehr grundlegende Optionen zur Verfügbarkeitssicherung (!) noch einmal kritisch und im Ergebnis teilweise anders bewertet.

  So wurde die Sinnfälligkeit einer vollständigen Auslagerung der redundanten RZ-Infrastrukturen zu einem

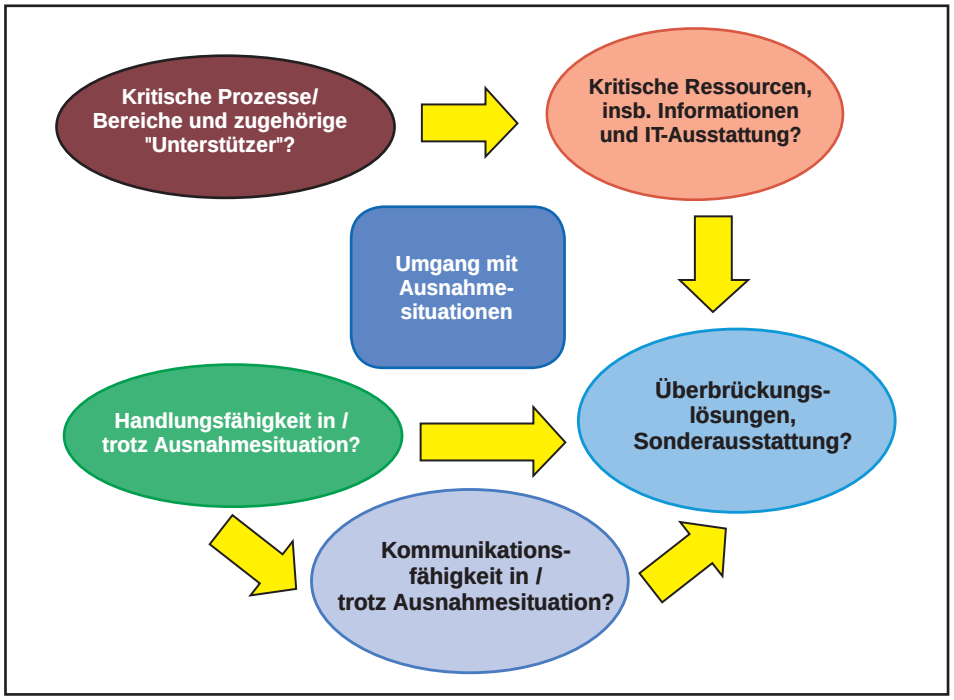


Abbildung 3: Wichtige Aspekte für Schadensbegrenzung im „Ausnahmezustand“

auf Hochverfügbarkeit spezialisierten Dienstleister in einem Fall abgewertet. In einem anderen Fall wurde entschieden, Möglichkeiten eines begrenzten Arbeitens mit lokalen Kopien akuter Patientendaten in bestimmten Krankenhausbereichen näher zu betrachten, trotz der damit verbundenen Problematik des Aufwands zu einer angemessenen Absicherung solcher Datenhaltung „nahe beim Anwender“.

Alle gewählten Beispiele haben bewusst mindestens bedingt mit Vernetzung und deren Nutzbarkeit zu tun. Alle dabei angerissenen besonderen Betrachtungsdetails und Maßnahmenoptionen können je nach Umgebung zunächst oder endgültig als überzogen, nicht machbar oder wegen damit verbundener erhöhter Risiken an anderer Stelle als untauglich eingeschätzt werden. In den konkreten Projekten und zugehörigen Umgebungen wurden sie aber wegen der jeweiligen Ausgangslage und Verpflichtungen in Ausnahmesituationen bewusst weiter verfolgt.

Die letztlich geschnürten Maßnahmenbündel und Detailentscheidungen waren dabei unterschiedlich, und dies zulässiger Weise: logistische Rahmenbedingungen, Machbarkeit mit Blick auf eigenen Kapazitäten und Kosten von Maßnahmenoptionen, die Größen der evtl. „besonders“ auch im Ausnahmefall handlungsfähig zu haltender Personenkreise unterschieden sich deutlich.

Das bewusste Finden eines „eigenen“, auf die individuelle Situation zugeschnittenen Wegs zum Umgang mit „Kritikalität“, wie es etwa vom IT-SiG insbesondere für Kritis-Umgebungen vorgesehen wird, ist also wichtig und richtig. Die Bedeutung wird mit immer weiter zunehmender Vernetzung und hierdurch verstärkten Abhängigkeiten von Infrastrukturen und „Anlagen“ weiter zunehmen. Die Beschäftigung mit den vorgeführten Sichtweisen lohnt sich für jeden - man muss über Hilfsmittel sowie geschickte „Selbstbefragung“ und Vorgehensweise allerdings das richtige Maß an Aufwand und „Risikoinkaufnahme“ finden. IT-SiG/ Kritis-Verordnung mit aus deren Umsetzung resultierenden Erfahrungen und Arbeitshilfen können und sollten dabei zukünftig in der Praxis nutzbringend berücksichtigt werden.

Aktuelle Sonderveranstaltungen

ComConsult RZ-Tage

Netzwerk-Architekturen der Zukunft im RZ 11.12.17 in Köln
Integration von Cloud-Lösungen in die RZ-Infrastruktur 12.12.17 in Köln

Die ComConsult Akademie veranstaltet am 11.12. und am 12.12.2017 ihre Sonderveranstaltungen "ComConsult RZ-Tage – Netzwerk-Architekturen der Zukunft im RZ" und "ComConsult RZ-Tage – Integration von Cloud-Lösungen in die RZ-Infrastruktur" in Köln.

Das Mega-Thema für alle Rechenzentren ist “One-Stop-Provisioning”: wie können die Infrastrukturen für neue Anwendungen durch Parametrierung mittels Orchestrierungs-Konsole schnell zur Verfügung gestellt werden? Projektzeiten sollen so aus dem Bereich von Jahren auf wenige Wochen verkürzt werden.

Dies erfordert:

- Infrastrukturen müssen ausreichende Kapazität haben, die Architektur muss auf eine schnelle Erweiterung ausgelegt sein
- Netzwerk-, Server- und Speicher-Kapazitäten müssen bei Bedarf exklusiv einer Anwendung zugewiesen werden können
- Eine Anwendung soll nur die ihr zugeordneten Ressourcen sehen und nicht auf die Ressourcen anderer Anwendungen zugreifen können
- RZ-Leistungen müssen gezielt um Funktionen aus der Cloud ergänzt werden, die dann wiederum in eine Gesamtarchitektur integriert werden
- Dies führt zu gravierenden Änderungen in der Planung und Bereitstellung von Infrastrukturen.

Wir analysieren auf dieser Top-Veranstaltung zentrale Fragen, die die Zukunft vieler Rechenzentren bestimmen werden. Die Anzahl der Teilnehmer ist aus logistischen Gründen begrenzt, wir empfehlen deshalb dringend eine frühzeitige Buchung. Die Tage sind einzeln und zusammen zum Paketpreis buchbar.

Aus diesem Grund basiert der erste Tag dieser Veranstaltung auf folgenden Kernfragen:

- Was bedeutet Layer 2 im Hypervisor? Welchen Stellenwert hat Layer 2 in Zukunft generell?
- Wie wollen bzw. müssen wir Layer-2-Lösungen im Hypervisor in Zukunft gestalten und segmentieren?
- Brauchen wir Underlay-Overlay-Architekturen? Warum überhaupt? Wenn ja, welche Konsequenzen hat das?
- Wo steht OSPF? Müssen wir es ersetzen? Wenn ja, wann und womit?
- Wie erklärt sich die zunehmende Nutzung von BGP in diesem Umfeld? Was wird darunter im Detail verstanden?
- Brauchen wir eine Control-Plane für Overlays? Wenn ja, sollte diese zentral oder dezentral sein? Wird sie unvermeidbar mit dem Hypervisor verbunden sein? Ist dies das Aus für OSPF oder gibt es einen sinnvollen Parallelbetrieb?
- Entsteht hier eine neue Form der Herstellerabhängigkeit oder gibt es eine standardbasierende Lösung? Wie stellt sich der Markt generell diesem Thema?

Am zweiten Tag beschäftigen wir un mit folgenden zentralen Fragen:

- Was passiert in der Cloud überhaupt und was leisten Plattformen wie AWS oder Microsoft Azure für ein Unternehmen? Gibt es da einen Mehrwert, der lokal nicht erbracht werden kann? Welche Bausteine bieten sich wann an?
- Office 365 wird für viele Unternehmen zu einem unvermeidbaren Cloud-Baustein werden, aber wie kann es sinnvoll integriert werden und was von Office 365 ist überhaupt gut genug, um integriert zu werden?
- Wie findet die technische Anbindung statt und vor allem wie kann das gestaltet werden, was auf der Seite der Infrastruktur in der Cloud gebraucht wird? Wie macht man zum Beispiel eine Netzwerkplanung in der Cloud und in Verbindung mit den Cloud-Netzwerken?
- Die Integration von Cloud-Bausteinen ist untrennbar verbunden mit einer Öffnung zur Cloud. Bei allen Vorteilen generiert dies erhebliche Anforderungen an Sicherheit. Die sind lösbar, aber sie sind auch neu und erfordern ein Umdenken in der technischen Gestaltung von Sicherheit. Eine Schlüsselfrage ist: Muss Sicherheit für die Cloud nicht aus der Cloud kommen?

Wenn Sie beide Veranstaltungen der "ComConsult RZ-Tage" buchen, bieten wir Ihnen einen Rabatt von 390,-- € an.

Sie zahlen für beide dann nur 1.790,-- € statt regulär 2.180,-- €.

Anmeldung an kundenservice@comconsult-research.de

ComConsult RZ-Tage

Ich buche die Veranstaltung(en)
ComConsult RZ-Tage in Köln

☐ 11.12.2017 - 1.090,-- € netto
☐ 12.12.2017 - 1.090,-- € netto
☐ 11. - 12.12.2017 - 1.790,-- € 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 RZ-Tage

Montag 11.12.2017 - Netzwerk-Architekturen der Zukunft im RZ

9:30 Uhr

Neue Hardware: Voraussetzung für neue Lösungen in RZ-Netzen

- Anforderungen an moderne Rechenzentren: Skalierbarkeit, Flexibilität, Universalität
- Evolution der Hardware: CPU, GPU, Speicher
- Hardware Protokoll-Unterstützung der aktuellen 100 GbE Switch ASICs mit 25/50 GbE Unterverteilung
- Möglichkeiten, Entwicklung und Verfügbarkeit von 200/400 GbE und Silicon Photonics

Dr. Franz-Joachim Kauffels, Technologie-Analyst

10:30 Uhr Kaffeepause

11:00 Uhr

Ist Layer 2 im DC noch zeitgemäß? Netzdesigns im Vergleich

- Neue Anwendungen erfordern ein neues Netzwerkdesign (Probleme des Spanningtree Protokolls, LACP – eine beschränkte Alternative)
- Layer 2 Design oder auch Switchfabric (TRILL; SPB, MC-LAG, SDN Einbindung)
- Layer 3 Design – Einführung (Hyper Scale DC von Microsoft und Facebook, Use Cases, Design Vorgaben)
- Layer 4 Design – Was ist das? (Multipath TCP, QUICK)

Markus Geller, ComConsult Research GmbH

12:00 Uhr Mittagspause

13:00 Uhr

EGP statt IGP: das Ende von OSPF? Wo ist die investitionssichere Zukunft? Welches Routing Protokoll im DC?

- Wie funktioniert modernes IP Routing? (Link State, Distance Vector, Path Vector)
- Topologie bekannt und nun?
  - Welche Auswirkungen ergeben sich aus der Kenntnis der Topologie?
- BGP statt OSPF: Die Gründe (Grenzen des Area Designs, Update Verhalten, Virtuelle Links)
- BGP Gestaltung und Aufbau (Pfad Auswahl im DC, SDN Controller)
- iBGP vs. eBGP (ECMP, BFD)
- Spine-Leaf, Scale-Out: Alles klar? (Skalierung, Multi Vendor Support)

Markus Geller, ComConsult Research GmbH

14:00 Uhr

Von der Server-Virtualisierung zur Private Cloud: Die Bedeutung des Software-defined Datacenters

- Server-Virtualisierung
- Storage-Virtualiserung
- Overlays und Software-defined Networking (SDN)
- Integration von Sicherheitskonzepten (Mikrosegmentierung)

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

15:00 Uhr Kaffeepause

15:15 Uhr

Overlays und das Problem mit dem Control-Layer

- Motivation: Warum Overlays?
  - Anforderungen an moderne RZ-Netzdesigns
  - Einflussfaktoren: Storage-Anbindung, Cloud-Anbindung, Redundanz
  - Vorteil und Nachteile typischer Designs
  - Hypervisor vs. Netzwerkkomponente: Wo enden die Overlays?
- Übersicht gängiger Overlay-Technologien
  - Welche Tunnelprotokolle stehen zur Verfügung?
  - MPLS / PBB / TRILL / VXLAN / NVGRE / Geneve
  - Wo liegen die Unterschiede und wie sieht deren Zukunft aus?
- Das Problem mit dem Control-Layer
  - Brauchen wir eine übergreifende Control-Plane?
  - Controllerbasierende vs. Data-Plane-basierende Lösungen
  - IS-IS, SDN, Multiprotokoll BGP
  - Auf dem Weg zur einheitlichen Control Plane?
- Lösungen im Vergleich:
  - SPBM (802.1Qaq), NSX und VXLAN, EVPN VXLAN
  - Eigenschaften, Protokolle, Leistungsmerkmale
  - Anwendungsfälle

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

ab 18:00 Uhr Happy Hour

Dienstag 12.12.2017 - Integration von Cloud-Lösungen in die RZ-Infrastruktur

9:30 Uhr

Nutzung von Public Clouds zur Unterstützung von Geschäftsprozessen

- Ziele und Erwartungen
- Was leisten Cloud-Dienste heute? Wo steht der Markt?
- Ausgewählte Einsatzszenarien

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

11:00 Uhr

AWS vs Azure: warum Cloud? Welche Cloud? Dienste, Preise, Konzepte in der Analyse

- Komponenten der Cloud: Dienste, Server, Regionen, Netzwerke
- Anbindung des RZ an die Clouds von Microsoft und Amazon: VPN, Direct Connect, ExpressRoute, Statisch oder BGP
- Netzwerkgestaltung in und mit der Cloud
- Projekterfahrungen aus Migration von ComConsult-Study.tv in die Cloud

Markus Schaub, ComConsult-Study.tv

11:30 Uhr Kaffeepause

11:45 Uhr

Microsoft Office 365: Erfolgreiche Nutzung und Anforderungen an die IT

- Software aus der Cloud
  - Ziele und Erwartungen
  - Warum Cloud-Anwendungen „anders“ sind
  - Beispiele
- Assessment von Office 365:
  - Nutzung der Office-365-Suite: Wer – Was – Wie
  - Lizenzmodelle
  - Anbindung an die Microsoft Cloud: Single Tenant vs. Multiple Tenants
  - Integration des Active Directory
  - Single Sign On
  - Anforderungen an die IT-Infrastruktur
  - WAN-Anbindung: Bandbreite, Laufzeit, Übertragungsqualität
  - Tools zur Prüfung der Netzqualität
  - Netzdesigns zur Anbindung von Niederlassungen
  - User Experience
  - Tuning-Möglichkeiten
  - Erfahrungen aus Kundenprojekten

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

13:15 Uhr Mittagspause

14:15 Uhr

Informationssicherheit in und aus der Cloud

- Herausforderung sicheres Cloud Computing
- Integration Private Cloud und Provider Cloud
- IAM und Data Loss Prevention für die sichere Nutzung von Cloud-Diensten
- Verschlüsselung von Daten in der Cloud: Möglichkeiten und Grenzen
- Standardisierte und zertifizierte Cloud-Sicherheit
- Virtuelle Sicherheits-Gateways und virtuelle Internet DMZ in der Cloud: Mehr als ein Trend!
- Rolle der Cloud bei der Abwehr von zielgerichteten Angriffen und von Distributed Denial of Service (DDoS)

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

15:45 Uhr

IT-Recht und die Cloud

- Vertragsrecht in der Cloud
  - Grundlagen und typologische Einordnung
  - Do´s und Don´ts in Cloudverträgen
- Datenschutz in der Cloud
  - Datenschutzrechtliche Ausgangslage (neues Recht vs. altes Recht)
  - Gestaltungstipps für sicheres Cloud Computing
- Informationssicherheit in der Cloud
  - Sicherheitslage in der Cloud
  - Rechtliche Anforderungen an die IT-Sicherheit beim Cloud Computing

Dr. Jan Byok, Bird & Bird LLP

16:30 Uhr Ende der Veranstaltung

Der Veranstalter behält sich Änderungen im Programm vor

Standpunkt

Im Fokus der Angreifer: Administration der IT-Infrastruktur

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

Die IT hat ein grundlegendes, eingebautes und natürlich seit Jahrzehnten bekanntes Dilemma: Ohne mächtige Administratoren und ebenso mächtige Werkzeuge gibt es einerseits keine funktionstüchtige IT, andererseits können eben diese Administratoren und Werkzeuge innerhalb von kürzester Zeit die komplette IT lahmlegen oder kritische Daten kompromittieren und einen erheblichen Schaden für die betroffene Institution verursachen. Vielleicht erinnern Sie sich an den Film Jurassic Park von 1993. Hier war es ein IT-Administrator, der die IT sabotierte, um Dinosaurier-Embryonen zu stehlen, und dabei als Kollateralschaden letztendlich die gefährlichen Dinosaurier frei gelassen hat [1]. Diese Problematik ist bis heute aktuell. Im Frühjahr dieses Jahres löschte ein ehemaliger Administrator eines niederländischen Providers „alle Kundendaten und die meisten Server“ – ein Desaster [2].

Es ist klar, dass eine wesentliche Maßnahme der Informationssicherheit die angemessene Authentisierung administrativer Zugriffe in Verbindung mit einem strengen Rollen- und Berechtigungskonzept, das zielgerichtet nur die für gewisse Tätigkeiten notwendigen Autorisierungen zulässt, ist. Bei einem Innentäter wie oben dargestellt, hilft eine Authentisierung allerdings nicht unmittelbar, jedoch kann ein feingranulares Rollen- und Berechtigungskonzept die Angriffsfläche deutlich reduzieren. Die funktioniert aber nur dann, wenn privilegierte Berechtigungen bei Änderungen der Rollenzugehörigkeit von Mitarbeitern auch schnell genug entzogen werden. Außerdem können sich Administratoren auch Hintertüren schaffen, die vielleicht zunächst die tägliche Arbeit erleichtern, aber nach Ausscheiden aus der Institution ein erhebliches Risiko darstellen können.

Erschwerend kommt hinzu, dass durch unzureichend abgesicherte Administrationsschnittstellen ein unberechtigter administrativer Zugriff mehr oder weniger leicht möglich ist. Ein plakatives Beispiel hierzu hat der Hersteller Fortinet vor wenigen Tagen geliefert: Der FortiWeb Manager bietet eine Webanwendung zur Administration der Fortinet Web Application Firewall (WAF) an.

Der CERT-Bund hat hierzu am 23.11.2017 gemeldet, dass ein Angreifer „eine Schwachstelle in FortiWeb Manager durch die Eingabe einer beliebigen Zeichenkette für das Passwort des Administrators ausnutzen, um Administratorrechte zu erlangen und dadurch alle darüber verwalteten FortiWeb Appliances kompromittieren“ kann [3]. Es ist natürlich erschreckend, dass eine Sicherheitskomponente eines etablierten Herstellers auf eine solch triviale Weise gekapert werden konnte (was natürlich auch die Qualität der Softwareentwicklung des Herstellers in Frage stellt). Solche Schwachstellen kommen aber leider immer wieder vor.

Zusätzlich haben wir das Problem, dass wir unsichere Protokolle, die für Angriffe ausgenutzt werden können, oft länger verwenden müssen, als es uns lieb ist. Das klassische Beispiel ist hier das Simple Network Management Protocol in der Version 2 (SNMPv2), das sich für das Monitoring der IT immer noch hartnäckig hält.

Ist die Absicherung administrativer Zugriffe nun eine Mission Impossible? Nein! Durch eine systematische Berücksichtigung von Administration, Monitoring und Protokollierung in den Sicherheitskonzepten und im Schwachstellenmanagement kann ein umfassender, ganzheitlicher Maßnahmenkatalog den Gefährdungen entgegen wirken. Ein Beispiel eines solchen Maßnahmenkatalogs liefert das im Oktober dieses Jahres als Final Draft veröffentlichte BSI IT-Grundschutzkompendium [4] mit dem Baustein NET.1.2 Netzmanagement. Hier werden auch Anforderungen an die Protokollierung von administrativen Zugriffen gestellt, die von der Protokollierung von Anmeldeversuchen, über die Protokollierung von Sitzungsdaten, bis hin zur Protokollierung der Inhalte von administrativen Zugriffen bei erhöhtem Schutzbedarf reichen.

Für die Absicherung administrativer Zugriffe ist auch ein Netzdesign erforderlich, das es erlaubt, administrative Kommunikation von produktiver Kommunikation zu trennen. Der Baustein NET.1.1 Netzarchitektur und -design spezifiziert hierzu in Anforderung A21 „Separierung des Management-Bereichs“ unter anderem, dass

- die IT-Komponenten möglichst über separate Interfaces administriert werden sollten,
- die Kommunikation mit diesen Interfaces in separaten Netzen über eine Firewall kontrolliert werden sollte,
- die zentralen Komponenten für Administration, Monitoring und Protokollierung in dedizierten Zonen über eine Firewall geschützt werden sollten und
- administrative Zugriffe auf dedizierte Endpunkte beschränkt werden sollten.

Letzteres wird in der Praxis auch durch die Bereitstellung von Terminal Servern für die Administration bzw. durch virtuelle Admin-PCs erreicht. Dies hat die Vorteile, dass die administrative Kommunikation zentralisiert wird, auf diese Weise leichter kontrollierbar ist und an einer Firewall zielgerichtet nur auf die notwendigen Zugriffe reduziert werden kann.

Eine umfassende Absicherung von administrativen Zugriffen mag aufwendig sein, Nachlässigkeiten können aber mehr als fahrlässig sein. Stellen Sie sich vor, ein PC wird Opfer eines zielgerichteten Angriffs und über einen Trojaner kontrolliert der Angreifer aus der Ferne mit den Berechtigungen des Nutzers den PC. Wenn der Nutzer nun ein Administrator wäre, hätte der Angreifer vielleicht sofort die Macht über die gesamte IT.

Verweise

[1] https://www.evolven.com/blog/5-it-operations-lessons-learned-from-jurassic-park.html

[2] https://www.heise.de/newsticker/meldung/Revenge-Wipe-Ex-Admin-loescht-Daten-bei-niederlaendischem-Provider-3740243.html

[3] https://www.cert-bund.de/advisory-short/CB-K17-2019

[4] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz-Kompendium/itgrundschutzKompendium_node.html

ComConsult Veranstaltungskalender

ComConsult RZ-Tage – Tag 1: Netzwerkarchitekturen der Zukunft im RZ, 11.12.2017 in Köln

Garantietermin

Schnelle und automatische Bereitstellung von Netzwerkinfrastrukturen erfordert eine Trennung in Underlay und Overlay-Netzwerke: Auf einer einheitlichen gerouteten IP-Basis werden verschiedene virtuelle Netzwerke zeitgleich betrieben. Ein virtuelles Netzwerk umfasst alle Teile einer Anwendung unabhängig von deren physischem Ort. Diese Vorgehensweise hat gravierende Konsequenzen, da Protokolle wie OSPF starke Einschränkungen in der Nutzung in diesem Umfeld haben. Gleichzeitig führen neue Software-Architekturen wie Mikro-Service-Architekturen zu einer starken Ausweitung von Layer-2-Bereichen im Hypervisor.

Preis: 1.090,-- €*

ComConsult RZ-Tage – Tag 2: Integration von Cloud-Lösungen in die RZ-Infrastruktur, 12.12.2017 in Köln

Garantietermin

Bei der Diskussion der Cloud beobachten wir ein radikales Umdenken. Die Diskussion um eine Verdrängung des RZs durch die Cloud ist vorbei. Jetzt geht es um die gezielte Nutzung von Funktionsbausteinen aus der Cloud, um die im RZ angebotenen Leistungen perfekt zu ergänzen. RZ plus Cloud bedeutet mehr Flexibilität, mehr Leistung und mehr Wirtschaftlichkeit. Dies bedeutet aber auch deutlich mehr Komplexität und ein Mehrbedarf an Arbeitskapazität.

Preis: 1.090,-- €*

Verkabelungssysteme für Lokale Netze, 11.12. - 12.12.2017 in Bonn

Garantietermin

Dieses Seminar erklärt praxisnah und herstellerneutral wie Sie hohe Qualität, Verfügbarkeit und lange Nutzbarkeit bei der Planung und im Betrieb einer Verkabelungs-Lösung erreichen. Die Bausteine einer Verkabelung werden vorgestellt und zu einem handhabbaren Gesamtsystem kombiniert. Lernen Sie wo sich gute von schlechten Lösungen unterscheiden. Neben der Erläuterung der aktuellen Normen wird die praktische Handhabung der Normungsvorgaben erklärt, wo macht eine Beachtung Sinn, wo nicht, wo ist es nicht ausreichend. Konkrete Durchführungen von Planungen in kleinen Übungsgruppen vertiefen die gewonnenen Erkenntnisse.

Preis: 1.430,-- €*

Betriebsvereinbarungen und Mitarbeiterdatenschutz bei IT- und TK-Systemen, 11.12. - 12.12.2017 in Bonn

Garantietermin

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

Preis: 1.590,-- €*

Die neue EU-Datenschutzgrundverordnung, 13.12.2017 in Bonn

Garantietermin

Am 25.05.2016 ist ein neues einheitliches Datenschutzrecht in der Europäischen Union in Kraft getreten. Die Verordnung wurde am 27.04.2016 verabschiedet und am 04.05.2016 im Amtsblatt der EU veröffentlicht. Bis zur einheitlichen Anwendung der Vorschriften gibt es 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 vorzubereiten.

Preis: 1.090,-- €*

iOS im Unternehmen, 19.02.2018 in Bonn

Apple Geräte mit iOS sind im Unternehmensalltag längst nicht mehr wegzudenken. Sie dienen nicht nur der Kommunikation, sondern werden oft für die Bearbeitung von Dokumenten und für den Zugriff auf Unternehmensressourcen verwendet. Im Gegensatz zur klassischen Unternehmens-IT unterliegen diese Geräte einem jährlichen Rhythmus neuer OS-Versionen mit neuen Möglichkeiten – aber auch mit neuen Herausforderungen. Dieses Seminar vermittelt kompakt und intensiv die Eigenschaften von iOS 11 zum sicheren und effizienten Einsatz in Unternehmen.

Preis: 1.090,-- €*

Sicherheit von Apps im Unternehmen, 20.02.2018 in Bonn

Der Markt für Apps explodiert. Die Potentiale für die Geschäftsprozesse sind enorm. Die damit verbundenen Risiken sind jedoch weitgehend unbekannt oder werden mehr oder weniger wissentlich ignoriert. Dieses Seminar bringt Licht in die bisher abgedunkelten oder verschleierten Stellen der mobilen IT Sicherheit ohne zu tief in die Bits und Bytes abzutauchen. Lassen Sie sich durch die größten Herausforderungen in der Konzeption und Nutzung von eigenen aber auch zugekauften Apps führen und nutzen Sie im Anschluss das erlernte Wissen zur sicheren Entwicklung und Beurteilung (Self-Assessment) von mobilen Apps.

Preis: 1.090,-- €*

IP-Wissen für TK-Mitarbeiter, 19.02. - 20.02.2018 in Bonn

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 praxisrelevanten Gesichtspunkten beleuchtet. Die Themen erstrecken sich von IP und LAN-Grundlagen hin zu praxisrelevanten Themen wie QoS, Jitter und Bandbreiten-Fragen. Ziel ist es dem IP-Unkundigen die wichtigen Grundlagen der Netzwerktechnik kompakt und praxisnah zu vermitteln.

Preis: 1.590,-- €*

Lokale Netze für Einsteiger, 19.02. - 23.02.2018 in Aachen

Garantietermin

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

Preis: 2.490,-- €*

* alle ausgewiesenen Preise sind Netto-Preise

Zertifizierungen

ComConsult Certified Network Engineer

Lokale Netze für Einsteiger
19.02. - 23.02.18 in Aachen
14.05. - 18.05.18 in Aachen
03.09. - 07.09.18 in Aachen

TCP/IP-Netze erfolgreich betreiben
12.03. - 14.03.18 in Berlin
04.06. - 06.06.18 in Bonn
08.10. - 10.10.18 in Bonn

Internetworking
09.04. - 12.04.18 in Aachen
18.06. - 21.06.18 in Aachen
12.11. - 15.11.18 in Aachen

Paketpreis für ein 5-tägiges, ein 4-tägiges, ein 3-tägiges Intensiv-Seminar € 6.000,--* (Einzelpreise: € 2.490,--*, € 2.290,--*, 1.890,--*)

ComConsult Certified Trouble Shooter

Trouble Shooting in vernetzten Infrastrukturen
24.04. - 27.04.18 in Aachen
11.09. - 14.09.18 in Aachen

Trouble Shooting für Netzwerk-Anwendungen
15.05. - 18.05.18 in Aachen
23.10. - 26.10.18 in Aachen

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

ComConsult Certified Voice Engineer

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen
12.03. - 14.03.18 in Bonn
14.05. - 16.05.18 in Köln
10.09. - 12.09.18 in Düsseldorf

Session Initiation Protocol Basis-Technologie der IP-Telefonie
11.04. - 13.04.18 in Düsseldorf
04.06. - 06.06.18 in Bonn
08.10. - 10.10.18 in Bonn

Umfassende Absicherung von Voice over IP und Unified Communications
23.04. - 25.04.18 in Bonn
25.06. - 27.06.18 in Düsseldorf
12.11. - 14.11.18 in Stuttgart

Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter
19.02. - 20.02.18 in Bonn
03.05. - 04.05.18 in Köln
03.09. - 04.09.18 in Bonn

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

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

* alle ausgewiesenen Preise sind netto-Preise

Impressum

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

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

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

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