ComConsult Research

Der Netzwerk Insider

Dezember 2016

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

Internet of Things – die vierte industrielle Revolution Teil 3

von Dipl.-Inform. Petra Borowka

Dieser Teil der Serie "Internet of Things" beschreibt als Alternative zum Europäischen Forschungsprojekt die IoT-Architektur, die das Industrial Internet Consortium spezifiziert hat. Daran anschließend beschreibt der Beitrag als pragmatische Vorgänger dieser Architektur aktuell verfügbare IoT-Lösungen und die hier eingesetzten Komponenten. Weiterführend geht der Beitrag auf verschiedene IoT-Protokolle ein, die heute um die Vorherrschaft im IoT-Markt streiten.

Teil 1 dieser Serie, in der Juli-Ausgabe des Netzwerk Insiders, beschäftigte sich unter anderem mit folgenden Fragen: hat IoT Revolutions-Potenzial für die Netzwerk-Technologie? Wo steht der IoT-Markt, Zeichnen sich bereits erkennbare Architekturen und Standards ab?

Im zweiten Teil, nachzulesen in der August-Ausgabe des Netzwerk Insiders, lag ein Schwerpunkt auf dem Draft D1.5 auch als "ARMv3" bezeichnet.

weiter auf Seite 10

Zweitthema

Das PSTN geht – Die Vielfalt kommt

von Markus Geller

Eine Erkenntnis unseres diesjährigen UC-Forums ist die Tatsache, dass immer noch viele Anwender mit der Entscheidung hadern, dass die klassische, kanalvermittelte Kommunikation von Seiten der Netzbetreiber aufgegeben wird. In diversen Diskussionen ging es dabei um solche Dinge wie:

- Was wird aus meinem FAX?
- Wenn es keinen Analoganschluss mehr gibt, was wird dann aus meinen Sonderanschaltungen?
- Und immer wieder die Frage: Wie realisiert man in Zukunft einen Notruf?

Die Gespräche kreisten dabei meistens um die Grundsatzfrage: Was muss der Netzbetreiber leisten und wer schreibt ihm vor, wie er diese regulatorischen Vorgaben erfüllen muss?

Dabei wird aber oft verkannt, dass es den „einen“ Netzbetreiber eben nicht mehr gibt und dass der Regulierer auch nur eine begrenzte, nationale Kompetenz hat.

Die Konsequenzen, die sich aus dieser Erkenntnis ergeben, möchte ich an folgendem kleinen Beispiel erklären, dem FAX.

Nach den aktuellen Vorgaben ist der Zugang zu Telefax-Diensten noch Teil der Grundversorgung, §78 TKG. Betrachtet man den Paragraphen einmal genauer, so steht dort aber nicht, wie diese Grundversorgung zu realisieren ist.

Dies ist aber gerade der entscheidende Punkt, da jeder Netzbetreiber für sich entscheiden darf, wie er diese eingeforderte Grundversorgung technisch umsetzt.

weiter auf Seite 23

Geleit

Machine Learning: das Ende des Netzwerk-Administrators?

auf Seite 2

Standpunkt

Schluss mit lustig: Eine umfassende und verbindliche Cyber-Sicherheitsstrategie muss her

auf Seite 22

Aktueller Kongress

ComConsult Netzwerk-Forum 2017

auf Seite 5

Sonderveranstaltung und Report

Wireless und Mobility Wireless Systeme

ab Seite 6

Geleit

Machine Learning: das Ende des Netzwerk-Administrators?

Seit der ersten Nutzung von Lokalen Netzwerken Anfang der 80er Jahre haben wir in regelmäßigen Abständen einen Bruch der eingesetzten Technologien und ein Aufkommen neuer Lösungen erleben können. Der Wechsel von Hubs zu Switches, der Übergang von Layer-2 auf Layer-3, das Aufkommen und Verschwinden von ISO/OSI und der Siegeszug von TCP/IP sind gute Beispiele für diese Umbrüche. Das bedeutet aber auch, dass wir nicht davon ausgehen können, dass alles so bleibt wie es jetzt ist. Und tatsächlich sehen wir die potentiell nächste große Entwicklungsstufe für Netzwerke am Horizont.

Was ist im Moment die erfolgreichste Vorlesung an der Stanford-Universität? Es ist Machine Learning mit 750 Teilnehmern. Berücksichtigt man, dass wir hier über eine massive Mathematik-Anwendung sprechen, dann spricht das für sich. Sieht man allerdings wie Machine Learning die Welt um uns herum verändert, dann ist das nicht verwunderlich. Nach Jahren der Stagnation haben neue Verfahren rund um neuronale Netzwerke in den letzten 3 bis 4 Jahren zu einem Durchbruch geführt. Am einfachsten wird das sichtbar in den Bereichen Spracherkennung (Google und Amazon) und der automatischen Bildbewertung (zum Beispiel Gesichtserkennung, ein Beispiel wäre Google Photo). Auf die Frage welche Technologie unsere Welt in den nächsten 10 Jahren am meisten prägen wird, gibt es dementsprechend im Moment von vielen Experten in der Forschung auch nur eine Antwort: Machine Learning oder allgemeiner Künstliche Intelligenz KI (Artificial Intelligence AI).

Was hat das mit Lokalen oder Weitverkehrs-Netzwerken zu tun? Wo ist die Anwendung, aus der ich einen Vorteil für den Betrieb oder die Konfiguration eines Netzwerks ziehen kann? Und warum überschlagen sich im Moment führende Hersteller mit dem Einstieg in diese Technologie?

Dazu müssen wir erst einmal die Frage beantworten was Machine Learning eigentlich macht. Einfach formuliert sucht es nach Mustern oder Gesetzmäßigkeiten in großen Datenmengen. Die Muster können entweder vorgegeben sein (man spricht von Labeln und die Vorgabe nennt sich Supervised Machine Learning) oder das Verfahren findet selber bestehende Muster. Die Erkennung ist nie 100% präzise. Tatsächlich haben die Fortschritte im Machine Learning viel damit zu tun wie die Fehlerquote verringert werden kann. So hat sich die Spracherkennung in den letzten Jahren von ca. 89% auf 94% verbessert. Diese Verbesserung wirkt marginal, aber sie repräsentiert einen Quantensprung, wenn man sich Beispiele anhört, die davon betroffen sind (zum Beispiel ein sehr hoher Anteil an Umgebungsgeräuschen, oder eine Sprachaufzeichnung, die bestimmte Frequenzen abschneidet und damit phonetisch zu nicht mehr eindeutigen Ergebnissen führt). Damit einher gehen dramatische Verbesserungen in der automatischen Übersetzung von Texten. (siehe Abbildung 1)

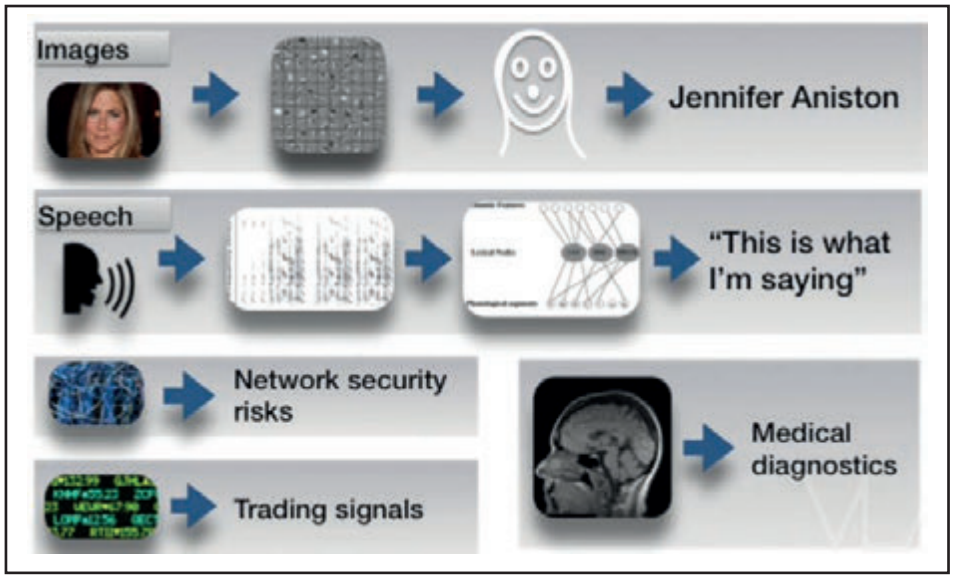


Abbildung 1: Anwendungsbereiche von Machine Learning
Quelle: Stanford Graduate School of Business 2016

Zurück zu unserer Ausgangsfrage: was hat das mit Netzwerken zu tun und besteht wirklich eine Gefahr für den Netzwerk-Administrator? Diese Frage lässt sich in zwei Fragen unterteilen: was wollen wir denn wissen und woher bekommen wir die Information?

Fangen wir mit der zweiten Frage an. Wir haben zwei sehr unterschiedliche Quellenreiche von Information. Eines sind die Pakete, die wir in Netzwerken transportieren und auf denen alles basiert, was wir machen. Sie erzählen uns wer mit wem kommuniziert, mit welchem Protokoll und ggf. auch mit welcher Anwendung. Durch unsere Kenntnis von Protokollen können wir aus den Paketen und einem spezifischen Messort Zusatzinformation wie Laufzeiten oder Störungen im Verbund mit Retransmissionen ableiten. Der zweite Bereich der Daten, die wir zur Verfügung haben, fällt in spezialisierten Sensoren oder Agenten an und bezieht sich in der Regel auf einen Teilbereich einer Technologie oder eines einzelnen Geräts. Ein Beispiel wäre die Auslastung des Pufferspeichers in einem Switch oder die Trefferrate in einem Cache eines Speichersystems.

Was ist das Grundproblem dieser Daten? Das traditionelle Netzwerk- und System-Management, das diese Daten verarbeitet, kommt an seine Grenzen, weil wir zu viel Information haben. Mit der Zunah-

Machine Learning: das Ende des Netzwerk-Administrators?

me der Leistung unserer Server und Speichersysteme, mit modernen Mikroservice-Architekturen und mit immer höheren Übertragungsraten kommen eigentlich bewährte Methoden der Fehleranalyse oder des Reporting an ihre Grenzen. Jeder, der einmal auch nur versucht hat, eine Protokollanalyse auf einer 100 Gigabit-Verbindung zu fahren, wird das vermutlich bestätigen. Kombiniert man das mit dem Problem, dass in einer dynamischen Architektur ja gar nicht klar ist welche 100 Gigabit-Verbindung untersucht werden muss, dann erkennt man die Grenze des Möglichen. In Konsequenz grenzt man die Analysen, die man in der Praxis ausführen kann, immer mehr ein. Das Ergebnis ist, dass temporäre oder dynamisch wiederkehrende Störungen kaum noch sauber analysiert werden können. Es "reduziert" sich auf die Erfahrung des Trouble-Shooters und dessen Intuition.

Gleichzeitig stehen wir vor einer zunehmenden Dynamik von Anwendungs-Architekturen. Mikroservice-Architekturen generieren neue Instanzen abhängig von der Nachfrage. Sie machen das an Orten wo gerade Kapazität ist. Dafür müssen nun Netzwerke konfiguriert werden, aber auch Server- und Speicher-Instanzen bereitgestellt werden. Dies kann man nun entweder statisch vorgeben oder man lässt es offen. Die statische Vorgabe funktioniert nur zu einem bestimmten Grad und sie wird die bestehenden Kapazitäten nicht optimal auslasten. Lassen wir es offen, dann stellt sich die Frage wo die Konfiguration herkommt.

Damit kommen wir auf die Frage zurück: was wollen wir denn wissen und was würden wir tun, wenn wir es wüssten?

Einfache Beispiele für Betriebssituationen, die wir gerne kennen würden, wären:

- Antwortzeiten in einer Applikation liegen weit außerhalb des zulässigen Bereichs
- Ein Hacker greift eine interne Ressource an
- Ein System ist fehlkonfiguriert, es wird auf "falsche" Ressourcen zum Beispiel aus einem Testbetrieb zugegriffen

Starten wir mit dem ersten Beispiel. Dies ist unser Tagesgeschäft und in immer komplexeren Architekturen der Alptraum schlechthin. In einer traditionellen zwei oder drei Tier-Architektur war es klar wo wir nachsehen können. Aber sobald eine Applikation aus 30 oder 40 Mikroservices besteht, die überall sein können und wilde Kommunikationsbeziehungen pflegen, ist die Frage eigentlich nicht, warum Antwortzeiten schlecht sind, sondern eher warum es überhaupt funktioniert (nicht wirklich, aber es wird hoffentlich klar wo das Problem ist).

Welche Informationen hätten wir denn zur Bearbeitung des Problems:

- wir wissen, welche Verbindungen zwischen den Instanzen der Applikation existieren und kennen die Details über die Performance der Verbindung
- wir kennen die Topologie und alle Infrastruktur-Komponenten, die betroffen sind. Vom virtuellen über den physikalischen Server über das Netzwerk bishin zum virtuellen und physikalischen Speicher
- wir kennen die Betriebszustände aller betroffenen Komponenten

Diese bekannte Information liegt dummerweise in Millionen von Paketen vor. Oder eventuell sogar in noch mehr Paketen. Der Zahl der Nullen ist hier keine Grenze gesetzt.

Was nun?

Schon die Gestaltung des Beispiels macht deutlich warum wir hier Machine Learning zum Einsatz bringen können. Zum Beispiel können wir definieren, wann wir einen guten, mäßigen oder nicht akzeptablen Betrieb haben. Das kann sich wahlweise auf Anwendungen, auf Server, Speicher oder das Netzwerk beziehen. Wir nennen das supervised learning, da wir die Label vorgeben. Und Machine Learning kann nun hingehen und in allen verfügbaren Daten nach typischen Mustern für gut, mäßig oder schlecht suchen. Sobald es die Muster kennt, kann es anfangen im laufenden Betrieb danach zu suchen. Und das System ist nicht statisch. Das System kann zum Beispiel bisher nicht definierte Muster finden und uns fragen, ob wir dafür ein Label vergeben wollen. Oder wir als Betreiber merken, dass uns etwas gefehlt hat und definieren ein neues Label und lassen das Muster dafür ermitteln. Liegen die Daten in gespeicherter Form vor, dann kann diese Analyse auch rückwirkend durchgeführt werden.

Diese Mustererkennung und die Zuordnung zu einem Label wie zum Beispiel "sicher", bei der wir keinen externen Angriff vermuten, kann sehr effektiv sein. Wir wissen zum Beispiel in einer Mikroservice-Architektur welche Instanzen wann und wie typischerweise miteinander sprechen. Taucht auf einmal entweder eine neue Instanz auf oder eine untypische Nutzung einer bekannten Verbindung erfolgt, dann kann das sofort festgestellt werden.

Damit sind wir bei den Reaktionen bzw. den Gegenmaßnahmen. So wie die Systeme heute ausgelegt sind, muss die Reaktion auf komplexe Betriebszustände von einem Administrator kommen. Aber es ist leicht erkennbar, dass das nur eine Frage der Zeit ist, bis das System lernt wie aus einem Label "schlecht" ein Label "gut" gemacht werden kann. Bei Angriffen ist das denkbar einfach, indem die Verbindung blockiert wird. Bei Performance-Problemen kann das komplexer sein. Da Machine Learning nicht 100% sichere Resultate erzeugt, muss auch genau überlegt werden, wann man eine automatische Reaktion zulässt und wann nicht. Auch 95% Sicherheit bedeutet 5% falsche Entscheidungen. Und das kann je nach Szenario nicht zumutbar sein.

Wird das auf Dauer den Administrator

Abbildung 2: Cisco Tatration Analytics, Dirk Stöckmann, ComConsult Study.tv
http://www.comconsult-study.tv/video.html?vid=1820

Machine Learning: das Ende des Netzwerk-Administrators?

komplett ersetzen? Nicht komplett, da ja jemand die Label bzw. die Betriebssituationen und ihre Bewertung vorgeben und pflegen muss. Und vermutlich muss auch immer jemand das Toolset der möglichen Reaktionen vorgeben und pflegen. Zum Beispiel, dass das Netzwerk eine weitere physikalische Verbindung aufmacht oder weitere VXLAN-Tunnel anlegt. Und meine persönliche Präferenz wäre, dass vollautomatische Deaktivierungen nach Möglichkeit nur mit menschlicher Zustimmung erfolgen. Aber gerade die Frage nach der Abwehr von möglichen Angriffen zeigt, wie schwer diese Entscheidung ist. Eine zu langsame Reaktion kann einem Angreifer genau das geben was er gesucht hat.

Aber wie immer man die aktuelle Lage bewertet, es wird deutlich, dass Netzwerk- oder Systembetrieb vielleicht vor dem größten Wandel der IT-Geschichte stehen kann. Dabei ist die Frage nicht, ob das technisch möglich ist. Die Antwort darauf ist ja. Die einzige Frage, die wir momentan stellen müssen, ist, ob das jemals wirtschaftlich sein wird und für welche Größenordnungen von Kunde das relevant wird. Es ist keine Frage von Rechenleistung oder ähnlichen Grenzen der Vergangenheit. Davon haben wir in Zukunft mehr als genug. Allerdings sei an dieser Stelle auch davor gewarnt, jedes Produkt, das mit dem Attribut “Machine Learning” oder AI verkauft wird, generell als gut anzusehen. Im Prinzip könnte man jede Interpolation oder Regression einer Zahlenmenge in MS Excel als Mustererkennung bezeichnen. Dies hat genauso wenig mit einem modernen Machine Learning zu tun wie ein Regelbasiertes Abarbeiten von Betriebsdaten (so wie wir es im Netzwerk- und System-Management seit 20 Jahren machen). Von daher ist wie immer Vorsicht geboten und an einem ausführlichen Test eines Produkts führt kein Weg vorbei.

Wir werden diese Frage auf unseren Netzwerk-Forum 2017 diskutieren. Naturgemäß stehen wir am Anfang dieser Entwicklung. Aber wir haben aktuelle Ansätze von Cisco und Extreme, über die es sich lohnt zu diskutieren. Auch weil es dabei um die mittelfristige Perspektive solcher Produkte geht. Und das ist nicht alles. Wer geglaubt hat, dass Technologien wie SDN bereits wieder verschwunden sind, der wird an diesem Beispiel sehen, dass sie genau in dem Bereich der möglichen Handlungs-Alternativen angesiedelt sind.

Ihr
Dr. Jürgen Suppan

Kongress

ComConsult Netzwerk Forum 2017
27.03. - 29.03.2017 in Köln

Das ComConsult Netzwerk-Forum 2017 stellt die vier momentan dominantesten Netzwerk-Themen in den Mittelpunkt der Veranstaltung: Anwendungs-Architekturen und Kommunikation im Rechenzentrum, Netzwerk-Design und Optimierung des Betriebs, WLAN-Design und die Herausforderungen neuer Standards, Netzwerk-Sicherheit in einem Cloud-Umfeld.

Am ersten Tag analysieren wir die Auswirkungen aktueller Anwendungs-Architekturen auf die schnelle Bereitstellung, die Gestaltung und die Leistung von Netzwerken. Anwendungs-Architekturen werden immer dynamischer und in Kombination mit der Forderung nach einer sehr schnellen Bereitstellung von Kapazitäten ergibt sich eine komplexe Orchestrierungs-Aufgabe. Die Dynamik ergibt sich dabei nicht nur beim Start einer Mikroservice-Architektur, sondern auch bei Lastveränderungen im laufenden Betrieb.

Am zweiten Tag stellen wir uns den aktuellen Veränderungen im Netzwerkdesign in Kombination mit der Frage, wie wir in einer immer komplexeren Situation zu einem optimalen Betrieb kommen können.

Am dritten Tag diskutieren wir die neuesten WLAN-Standards und zum Abschluss des Tages die Frage, wie eine umfassende Sicherheits-Lösung unter Berücksichtigung der Cloud aussehen kann.

Wie in jedem Jahr so wird auch 2017 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.

Frühbucherphase bis zum 31.12.2016

Top-Referenten, die Analyse der neuesten Entwicklungen, praxisnahe Empfehlungen, mehr Sicherheit für Ihre Entscheidungen und viele, viele Diskussionen prägen diese Veranstaltung.

Preis: € 2.190,- netto*
*gültig bis zum 31.12.016 - dann regulärer Preis € 2.390,- netto

Buchen Sie über unsere Web-Seite

www.comconsult-akademie.de

Aktueller Kongress

ComConsult Netzwerk Forum 2017
27.03. - 29.03.17 in Köln

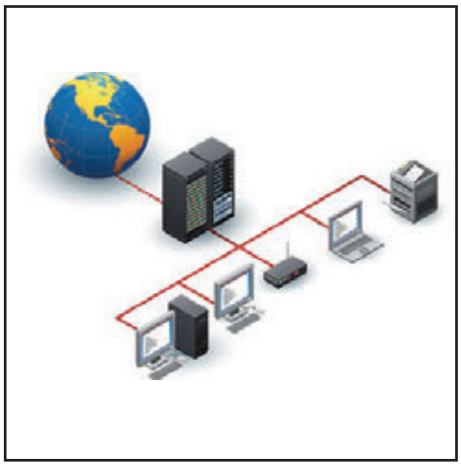
Die ComConsult Akademie veranstaltet vom 27.03. bis 29.03.2017 ihren Kongress "ComConsult Netzwerk Forum 2017" in Köln.

Das ComConsult Netzwerk-Forum 2017 stellt die vier momentan dominantesten Netzwerk-Themen in den Mittelpunkt der Veranstaltung:

- Anwendungs-Architekturen und Kommunikation im Rechenzentrum
- Netzwerk-Design und Optimierung des Betriebs
- WLAN-Design und die Herausforderungen neuer Standards
- Netzwerk-Sicherheit in einem Cloud-Umfeld

Am ersten Tag analysieren wir die Auswirkungen aktueller Anwendungs-Architekturen auf die schnelle Bereitstellung, die Gestaltung und die Leistung von Netzwerken. Anwendungs-Architekturen werden immer dynamischer und in Kombination mit der Forderung nach einer sehr schnellen Bereitstellung von Kapazitäten ergibt sich eine komplexe Orchestrierungs-Aufgabe. Die Dynamik ergibt sich dabei nicht nur beim Start einer Mikroservice-Architektur, sondern auch bei Lastveränderungen im laufenden Betrieb.

Wir stellen uns dementsprechend den Fragen:



- wie sieht die Schnittstelle zwischen Anwendung und Netzwerk aus?
- schnelle Bereitstellung und dynamische Kapazitätsanforderungen: wie geht das?
- welche Basis-Technologien sind auf der Netzwerkseite erforderlich?
- was muss Orchestrierung leisten?

Am zweiten Tag stellen wir uns den aktuellen Veränderungen im Netzwerkdesign in Kombination mit der Frage, wie wir in einer immer komplexeren Situation zu einem optimalen Betrieb kommen können.

Wir analysieren:

- wie sehen die aktuellen Design-Entwicklungen aus?
- Software Defined WAN: Hype oder bringt es wirklich etwas?
- Künstliche Intelligenz als Basis des Netzwerk-Betriebs: ist Machine Learning die Zukunft des Betriebs?

Am dritten Tag diskutieren wir die neuesten WLAN-Standards und zum Abschluss des Tages die Frage, wie eine umfassende Sicherheits-Lösung unter Berücksichtigung der Cloud aussehen kann.

Im Detail stellen wir vor:

- die neuen WLAN-Standards mit immer mehr Leistung: kommen wir an die Grenzen des Planbaren? wie viel Leistung können wir in Zukunft in welchen Szenerien liefern?
- WLAN und 5G: wie sieht in Zukunft das Zusammenspiel von WLAN und Mobilfunk aus?
- Kommunikation mobiler Endgeräte: wie integrieren wir welches Gerät wann und an welchem Ort optimal?
- Netzwerke und die Cloud: ein unlösbarer Widerspruch in der Gestaltung von Sicherheit?

Wie in jedem Jahr so wird auch 2017 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@comonsult-research.de

ComConsult Netzwerk Forum 2017

Ich buche den Kongress
ComConsult Netzwerk Forum 2017
27.03. – 29.03.17 in Köln

☐ zum Preis von € 2.190,-- netto*
* Preis gültig bis zum 31.12.16 - danach regulär € 2.390,-- 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

Sonderveranstaltung

Sonderveranstaltung Wireless und Mobility 12.12.-13.12.16 in Köln

Die ComConsult Akademie veranstaltet vom 12.12. bis 13.12.16 ihre Sonderveranstaltung "Wireless und Mobility" in Köln.

Die permanente Steigerung der Anzahl mobiler Endgeräte mit immer mehr Leistung ist ein längst nicht mehr aufzuhaltender Trend. Provider sind schon seit einiger Zeit dabei, die Mobilfunknetze deutlich aufzurüsten. Dies betrifft auch Betreiber privater wireless Infrastrukturen. Sie werden kaum Videos oder Spiele in großem Umfang unterstützen müssen. Man kann aber davon ausgehen, dass die hohe Leistung der mobilen Endgeräte auch für die Realisierung eines verbesserten Benutzer-Erlebnisses bei bestehenden und neuen Anwendungen genutzt wird. Die vielen unterschiedlichen Ansätze für Augmented Reality sprechen z.B. eine deutliche Sprache. Ist eine Technologie, wie in diesem Falle die mobile Anbindung intelligenter Endgeräte verfügbar und erfolgreich, kommen im Laufe der Zeit sozusagen „natürlich“ neue Anwendungen hinzu.

Mega-Treiber: Cloud, Video und IoT

Moderne Arbeitsplatzmodelle gehen von vollständig mobilen Endgeräten aus. Es darf auf die Dauer keine spürbaren qualitativen Unterschiede bei der Benutzung Cloud-basierter oder sonstiger Dienste und Kollaborationstechniken in Abhängigkeit vom Ort oder dem grade vorliegenden Mobilitätsgrad geben.

Es besteht die quasi unabwendbare Tendenz, drahtlose Netze zur Lieferung immer reicherer Inhalte an immer mehr Endgeräte zu benutzen. Dies erzeugt einen erheblichen Druck auf die Ressource, über die wir liefern: die Kapazität des (drahtlosen) Netzes und der dahinter liegenden Infrastruktur.

Ein weiterer Mega-Treiber ist das IoT, die automatische Kommunikation von Maschinen, Sensoren und Aktoren untereinander. Viele IoT-Konzepte könnten ohne drahtlose Verbindungen nicht implementiert werden. Das erzeugt eine völlig neue Dimension von Anforderungen, Leistungsprofilen und Spezial-Technologien.

Private flächendeckende WLAN-Versorgungsstrukturen nach IEEE 802.11ac: mehr Fragen als Antworten!

Mit IEEE 802.11ac Wave2 steht eine neue Evolutionsstufe für WLANs zur Verfügung. Vereinzelt wurde auch schon Wave3 mit einer theoretischen Leistung von 10 Gbps angekündigt. Die wichtigen neuen Funktionen von Wave2 und 3 müssen auf den Prüfstand. Was können sie bewirken? Und: ist ihre Nutzung überhaupt erlaubt? Für die Nutzung von 160 MHz breiten Kanälen in flächendeckenden Infrastrukturen ist eine Erweiterung der bisher zulässigen Frequenzbereiche notwendig. Die ist auf dem Weg, aber erreicht sie uns rechtzeitig?

Man kann behaupten, dass Wave2 und Wave3 die ersten wirklich für den professionellen Einsatz gedachten Varianten von IEEE 802.11ac sind. Was bedeutet das in der Praxis? Welche Steuerungsmöglichkeiten bieten uns die einschlägigen Hersteller an?

Eine wesentliche Frage ist: wie werden die neuen Systeme in die Gesamt-Architektur integriert? Die oftmals propagierte „gesteigerte Benutzererfahrung“ ist ja gut und schön, aber welche Anforderungen stellt sie an die betriebliche Logik der Infrastrukturen?

Nach wie vor sollte doch der sichere und wirtschaftliche Betrieb der privaten drahtlosen Infrastrukturen im Vordergrund stehen. Provider erwarten die Möglichkeit, ihre Strukturen aus der Cloud mittels SDN/NFV zu steuern und z.B. Instanzen virtueller Small Cells dynamisch auf der physikalischen Infrastruktur zu schaffen. Sind derartige Funktionen für „normale“ private Betreiber wirklich erforderlich? Wie können Sicherheitskonzepte elegant und wirkungsvoll umgesetzt werden?

Es gab in den letzten Monaten eine Menge von Mergern zwischen Infrastruktur-Anbietern und WLAN-Spezialisten. Cisco hat sich Meraki einverleibt, Aruba gehört jetzt zu HP Enterprise, Brocade funkt jetzt mit Ruckus und auch Extreme/Enterasys haben sich noch einen kleinen WLAN-Spezialisten organisiert. Die Erwartung ist, dass dadurch Synergien zwischen den WLAN-Lösungen und der notwendigen Switching-Infrastruktur entstehen. Wie sieht das aber genau aus? Welche Vorteile ergeben sich möglicherweise für den Betreiber?

Mobilfunk: letztlich das Ende der privaten WLANs?

Schließlich: wie geht es weiter mit dem Mobilfunk? Ausgehend von LTE entwickeln sich nicht nur die nächsten Releases mit deutlich erhöhter Funktionalität bis hin zu 5G, sondern parallel dazu auch Begehrlichkeiten hinsichtlich der bislang den WLANs vorbehaltenen lizenzfreien Frequenzbereiche. Um nämlich die hochgesteckten Ziele von 5G erreichen zu können, brauchen die Provider alle Frequenzen, die nicht bei „3“ auf dem Baum sind, von stillgelegten TV-Kanälen bis hin zu gelegentlichen Lücken in systematischen Funkdiensten. Die Zukunft gehört dem dynamisch etablierten virtuellen Spektrum. Treffen aber konventionelle WLANs mit LTE oder 5G-Signalen zusammen, werden sie höchst wahrscheinlich den Kürzeren ziehen. Oder kann man vorbeugen?

Schon vor über fünf Jahren wurde der Standard IEEE 802.11ad für die Multi-Gigabit-Kommunikation im 60 GHz Millimeterwellen-Bereich definiert. Auch Small Cells werden zunehmend im Millimeterwellenbereich aufgesetzt. Wie sind derartige Trends für private Betreiber zu werten?

Die Entwicklung internationaler Mobilfunkstandards ist deutlich aufwändiger als z.B. eine neue Ethernet-Norm. Die meis-

ten Kunden bekommen heute LTE nach Release.10. Rel. 10 bis ca. Rel .12 heißen auch „LTE Advanced“. Schon in diesen Versionen wird das Konzept aufgegriffen, die Leistung von LTE durch die Hinzunahme von passenden Zellenkonzepten zu erhöhen. Unter Voraussetzung eines guten Interferenz-Managements steigt die mögliche Leistung eines LTE-Versorgungsbereiches (einer Basis-Station) deutlich mit der Anzahl von kleinen Zellen (Small Cells). Richtig spannend wird es mit den Versionen ab Rel. 13 und 5G.
Wie könnte sich das auswirken? Normalerweise wird ein LTE Netz von einem Provider betrieben und auch WLAN oder auf anderer Technik beruhende Small Cells werden auch von ihm kontrolliert.

Gravierende Auswirkungen auf die unterstützende Infrastruktur

Die Anforderungen an die mobile Versorgung steigen stark und man wird darauf Antworten finden müssen. Es wird sicher nicht zu weniger, sondern eher zu mehr WLAN-Zellen kommen. Das wird glücklicherweise durch die entsprechenden Ethernet-Technologien für die Integration der vielen APs unterstützt.

Allgemein werden heute WLAN-Access Points mit 1 GbE und PoE versorgt. Im letzten Jahr wurden neue Ethernet Datenraten definiert, nämlich 2,5 und 5 GbE, die für die Versorgung anspruchsvollerer Access Points nach 802.11ac noch über ältere Kabel gedacht sind. Betrachtet man aber die jetzt schon in Entwicklung befindlichen Nachfolgestandards IEEE 802.11 ad (schon längst fertig), ax und ay, sieht man schnell, dass 5 GbE viel zu kurz greifen. Provider nutzen optische Infrastrukturen, alleine wegen der Latenzen. Ist das auch der Weg für ambitionierte private Betreiber?

Sie sehen: viele Entwicklungen, viele Technologien, Fragen über Fragen. Auf unserer einzigartigen Sonderveranstaltung hören Sie, was erfahrene Top-Spezialisten, Planer, Hersteller und Berater empfehlen. Nutzen Sie die Gelegenheit auch zur ausführlichen Diskussion, bevor die Wireless Welle Sie überflutet.

Die Referenten


Dr. Jan Byok


Dipl.-Ing. Stefan Bien


Dr. Johannes Dams


Christian Goldberg


Dipl.-Ing. Olaf Hagemann


Dr. Simon Hoff


Dr. Franz-Joachim Kauffels


Reinhard Lichte


Dipl.-Ing. Markus Nispel


Dipl.-Ing. Michael Schneiders


Dr. Joachim Wetzlar


Dipl.-Ing. Dominik Zöller

Anmeldung an kundenservice@comonsult-research.de

Sonderveranstaltung Wireless und Mobility

Ich buche die Sonderveranstaltung
Wireless und Mobility

☐ 12.12.-13.12.16 in Köln
zum Preis von € 1.990,--

☐ inklusive Report "Wireless-Systeme der nächsten Generation"
zum Teilnehmer Sonderpreis von 174,- €

☐ 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 Sonderveranstaltung Wireless und Mobility

Montag 12.12.2016

9:30 - 10:15 Uhr
Wireless World: Anforderungen der Digitalen Zukunft
- Implikationen der wachsenden Cloud-Nutzung
- Neue Anwendungen und Anforderungen an Multi-Gigabit WLANs
- IoT und die enge Verbindung zu Mobilfunktechnologie (5G)
- Strukturelle Aspekte unterstützender Infrastrukturen

Dr. Franz-Joachim Kauffels, Technologie-Analyst

10:15 - 11:00 Uhr
Stand der Technik bei WLAN
- IEEE 802.11ac in den verschiedenen Geschmacksrichtungen
- Ist mit 10 Gbit/s auf 2,4 und 5 GHz Schluss oder geht zukünftig noch mehr?
- WLAN im 60-GHz-Band: Es gibt Standards aber kaum Anwendungen • Was sagt die IEEE zur Mobilfunk-Integration?

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

11:00 - 11:30 Uhr Kaffeepause

11:30 - 12:15 Uhr
WLAN, ein Medium für alle Anwendungen?
- Mobilität und Einfachheit sind Triebfedern für die WLAN-Vernetzung
- Hohe Verfügbarkeit, Reaktivität und Bitrate: Geht das überhaupt mit WLAN?
- Wie bekommt man die optimale Ausleuchtung in Büros und Hallen am besten hin?
- Welche Frequenzen sollen für welche Anwendungen genutzt werden? • An allen Ecken funkt es: Lassen sich Störungen überhaupt vermeiden?
- „Fremde" Funkanwendungen sickern unbemerkt ein! Wie geht man damit um?

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

12:15 - 13:00 Uhr
Einführung in Cloud Managed IT
- Cloud Management, was bedeutet das?
- Mehrwerte für Unternehmen jeder Größe
- Hybride Infrastrukturen – Realität oder Wunschdenken
- Anwendungsbeispiele

Christian Goldberg, Cisco Systems GmbH

13:00 - 14:30 Uhr Mittagspause

14:30 - 15:30 Uhr
WLAN-Zellplanung auf dem Prüfstand
- Welchen Stellenwert hat die WLAN-Zellplanung bei der Konzeptionierung einer WLAN-Infrastruktur?
- Welche Parameter sind bei einer professionellen WLAN-Zellplanung zu berücksichtigen?
- Ausleuchtungsmessung vs. Simulation
- Häufige Fehler, die Sie unbedingt vermeiden sollten. Dos and Don'ts

Dipl.-Ing. Stephan Bien und Dr. Johannes Dams, ComConsult Beratung und Planung GmbH

15:30 - 16:00 Uhr Kaffeepause

16:00 - 17:00 Uhr
All-IP: ein einheitlicher Access für jegliche Sprachkommunikation. Sind DECT und VoWLAN tot?
- Die Rolle von LTE und 5G im All-IP-Netz
- Mobilfunk in Enterprise-Kommunikationslösungen
- VoLTE und 5G als Ersatz für VoWLAN und (IP-)DECT

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

17:00 - 18:00 Uhr
Von LTE Advanced zu 5G
- Mobilfunk: Stütze der nächsten digitalen Revolution
- Techniken von LTE Advanced
- Koexistenz von LTE / 5G und WLANs
- 5G: Konzepte, Technologien, Feldversuche, Standardisierung

Dr. Franz-Joachim Kauffels, Technologie-Analyst

ab 18:00 Uhr Happy Hour

Dienstag 13.12.2016

9:00 - 10:30 Uhr
Wireless / Mobile / Cloud Security: Ganzheitliche Konzepte sind gefragt
- Sicherheit im WLAN: Ein alter Hut?
- Warum es trotz Hotspot 2.0 kaum sichere Hotspots gibt
- Absicherung von iOS und Android
- Sichere Integration mobiler Endgeräte
- Schlüsselelement sichere Cloud-Dienste
- Rolle von MDM und WLAN Management aus der Cloud

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

10:30 - 11:00 Uhr Kaffeepause

11:00 - 11:45 Uhr
Auf dem Weg zum All Wireless Office
- WLAN als normales Office Connect muss wie Strom, Wasser, Klima als Infrastruktur leistungsstark zur Verfügung stehen
- Nutzung der WLAN Infrastruktur von allen User- und Gerätetypen
- WLAN und dann ... – Analytics, Locationbased Serivces. Beispiel: der intelligente Meetingraum
- WLAN als Offload von Mobilnetzen in empfangsschwachen Officebereichen
- On-premise, private Cloud oder Public Cloud Lösungen – eine Portfolio für alles

Reinhard Lichte, Aruba - a Hewlett Packard Enterprise Company

11:45 - 12:30 Uhr
Moderne flächendeckende Enterprise WLANs
- Neue Anforderungen durch Cloud und Hybrid Enterprise
- Rolle von SDN/NFV bei der WLAN-Steuerung
- Integriertes Produktspektrum für Zellen und Infrastruktur
- Anwendungsbeispiele

Dipl.-Ing. Markus Nispel, Dipl.-Ing. Olaf Hagemann, Extreme Networks GmbH

12:30 - 14:00 Uhr Mittagspause

14:00 - 15:00 Uhr
Netz-Architekturen für (High Speed) WLANs
- Welche Anforderungen bestehen an die Netzarchitektur für den Aufbau von WLANs
- Der WLAN-Controller: Flaschenhals oder Mittel der Wahl?
- Alternativen zum WLAN Controller: Was bieten die Hersteller?
- IEEE 802.3bz: Seit dem 27.09.2016 gibt es „Breitreifen" für Access Points

Dipl.-Ing. Michael Schneiders, ComConsult Beratung und Planung GmbH

15:00 - 16:00 Uhr
Rechtliche Aspekte des Betriebs privater WLAN-Infrastrukturen
- Grundlagen der deutschen Störerhaftung nach ständiger BGH-Rechtsprechung (Neueste Entwicklungen im Bereich der Störerhaftung)
- Gesetzesänderung des TMG aus Sommer 2016
- EuGH Urteil aus Herbst 2016 (Zukunft der deutschen Störerhaftung, Gestaltungstipps für Betreiber privater WLAN-Infrastrukturen)

Dr. Jan Byok, Bird & Bird LLP

16:00 Uhr der Veranstaltung

Report-Neuerscheinung

Wireless-Systeme der nächsten Generation:

Anwendungen, Systeme, Anforderungen

In den nächsten Tagen erscheint ein neuer Technologie-Report von Dr. Franz-Joachim Kauffels bei der ComConsult Research GmbH.

Dieser Report ist ein unverzichtbares Hilfsmittel für alle, die sich mit der Schaffung von Wireless Versorgungsstrukturen für die Anforderungen der digitalen Zukunft rüsten. Die Studie hilft, die neuen drahtlosen Übertragungstechniken und ihre Wechselwirkungen besser einzuschätzen und die passende Infrastruktur vorzubereiten.

Blickt man auf die Anforderungen der jetzt in Entwicklung befindlichen Systeme wie IEEE 802.11ax und 11ay, sieht man sofort, dass diese mit 2,5 oder 5 GbE absolut nicht auskommen. Ein sehr wesentlicher Schritt bei diesen Versionen ist, dass das DCF-Verfahren wohl endlich abgelöst wird, was der Autor aber erst glaubt, wenn er es sieht. Dadurch wird hier schon eine vollwertige 10 GbE Infrastruktur mit entsprechender Verkabelung notwendig. Aber auch schon für IEEE 802.11ac Wave 2 oder 3 wird es Access Points mit 10 GbE-Ports Richtung Infrastruktur geben. Ein in 2016 noch fehlender Baustein ist Power over 10 GBASE-T, aber auch hier gibt es eine Reihe von Alternativen und Prototypen, die mit Sicherheit sehr bald zu guten standardisierten Lösungen führen werden. Die Angst mancher Betreiber vor zu hohen Kosten einer 10 GbE Infrastruktur ist nicht begründet.

10 GbE ist angesichts der Verfügbarkeit von 25/50/100 GbE Switching-Lösungen schon jetzt eine Technologie der zweiten Reihe. Es gibt 10/40 GbE Switch-Chips in rauen Mengen, ein Switch-Port tendiert jetzt schon hinsichtlich der Kosten in Richtung zweistelliger US$-Bereich und wird sich in nächster Zeit alle rund 18 Monate halbieren. Möchte man dann z.B. 2020 auf eine vollständige 10 GbE-Infrastruktur für die WLANs hochrüsten, kosten die Switches höchstens so viel wie heute 1 GbE-Switches. Sind dann aber Kabel und ältere Switches ungeeignet und von zu schlechter Qualität, wird es ärgerlich und teuer!

Der Report hat abgesehen von einer Einleitung fünf Kapitel. Im ersten Kapitel betrachten wir die Entwicklung der Anwendungen und die sich daraus ergebenden Anforderungen genauer. Das zweite Kapitel ist der aktuell neu verfügbaren WLAN-Technik, primär 802.11ac ab „Wave 2“, gewidmet. Kapitel drei beleuchtet die Entwicklung kleinerer Funkzellen, Mikrozellen oder Arbeitsplatz-Zellen im Millimeterwellen-Bereich (50 – 60 GHz-Bänder). Mit vergleichsweise geringem Aufwand können hier Multi-Gigabit Datenraten erzielt werden, aber eben mit einer recht begrenzten Ausdehnung der Zelle. Der bereits länger bestehende Standard IEEE 802.11ad wurde durch WiGig® zu neuem Leben erweckt. Was die Zukunft der drahtlosen Übertragung in der Zukunft ganz bedeutend prägen wird, ist die Entwicklung von LTE und LTE Advanced hin zu 5G Mobilfunk, die wir im vierten Kapitel darstellen. Hier wird die Messlatte für private Versorgungsinfrastrukturen immer höher gesetzt. Gleichzeitig könnte es vermehrt zu Konflikten kommen, wenn die Provider auch mit LTE in die bisher den lizenzfreien WLAN-Systemen vorbehaltenen Frequenzbereiche eindringen möchten. Diese Diskussion ist längst noch nicht ausgestanden. Das fünfte Kapitel stößt dann in den Bereich der in absehbarer Zukunft neu hinzu kommenden Techniken und Verfahren, auch im Hinblick auf die Koexistenz mit 5G, vor. Hierbei werden auch die sich jeweils im Rahmen der Technologien ergebenden Anforderungen an die Infrastruktur diskutiert.

Sparen Sie 50% als Teilnehmer an der Sonderveranstaltung Wireless und Mobility

Bestellung an kundenservice@comonsult-research.de

Ich bestelle den Report **"Wireless-Systeme der nächsten Generation"**

☐ zum Preis von 349,- € netto
zzgl. Versandkosten

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

Bestellen Sie über unsere Web-Seite

www.comconsult-research.de

Schwerpunktthema

Internet of Things – die vierte industrielle Revolution

Teil 3

Fortsetzung von Seite 1

Dipl.-Inform. Petra Borowka-Gatzweiler leitet das Planungsbüro UBN und gehört zu den führenden deutschen Beraterinnen für Kommunikationstechnik. Sie verfügt über langjährige erfolgreiche Praxiserfahrung bei der Planung und Realisierung von Netzwerk-Lösungen und ist seit vielen Jahren Referentin der ComConsult Akademie. Ihre Kenntnisse, internationale Veröffentlichungen, Arbeiten und Praxisorientierung sowie herstellerunabhängige Position sind international anerkannt.

3.2 IoT-Architektur des Industrial Internet Consortiums

Die "Industrial Internet Reference Architecture (IIRA)" des IIC datiert aus 06/2015. Ähnlich wie beim Europäischen Forschungsprojekt finden wir hier renommierte Namen, etwas praxisorientierter als beim Europäischen Forschungsprojekt: ABB, AT&T, Cisco Systems, Fujitsu, GE, IBM, Infineon, Intel, OMG, RSA/EMC, SAP SE, Symantec, MITRE und andere. Der Begriff "Industrial Internet" wird bei IIC gleichbedeutend mit IoT verwendet.

Die IIRA geht auf vier verschiedene Sichtweisen ein (siehe Abbildung 3.9):
- Geschäftsmodell (Business)
- Nutzung (Usage)
- Funktionalität (Functional)
- Implementierung (Implementation)

Funktionalität

Dieser Beitrag geht nachfolgend näher auf die funktionale und Implementierungs-Spezifikation ein. Das IIC unterteilt die Funktions-Architektur in verschiedene Domänen:

- Kontroll-Domäne
- Operations-Domäne
- Informations-Domäne
- Applikations-Domäne
- Geschäfts-Domäne

Zusammenhang und Interaktion der Domänen sind in Abbildung 3.10 dargestellt. Wie an der Abbildung klar erkennbar ist, finden Daten- und Kontrollflüsse innerhalb der funktionalen Domänen und zwischen den funktionalen Domänen statt. Grüne Pfeile zeigen, wie Datenflüsse über die Domänen hinweg zirkulieren, Rote Pfeile zeigen dasselbe für Kontrollflüsse. Andere horizontale Pfeile zeigen, wie innerhalb jeder Domäne Entscheidungs-Prozesse stattfinden, um Input zu verarbeiten und neue Daten oder Kontrollflüsse zu generieren.

Kontrolle, Koordination und Orchestrierung jeder funktionalen Domäne haben unterschiedliche Granularität und laufen mit unterschiedlichen Zeitzyklen. Betrachten Sie die Domänen von unten nach oben, nehmen die Interaktionen zu, die Zeitzyklen werden länger und die jeweiligen Auswirkungen werden mit hoher Wahrscheinlichkeit größer. Die Informationen werden breiter und vielfältiger, neue Informationen können abgeleitet werden und in breiteren Kontextzusammenhängen kann neue Intelligenz entstehen.

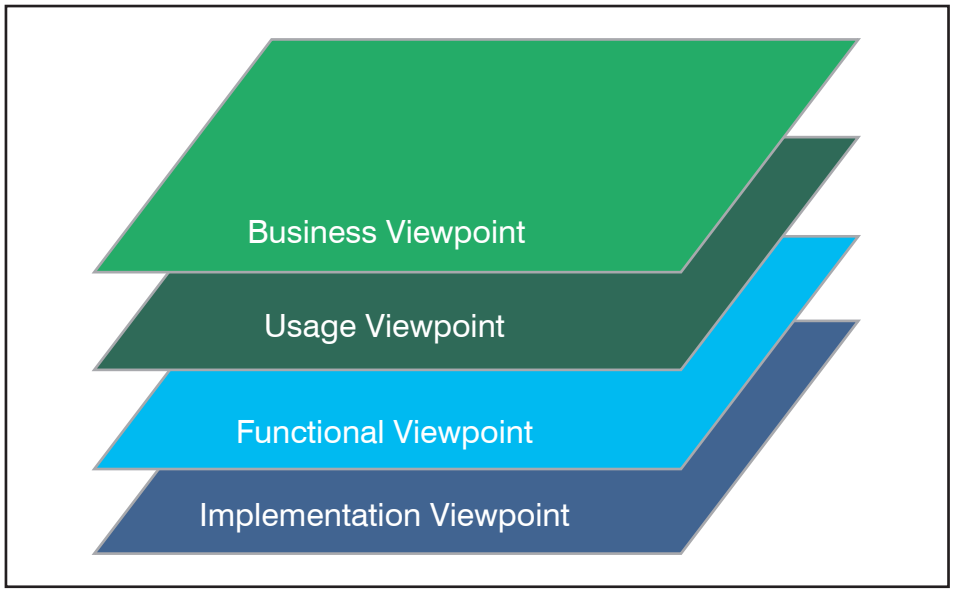


Abbildung 3.9: IIRA Architektur Sichtweisen

Quelle: IIC: Industrial Internet Reference Architecture S. 17

Implementierung

Die Implementierungs-Sichtweise befasst sich mit der technischen Repräsentation eines IoT / Industrial Internet Systems (IIS) und mit den Technologien und Systemkomponenten, die zur Implementierung der Funktionen und Aktivitäten der Funktionalität erforderlich sind. Eine IIS Architektur und die Auswahl der zu ihrer Implementierung verwendeten Technologien werden natürlich auch ebenso durch die geschäftliche Sichtweise beeinflusst, hierbei fallen insbesondere Kosten und Go-To-Market Zeitrestriktionen ins Gewicht, Geschäftsstrategie hinsichtlich des angestrebten Zielmarktes, relevante Regulierungs- und Konformitäts-Anforderungen sowie die geplante Erweiterbarkeit und Technologie-Evolution. Daher beschreibt die Implementierungs-Sichtweise folgende Punkte:

- die grundsätzliche Architektur eines IIS: seine Struktur, die Komponenten-Vertei-

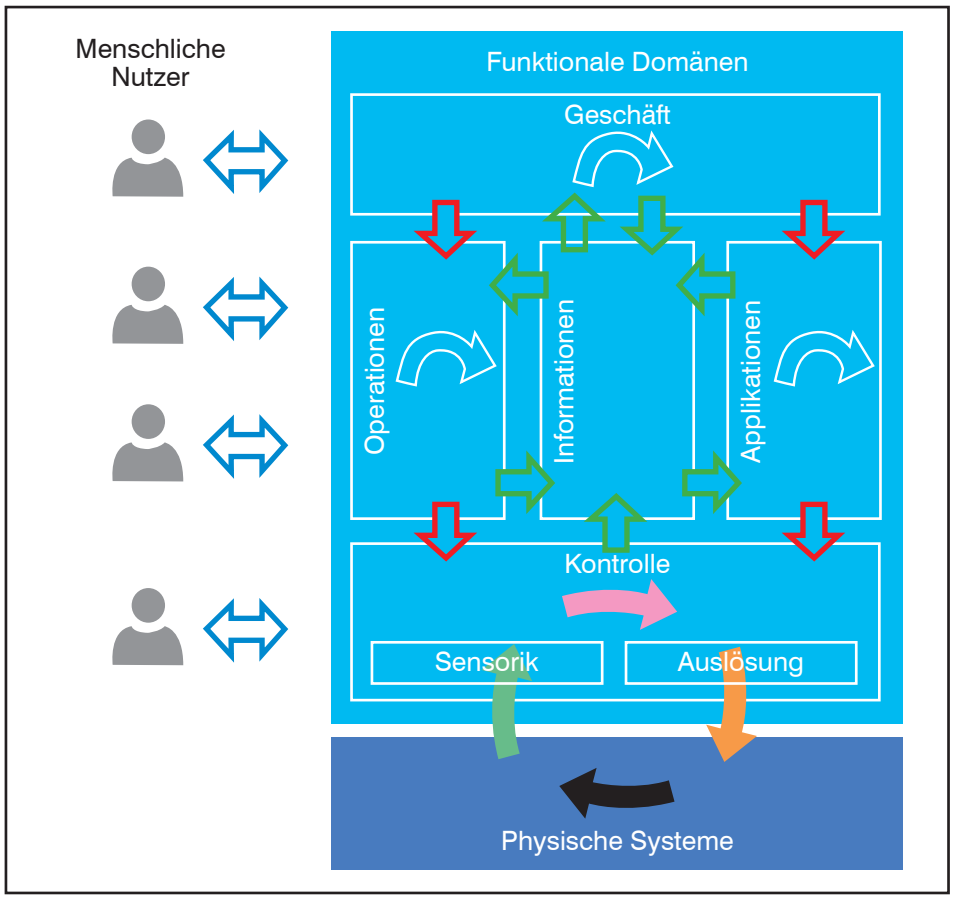


Abbildung 3.10: IIRA Funktions-Domänen

Quelle: IIC: Industrial Internet Reference Architecture S. 28

lung und die Topologie, die die Komponenten verbindet

- eine technische Beschreibung der Komponenten inklusive Schnittstellen, Protokolle, Verhalten und anderer Eigenschaften
- ein Mapping der Implementierungs-Aktivitäten, die aus der Nutzungssicht erkennbar sind, auf die funktionalen Komponenten sowie ein Mapping der Funktions-Komponenten auf tatsächlich implementierte Komponenten
- eine Implementierungs-Darstellung der Kern-Charakteristiken des Systems

Stimmige IIS Implementierungen folgen daher bestimmten wohlbekannten Architektur-Vorlagen wie

- 3-Tier Architektur
- Gateway-angepasste Edge Konnektivität und Management Architektur
- alternativ: Edge-Cloud Architektur (gegensätzlich zur Gateway-Architektur, da sie WAN-Konnektivität und Adressierbarkeit von Geräten und Objekte voraussetzt)
- Multi-Tier Speicher Architektur (zum Beispiel Leistungs-Speicher, Kapazitäts-Speicher, Archiv-Speicher)
- Architektur mit verteilten Analyse-Ebenen

Da die 3-Tier Architektur und Gateway-Architektur aktuell die etabliertesten sind, werden sie nachfolgend weiter detailliert.

Die 3-Tier Architektur

Die 3-Tier Architektur beinhaltet die in Abbildung 3.11 dargestellten Ebenen

- Edge
- Plattform
- Enterprise

Die **Edge-Ebene** sammelt Daten von den Edge Knoten. Sie nutzt dazu ein so genanntes Proximity Netzwerk. Diese Architektur-Ebene hat sehr unterschiedliche

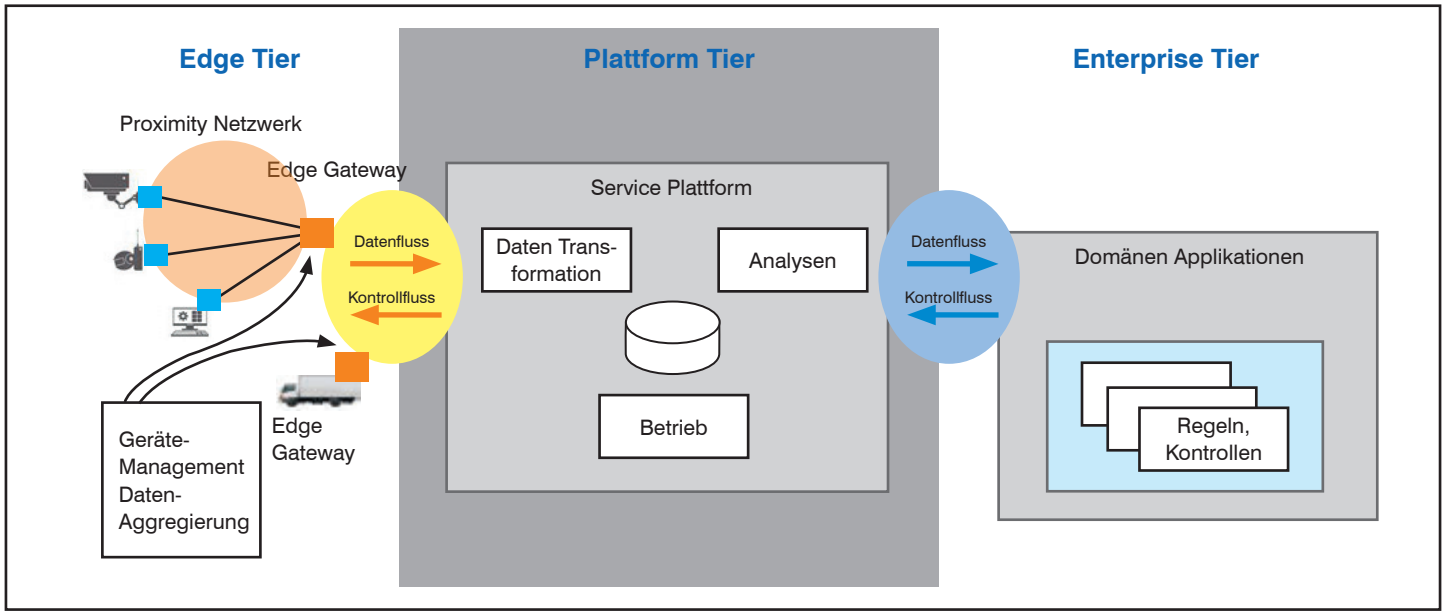


Abbildung 3.11: IIRA Funktions-Domänen

Quelle: IIC: Industrial Internet Reference Architecture S. 38

Internet of Things – die vierte industrielle Revolution - Teil 3

Ausprägungen hinsichtlich Verteilung, Lokationen, Aufgabenbereich und tatsächlich genutztem Proximity Netzwerk (vielfach lokale Funknetze).

Die **Plattform-Ebene** empfängt und verarbeitet Kontroll-Kommandos und leitet diese von der Enterprise Ebene zur Edge Ebene weiter. Die Plattform-Ebene konsolidiert Prozesse und analysiert Datenflüsse der Edge-Ebene und anderer Ebenen (zum Beispiel Enterprise-Ebene). Sie stellt Management-Funktionen für Geräte und Objekte bereit. Zudem bietet die Plattform-Ebene domänen-übergreifende Dienste wie Datenabfrage und Daten-Analyse an.

Die **Enterprise-Ebene** implementiert domänen-spezifische Anwendungen und Entscheidungshilfe-Systeme und stellt diese für Endnutzer, insbesondere auch Betriebsspezialisten bereit. Die Enterprise-Ebene empfängt Datenflüsse von der Plattform-Ebene und (weitergeleitete Datenflüsse) von der Edge Ebene. Sie erzeugt Kontroll-Kommandos für die Plattform- und Edge-Ebene.

Die Gateway-Architektur

Die Gateway-Architektur beinhaltet eine lokale Verbindungs-Lösung für den Edge-Bereich eines Industrial Internet / IoT Systems, bei der ein Gateway die Verbindungsbrücke zum WAN realisiert wie in Abbildung 3.12 gezeigt. Aus Sicht des WAN verhält sich das Gateway wie ein Endgerät, aus Sicht des Edge isoliert es das lokale Edge-Knoten-Netzwerk vom WAN. Diese Architektur erlaubt es, Operationen und Kontrolle, das heißt Edge Analyse und lokale Berechnungen lokal abzuhandeln.

Der Hauptvorteil dieser Architektur ist die reduzierte Komplexität, so dass solche IoT / Industrial Internet Systeme sowohl hinsichtlich Anzahl als auch Vernetzung der verwalteten Objekte vergleichsweise hoch skalieren können. Als Nachteil kann sich auswirken, dass diese Architektur sich nicht so gut für IoT / Industrial Internet Systeme eignet, in denen Objekte dergestalt mobil sind, dass sie keine stabilen Gruppen innerhalb der lokalen Netzwerk-Grenzen bilden können.

Typischerweise kann das Edge Gateway ebenso der Management-Punkt für Geräte und Objekte als auch darüber hinaus als Daten-Aggregationspunkt agieren, der bis zu einem gewissen Grad Bearbeitung und Analyse sowie Kontroll-Logik lokal implementiert.

Das Lokale Netzwerk kann verschiedene Topologien nutzen, insbesondere unterschieden nach Hub-and-Spoke und vermaschtem Netzwerk.

In der **Hub-and-Spoke** Topologie agiert das Gateway als Konzentrator, der eine Gruppe Edge Knoten an das WAN anbindet, das heißt insbesondere auch die Routing Funktionalität implementiert. Das Gateway seinerseits hat eine direkte Verbindung zu jedem Edge Knoten der gesamten Gruppe und handhabt eingehende Datenflüsse von den Edge Knoten zum Gateway und ausgehende Kontroll-Kommandos vom Gateway zu den Edge Knoten.

In einem vermaschten Netzwerk (Mesh Network), auch Peer-to-Peer Topologie genannt, gibt es ebenfalls ein Edge Gateway, das als Konzentrator und Router agiert, um eine Gruppe Edge Knoten an das WAN anzubinden. Allerdings können in dieser Topologie einige Edge Knoten ebenfalls Routing Funktionalität besitzen. Das führt dazu, dass die Routing-Pfade eines Edge-Knoten zu einem anderen und zum Gateway variieren und sich dynamisch ändern können. Diese Topologie eignet sich am besten, wenn ein großer Bereich für Anwendungen mit niedrigem Strombedarf und niedriger Datenrate abgedeckt werden soll und wenn sich in diesem Bereich Objekte mit stark eingeschränkten Ressourcen befinden, die über den ganzen Bereich (geografisch) verteilt sind.

Ein wichtiges Merkmal beider Topologien ist es, dass kein Edge Knoten direkt vom WAN aus zugreifbar sind. In diesem Sinn agiert das Gateway als ein singulärer Zugangspunkt zu den Edge Knoten gleichwie als Management-Punkt, der Routing und Adress-Translation-Funktionen bereitstellt.

Das Edge Gateway unterstützt mindestens die folgenden Funktionen:

- Lokale Verbindungsfunktionalität mit verkabelten seriellen Bussystemen und Funknetze über kurze Entfernungen (Short Range). Hier erleben wir mit fortlaufenden Entwicklungszyklen fortlaufend neue Technologien
- Netzwerk- und Protokoll-Anpassung, die verschiedenste Daten-Transfer-Modi zwischen den Edge Knoten und dem WAN unterstützt wie zum Beispiel asynchron, Streaming, ereignisgesteuert oder Store-and-Forward.

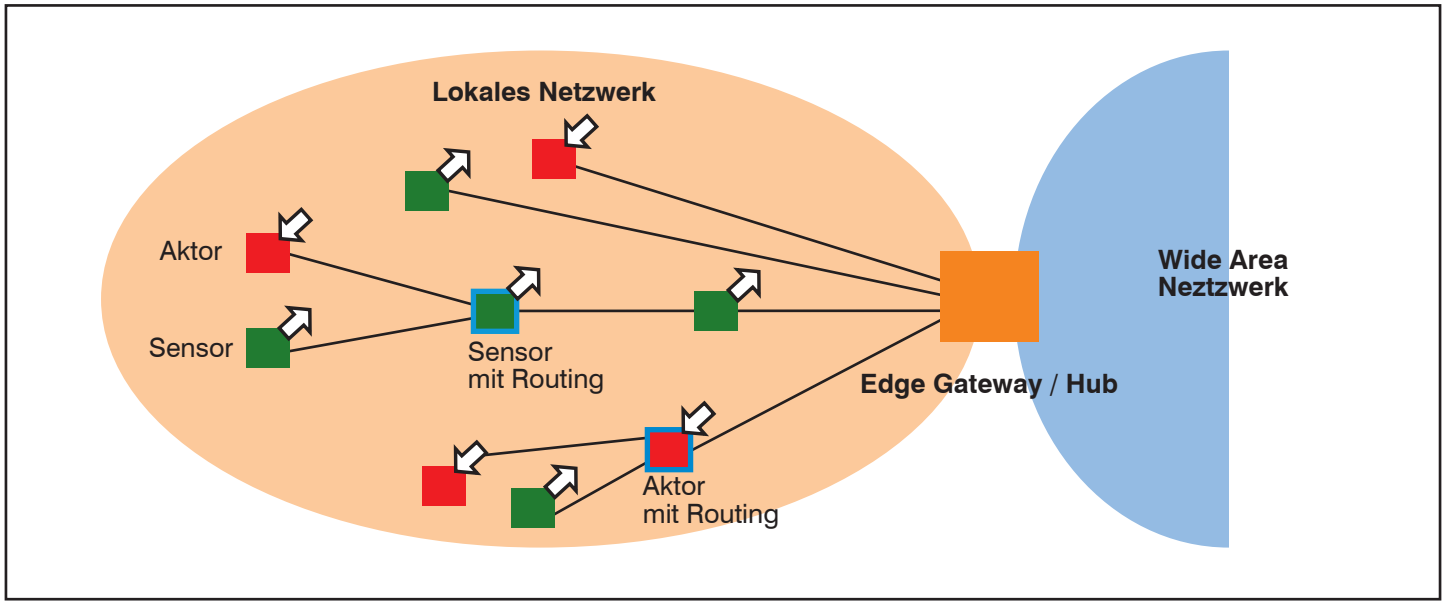


Abbildung 3.12: Gateway-Anpassung des Edge an das WAN

IC: Industrial Internet Reference Architecture S. 38

Internet of Things – die vierte industrielle Revolution - Teil 3

- Lokale Daten(vor)verarbeitung, insbesondere Aggregierung, Transformation, Filterung, Konsolidierung und Analyse.

- Kontroll- und Management-Punkt für Geräte und Objekte, der einerseits die Edge Knoten lokal administriert, andererseits als Agent fungiert, der Remote Management der Edge Knoten über das Weitverkehrsnetz ermöglicht.

- Standort-spezifische Entscheidungs- und Anwendungs-Logik, die innerhalb des lokalen Wirkungsbereichs ausgeführt wird.

Sicherheit

Um ein IoT System / IIS abzusichern, spezifiziert die Referenz-Architektur des Industrial Internet Consortiums eine Reihe von Sicherheits-Aspekten, die bei einer Implementierung zu berücksichtigen sind.

Ende-zu-Ende Sicherheit: Hierfür muss die Implementierung folgende Sicherheits-Features bereitstellen:

- geschützte Gerät-zu-Gerät Kommunikation

- Vertraulichkeit und Schutz der gesammelten Daten

- remote Zugang für Sicherheits-Management und Monitoring

- parallele Abdeckung verfügbarer und zukünftig neuer Technologien

- nahtlose Abdeckung sowohl der Informations-Technologie-Subsysteme (IT) als auch der operationalen Technologie-Subsysteme (OT) und Prozesse, ohne dabei in die operationellen Geschäftsprozesse einzugreifen

Dieser Ansatz erfordert es, die entsprechende Sicherheit schon beim Design vorzusehen, anstatt das so oft praktizierte und ebenso oft fehlgeschlagene "wir machen das im nächsten Schritt"-Paradigma heranzuziehen.

Legacy Systeme absichern: In industriellen Werksumgebungen, Krankenhäusern und Infrastruktur-Betrieben kommen allein aus Kostengründen vielfach "Legacy Systeme" zum Einsatz. Oft implementieren solche Endpunkte sehr begrenzte oder gar keine Sicherheits-Funktionalität hinsichtlich Datenbearbeitung und genutzter Protokolle. Die Sicherheit des Gesamtsystems erfordert es an dieser Stelle, das Angriffspotential dieser Legacy Systeme zumindest weitestmöglich zu minimieren.

Sicherheit der Architektur-Vorlage: Jede Architektur hat ihre eigenen spezifischen Sicherheits-Anforderungen und Sicherheits-Herausforderungen. In der 3-Tier Architektur beispielsweise gibt es vier kritische Bereiche und Prozesse, die abzusichern sind:

- Endpunkte
- Informations-Austausch
- Management und Kontrolle
- Verteilte Daten und Speicher

Soweit Legacy Systeme nicht selbst adäquat schützbar sind, können sie mittels Sicherheits-Gateway nach und von außen abgesichert werden (siehe Übersicht in Abbildung 3.13).

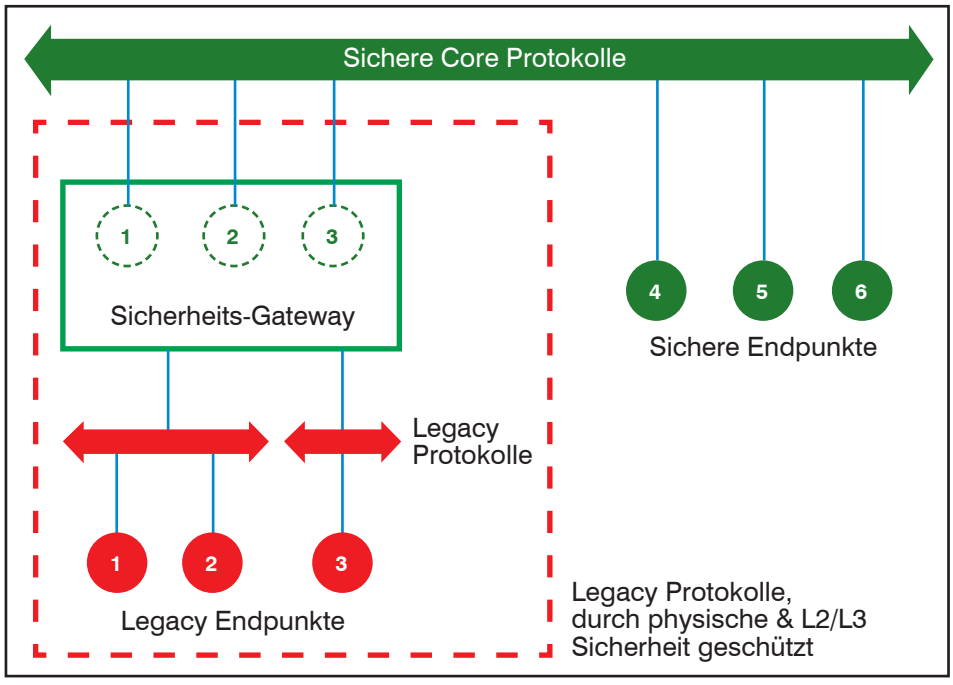


Abbildung 3.13: Sicherheits-Gateway zur Absicherung von Legacy Systemen
Quelle: IIC: Industrial Internet Reference Architecture S. 38

3.3 IoT Architektur aus der Praxis aktuell verfügbarer Lösungen

Die zuvor beschriebene Industrial Internet Reference Architecture des IIC lässt sich ziemlich gut auf die aktuell verfügbaren Lösungen abbilden. Praktisch betrachtet besteht ein IoT-System aus vier Komponenten (siehe auch Abbildung 3.14):

- Das "Ding" selbst – Geräte und Objekte, vielfach Sensoren / Aktoren

- Das lokale Netzwerk (funk- oder kabelgebunden), das zusätzlich ein Gateway beinhalten kann

- Das Internet

- Back-End-Dienste auf Basis von IoT-Plattformen, Enterprise-Datensystemen, oder einzelnen Nutzer-Zugängen via PC oder Mobilgerät

Aus Sicht der Hardware- und Software-Ingenieure gibt es somit ein wesentliches Element bei Internet of Things: miteinander vernetzte "Dinge" zu bauen. Hierbei spielen auf der Objekt-Ebene so genannte Embedded Systems (Computersysteme, die in Geräten, Anlagen und Maschinen eingebettet sind und spezielle Anwendungen abarbeiten) eine entscheidende Rolle bei der IoT Entwicklung.

In der Praxis beobachten wir zwei Kategorien der IoT Ausprägung:

- Industrielles IoT: Hier basiert das lokale Netzwerk auf den verschiedensten unterschiedlichen Technologien (wie weiter unten beim Thema Gateway beschrieben). Das IoT Objekt / Gerät wird typischerweise über ein IP-Netzwerk (dies kann durch ein Gateway verkörpert sein) an das globale Internet angebunden.

- Kommerzielles IoT: Hier basiert die lokale Kommunikation entweder auf WLAN/ Bluetooth (IEEE 802.11 / IEEE 802.15) oder Ethernet. Das IoT Objekt / Gerät kommuniziert typischerweise nur mit lokal erreichbaren Objekten / Geräten.

Betrachten wir als Beispiel ein Unternehmen aus der produzierenden Industrie und sein Fabrikgelände. Dies erfordert

Internet of Things – die vierte industrielle Revolution - Teil 3

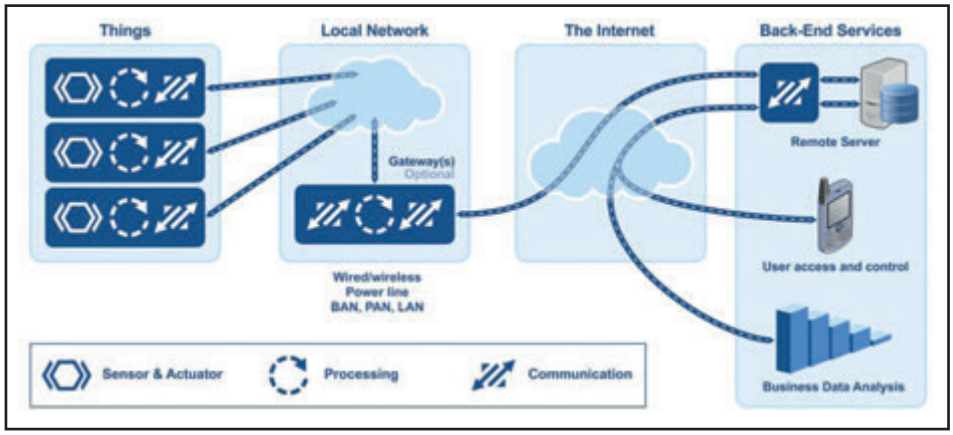


Abbildung 3.14: IoT Gesamt-Szenario Quelle: Micrium: Internet of Things

eine hohe Anzahl miteinander vernetzte Sensoren und Aktoren, die über das gesamte Gelände verteilt positioniert sind. Somit würde eine Funktechnik als LAN am besten passen. Ein solches Wireless Sensor Netzwerk (WSN) besteht dann aus einer Ansammlung verteilter Sensoren, die physische oder Umgebungs-Bedingungen wie Temperatur, Lautstärke oder Druck überwachen. Die Daten eines jeden Sensors werden von Knoten zu Knoten durch das Sensor-Netzwerk weitergeleitet. Ein typisches WSN Szenario zeigt Abbildung 3.15.

Soweit die WSN-Knoten kein IP, sondern proprietäre Protokolle nutzen, muss wie immer zur Kopplung unterschiedlicher Welten ein Gateway herhalten (WSN Edge), das den Übergang des WSN-Netzwerks zu einem unternehmensinternen IP-Netzwerk oder zum globalen Internet ermöglicht. Beispiele für Gateways sind AMR Cortex-M3/M4 oder Renesys RX600. Solche Gateways verbinden im Regelfall genau zwei disjunkte Netze – nämlich ein proprietäres und ein IP-Netz – und ermöglichen so Datenflüsse zwischen beiden Netzwerken. Hierfür müssen sie die üblichen Funktionen wie Switching und Routing, Protokoll-Konversion, Firewall und VPN, Sicherheit – und natürlich die auf der jeweiligen Netzseite implementierten Protokolle unterstützen. Auf der LAN-Seite sind dies Protokolle wie 6LoWPAN, ANT, Bluetooth, DASH7, ISA100, Modbus, Profinet, Wi-Fi, Wireless HART, Wireless M-Bus, Z-Wave, Zigbee, und andere mehr, auf der IP-Seite stehen Layer-2 Protokolle wie Ethernet, LTE/UMTS, IEEE 802.11 WLAN, Satellitenverbindungen PowerLink zur Auswahl. Eine Übersicht über denkbare IoT Gateway Szenarios zeigt Abbildung 3.16.

Diese Übersicht ist so zu verstehen, dass für die Verbindung jeweils zweier Welten mit der proprietären Lösung ein entsprechendes Gateway zur Anbindung an die Internet-Welt mitgeliefert wird. Nehmen wir ein Beispiel aus dem Bereich "Smart Homing": Verschiedene Energie- und andere Dienstleister installieren verschiedenste IoT Objekte wie Gaszähler, Wasserzähler, Stromzähler, Alarmsystem, medizinische Geräte und anderes mehr. Jeder Dienstleister wird dann sein eigenes Gateway dazustellen… Nicht gerade eine verlockende Vorstellung.

Die WSN Knoten, also Sensoren und Aktoren, sind Low-Cost Geräte – hiervon sind ja auch hohe Stückzahlen erforderlich. Sie arbeiten als Low-Power Geräte und laufen batteriebetrieben oder arbeiten sogar mit Energiegewinnung aus ihrer Umgebung (Stichwort Energy Harvesting). Ein WSN Knoten ist typischerweise ein Embedded System, das eine einzelne Funktion ausführt wie Temperatur-Überwachung oder Druckmessung oder Licht einschalten oder Motor einschalten etc.).

Wie sieht so ein Embedded System aus? Es läuft im Regelfall auf Basis eines Microcontrollers (MCU) und seine Software benötigt nur wenig Hauptspeicher. Einige Embedded Systeme verwenden ein ge-

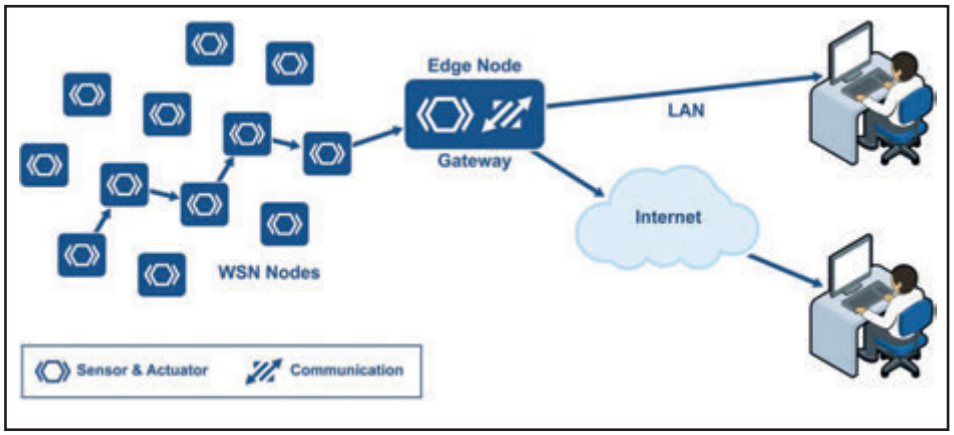


Abbildung 3.15: IoT Wireless Sensor Netzwerk Szenario Quelle: Micrium: Internet of Things

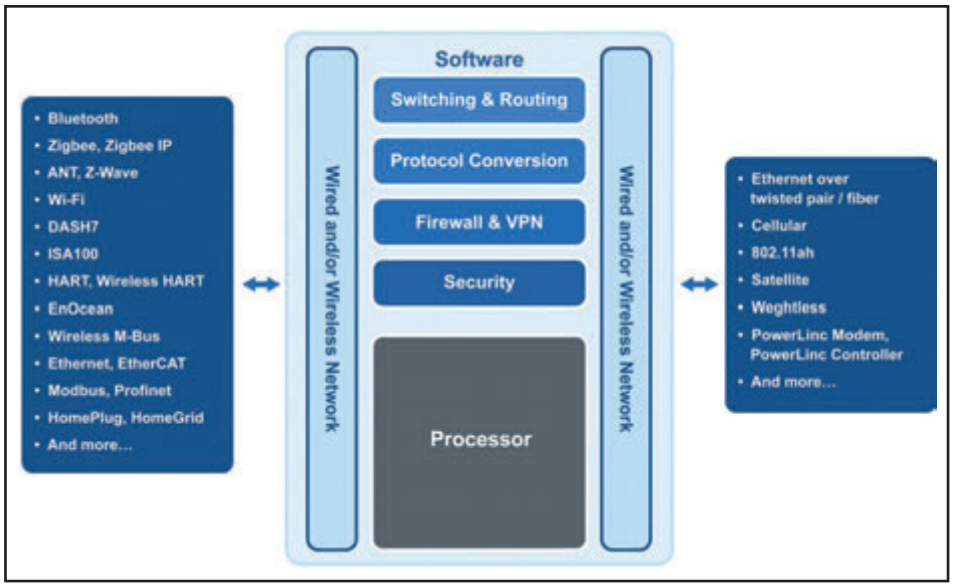


Abbildung 3.16: IoT IoT Gateway Szenarios Quelle: Micrium: Internet of Things

neral-purpose Betriebssystem (das kann auch Android oder Linux sein), meistens jedoch kommt für ein IoT Objekt ein spezieller Anwendungs-Prozessor mit zusätzlichen Funktionen wie dynamisches Laden des Applikations-Codes zum Einsatz. Letzteres wird oft als "Deeply Embedded System" bezeichnet. Die Deeply Embedded Systeme haben sich inzwischen von 8-Bit über 16-Bit zur 32-Bit MCU weiterentwickelt und nutzen Echtzeit-Betriebssysteme (RTOS), die mit einer Hauptspeichergröße von 1 MB einen BS-Kern, eine grafische Nutzerschnittstelle, ein Dateisystem, einen USB Stack, eine Netzwerk-Schnittstelle im System unterbringen (siehe auch Abbildung 3.17). RTOS Systeme sind vergleichsweise flexibel, insbesondere Diagnosefunktionen und die Einbettung neuer Funktionen vereinfachen sich dramatisch im Vergleich zu den früher verwendeten Foreground/Background Systemen (8-Bit, 16-Bit). Beispiele für MCUs sind ARM Cortex-M0 oder Renesas RL78, RX100.

Programmiert werden die Systeme mit Java, C oder C++. Java ist zwar aufwändiger als C/C++, ist aber aufgrund ca. einer halben Million verfügbarer "Embedded Software Ingenieure" und rund 9 Millionen weltweit verfügbarer Java Entwickler dennoch attraktiv für IoT Systeme (Beispiel: Java ME Embedded von Oracle als ARM-basierte SOC Architektur).

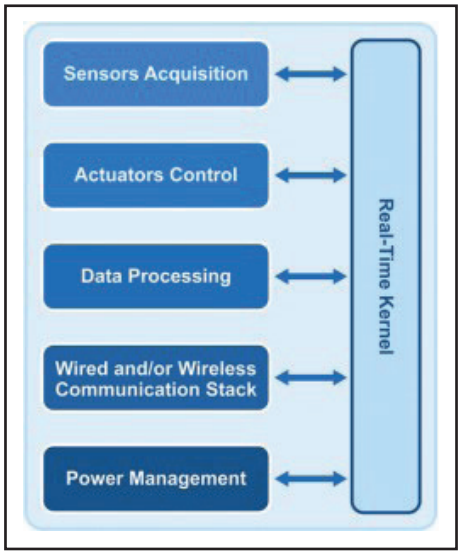


Abbildung 3.17: IoT Geräte-Architektur eines Embedded Systems

Quelle: Micrium: Internet of Things

IoT Plattformsysteme

IoT Plattformsysteme sind mittlerweile fester Bestandteil von IoT-Architekturen. Sie bringen im Rahmen der Backend-Dienste auf einer höheren Ebene als die zuvor beschriebenen Edge Komponenten verschiedene IoT-Welten zusammen. McKinsey zum Beispiel schätzt, dass 40 Prozent der gesamten IoT-Wertschöpfung daraus resultiert, dass verschiedene IoT-Systeme interoperabel zusammengebracht werden sollen und müssen. Um diese Herausforderung erfüllen zu können, bestehen IoT Plattformen aus verschiedenen Architektur- und Funktionsblöcken (wie in Abbildung 3.18 gezeigt):

- Konnektivität und Normalisierung
- Geräte-Management
- Verarbeitung und Aktions-Management
- Daten-Visualisierung
- Analytik und Zusatztools
- Externe Schnittstellen (APIs, SDKs, Gateways und ähnliches)
- Datenablage, Datenbank (flankierend zu allen oben genannten Bereichen)

Konnektivität und Normalisierung: Jede IoT Plattform passt als Basis-Funktion im Sinne von Konnektivität und Normalisierung verschiedene Protokollwelten und verschiedene Datenformate in ein "Software-Interface" ein. Dies ist die Voraussetzung dafür, dass die Plattform mit allen Objekten, die sie "bedient", interagieren und deren Daten korrekt einlesen kann. Erst nach einer solchen Normalisierung können alle Objekte und Daten, die eine IoT Plattform handhabt, überwacht, administriert und analysiert werden.

Das klingt jetzt ziemlich simpel, kann sich aber für den Software-Ingenieur zu einem Alptraum entwickeln – muss er doch für jeden individuellen Objekttyp eine Library anlegen. Das reicht von "ein industrieller Druck-Sensor schickt analoge Signale" bis zu "ein Wearable oder Smartphone Gerät sendet Daten und Grafiken". Zwar würde man erwarten, dass fortgeschrittene IoT-Geräte einer Plattform ein etabliertes API als Standard-Kommunikations-Schnittstelle anbieten, aber leider ist die Wirklichkeit noch immer davon entfernt, soll heißen: ein spezieller Objekt-Typ erfordert einen speziellen Software-Agenten,

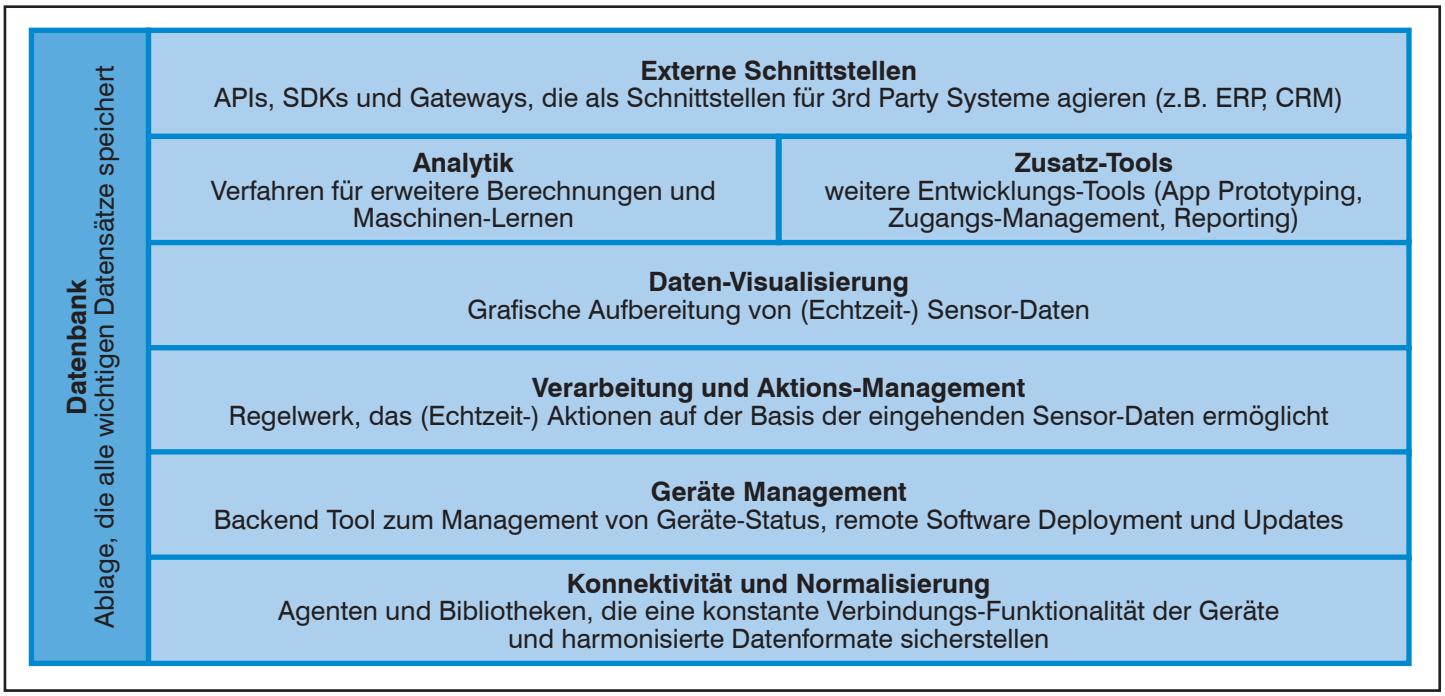


Abbildung 3.18: IoT Plattform-Architektur

Internet of Things – die vierte industrielle Revolution - Teil 3

der auf der IoT Plattform implementiert werden muss, um eine zuverlässige und stabile Kommunikation zwischen Plattform und verwalteten Objekten zu ermöglichen.

Geräte Management: Das Geräte Management-Modul der Plattform stellt sicher, dass alle verwalteten Objekte ordnungsgemäß arbeiten und dass ihre Betriebssoftware und Applikationen up and running sind. Hierzu führt die Plattform Funktionen wie Provisionierung, remote Konfiguration, Firmware/Software Updates oder auch Fehlerdiagnose durch. Stellen Sie sich nun eine Plattform vor, die Millionen verschiedener Geräte einer IoT-Lösung handhaben muss – schon wird klar, dass Massenaktionen und Automatisierung unverzichtbare Elemente einer IoT Plattform sind.

Datenbank: Das bringt uns direkt zur Plattform-Datenbank, die alle Daten aller Funktionsmodule geordnet ablegen und wieder abrufbar machen muss. Dies führt zu Datenbank-Anforderungen einer neuen Qualität:

- Das schiere Datenvolumen ist schon einmal riesig und oft kann nur ein Bruchteil der generierten Daten tatsächlich gespeichert werden.
- Die Datenformate verschiedener Objekte sind sehr unterschiedlich.
- Eine Reihe von IoT Anwendungsfällen erfordern die Analyse von Streaming-Daten, um Augenblicks-Entscheidungen treffen zu können. Dies erfordert sehr schnelle Zugriffszeiten.
- In einigen Fällen generieren Sensoren nicht-eindeutige oder auch falsche Daten. Hier muss die Plattform die Korrektheit und / oder Eindeutigkeit prüfen und gegebenenfalls herstellen können.

Aufgrund dieser hohen Anforderungen nutzen IoT Plattformen üblicherweise eine cloudbasierte Datenbank-Lösung, die über verschiedene Sensor-Netze verteilt arbeitet, die für "Big Data" skaliert und die sowohl strukturierte (SQL) als auch unstrukturierte (NoSQL) Daten ablegen und wieder abrufen kann.

Verarbeitung und Aktionsmanagement: Nachdem die Daten normalisiert und abgespeichert wurden, ermöglicht ein regelbasierter Event-Action-Trigger ihre Weiterverarbeitung und die Generierung "smarter" Aktionen auf der Basis der Sensor-Daten. Bleiben wir beim Beispiel Smart Homing: Ein Event-Action-Trigger kann so definiert werden, dass alle Lampen ausgehen, wenn eine Person das Haus verlässt. Die technische Realisierung erfolgt vielfach in Form einer IFTTT-Regel (If-This-Then-That), in unserem Beispiel könnte das sein: "Wenn das GPS Signal anzeigt, dass Sheilas Smartphone mehr als 10 Meter von ihrem Haus entfernt ist, dann schalte alle Lichter in diesem Haus ab."

Daten-Visualisierung: Dieses Modul einer IoT-Plattform wird oft unterschätzt. Aktuell ist es immer noch so, dass das menschliche Auge und Gehirn den meisten analytischen und regelbasierten Automaten überlegen sind. Daten-Visualisierung ist somit sehr wichtig, erlaubt sie doch dem Menschen vor der IoT Plattform, Muster zu erkennen und Trends einzuschätzen.

Analytik und Zusatz-Tools: Um aus den erhaltenen Daten das bestmögliche herauszuholen, erfordern viele IoT-Einsatzszenarien eine komplexe Analyse der Datenströme, die weit über bloßes Aktions-Management hinausgeht. Im Beispiel Smart Homing könnte ein Analytik-Modul Algorithmen bereitstellen, der der IoT Plattform zu lernen erlaubt, welche Licht- und Heizungs-Kombination zu welcher Tageszeit und im Verhältnis zu den draußen vorhandenen Wetterbedingungen vom Nutzer gewünscht und bevorzugt einzuregeln sind.

Zu den Zusatztools gehören vielfach Test- und Prototyping Werkzeuge. Das kann bis hin zu WYSIWYG-Editoren gehen, mit denen sich einfache Smartphone Apps entwickeln lassen, um IoT-Geräte zu visualisieren und zu kontrollieren. Ebenso gehören Tools für das Tagesgeschäft, das Reporting und den Management-Zugang der IoT-Lösung dazu.

Externe Schnittstellen: IoT Geschäftsideen werden selten isoliert und auf der grünen Wiese implementiert. In einem typischen Unternehmen ist es daher entscheidend, dass ein IoT System sich mit vorhandenen ERP Systemen, Management Tools, Produktionssystemen und dem IT-Ecosystem im weiteren Sinne integriert. Daher sind entsprechende APIs, SDKs und / oder Gateways ein Schlüsselfaktor für die Integration von Drittsystemen und weiterführenden Anwendungen.

Der Begriff "IoT Plattform" kommt sehr schillernd zur Verwendung. Grob betrachtet lassen sich Plattformen je nach implementierter Technologietiefe in drei verschiedene Stufen einteilen.

Stufe 1: Die Konnektivitäts-Plattform ist die einfachste Realisierung. Sie agiert als Datenkollektor und stellt einen einfachen Nachrichten-Bus bereit.

Stufe 2: Die Aktions-Plattform handhabt nicht nur die vernetzten Objekte sondern erlaubt auch Ereignis-Trigger, die spezifische Aktionen auslösen. In diese Klasse passt die zuvor beschriebene Beleuchtungs-Steuerung eines Hauses im Smart Homing Umfeld.

Stufe 3: Die Vollfunktions-Plattform geht über die Konnektivität und Aktionssteuerung hinaus, indem sie in verschiedenen Modulen verschiedene Dienste bereitstellt, Schnittstellen für Dritt-Anwendungen bietet und eine breite Vielfalt an

Protokollen und Standards unterstützt. Dieser Plattformtyp ist im Regelfall auch mit den höchst-skalierenden Datenbanken ausgestattet.

4. Internet of Things: Krieg der Protokolle

Die Vielfalt der aktuell miteinander wetteifernden Protokolle im Edge-Bereich – und der jeweiligen Industrie-Konsortien, die sie unterstützen – verspricht einen langen Zermürbungs-Krieg zwischen Unternehmen, die Protokolle als Mittel zum Zweck, in diesem Fall zur Marktkontrolle, betrachten. Mag die hehre und theoretische IoT Vision ein gemeinsames Protokoll für alle IoT Bedarfe sein, so besteht die eher trübe Wirklichkeit in Abhängigkeit der vertikalen Märkte und der Geografie leider aus vielen Protokollen, die auch von den speziellen Anforderungen der verschiedenen IoT Märkte und IoT Geräte geprägt sind.

M2M Kommunikation und Embedded Systeme als Wurzeln des IoT Marktes riefen eine Reihe von inzwischen als Legacy Protokollen betrachteten Verfahren auf den Plan, die ursprünglich separate vertikale Märkte bedienten, inzwischen jedoch einander bekämpfen, um selbst das einzig und allein überlebende Protokoll zu werden. Da kämpft ein 6LoWPAN gegen ein AMQP gegen ein CoAP gegen ein MQTT gegen ein XMPP und andere mehr. Wenn ich nun 25 Jahre zurückdenke, so hatten wir diese Situation in der IT-Kommunikation ganz ähnlich. Es stritten sich Apollo Domain, AppleTalk, DECnet, IPX, SNA, Trandsata, XNS und TCP um die Vorherrschaft und wir hatten Gateway-Produkte zwischen allen Welten. Heute sehen wir Hersteller und Open Source Ansätze, die Message Exchange Systeme für IoT vermarkten wollen (beispielsweise PrismTech, Mosquitto, RabbitMQ).

Der pragmatische Ansatz nimmt dagegen dem ganzen Getöse die Lautstärke und ersetzt die Vision durch schnöde Gateways – sprich ein Translation Layer zwischen den Protokollwelten, soweit dies erforderlich ist:

Im zweiten Schritt wurde vor 20 Jahren die Gateway-Welt darauf reduziert, alle Protokolle an TCP anzupassen. Dieser Ansatz ist vermutlich auch für IoT ganz pragmatisch anwendbar. Insofern vertrete ich die Überzeugung, dass der Single Protokoll Ansatz unter Berücksichtigung der Verschiedenheit der IoT Märkte, Anwendungen und Einsatzbereiche aktuell ein Irrtum ist: Die Anpassung vorhandener IoT "Legacy" Protokolle an TCP/IP und HTTP sollte nun für alle Beteiligten kein ganz so schweres Ungemach darstellen; bringt sie doch Welten zusammen, die recht unterschiedliche Kommunikations-Charakteristiken aufweisen (siehe auch Abbildung 4.1).

Während im Web Megabytes an Daten mit vergleichsweise ineffizienter Codierung und riesigem Overhead übertragen werden, die komplexe Parser und voll Internet-fähige Geräte erfordern, dreht sich das Internet der Dinge um die Übertragung weniger Byte mit effizient implementierten Geräten, effizienter Webanbindung und optimiertem IP Zugang.

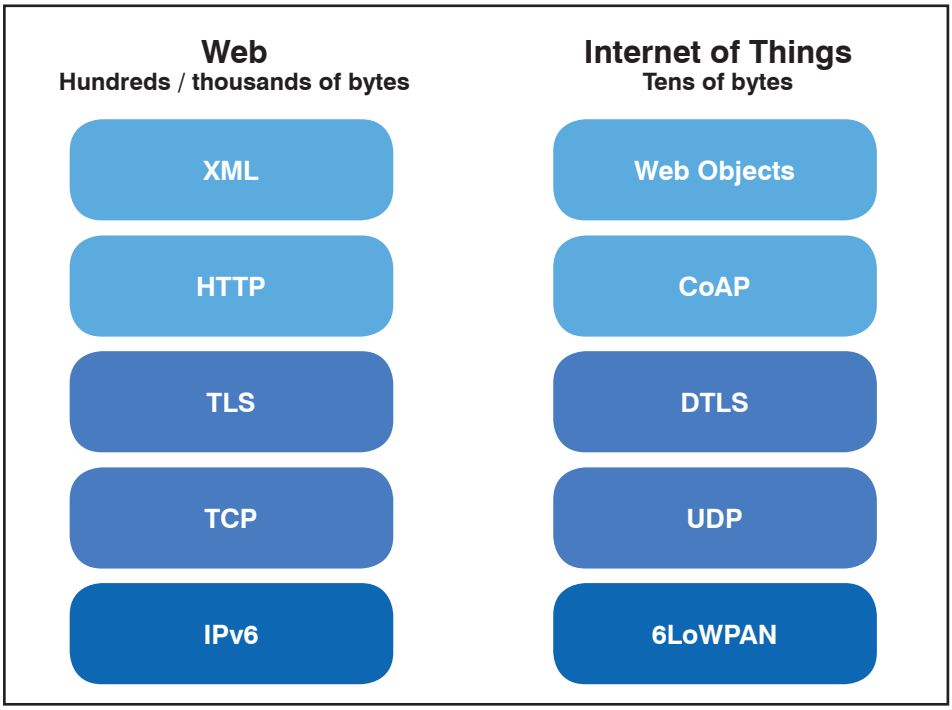


Abbildung 4.1: Vergleich der Web und IoT Protokoll-Stacks

Wenden wir uns daher einigen Legacy Protokollen zu (siehe die Übersicht in Abbildung 4.2), die Ihnen zumindest mittelfristig in der IoT Welt begegnen können.

6LoWPAN – Ipv6 over Low power Wireless Personal Area Networks

Low Power Betrieb ist im IoT-Umfeld interessant, da es effiziente Radios, Energie-Einsparung durch Stromrückgewinnung und die Nutzung vermaschter Funknetze für M2M Kommunikation im Langzeit-Betrieb ohne menschliche Interaktion ermöglicht. IPv6 ist im IoT-Umfeld unverzichtbar für remote Kontrolle, Datenübermittlung ins Internet und globale Kommunikation. Um beide Technologien nun sinnfällig zusammenzubringen, wurde die 6LoWPAN Arbeitsgruppe der IETF gegründet (und in 2014 wieder geschlossen), die 6LoWPAN mit einer Reihe RFCs standardisiert hat (RFC 7728, RFC 7388, RFC 7400, RFC 7668 "IPv6 over BLUETOOTH", RFC 7731, RFC 7973).

IoT Geräte, die Energie-Gewinnung betreiben, müssen ihre Rechenoperationen in der denkbar kürzesten Zeit durchführen, was bedeutet, dass die übermittelten Nachrichten so klein wie möglich sein müssen. Diese Anforderung beinhaltet deutliche Implikationen für das Protokoll-Design. 6LoWPAN erfüllt die entsprechenden Anforderungen recht gut und wurde von Herstellern wie ARM und Cisco für IoT Produkte implementiert. Es durchaus Chancen, den Protokoll-Wettbewerb bei WSN-Netzen für sich zu entscheiden.

6LoWPAN ist ein Adaptions-Layer, um IPv6 auf IEEE 802.15 (Bluetooth) Netzwerke aufzusetzen. Es leistet Anpassungs-Funktionen wie Header-Komprimierung (IP Header von 40 auf 12 Byte, UDP Header von 8 Byte auf 1 Byte), Fragmentierung, Ethernet Enkapsulierung, Routing und Autokonfiguration (für IPv6). 6LoWPAN Protokoll arbeitet nur im 2,4 GHz Frequenzbereich und hat eine Übertragungsrate von 250 kbps (!).

Abhängig von der Schicht, in der das Routing zum Einsatz kommt, gibt es zwei verschiedene Protokoll-Kategorien: Mesh-Under und Route-Over. Mesh-Under nutzt die MAC-Adresse bzw. eine 16-Bit Short Adresse, um Pakete weiterzuleiten, Route-Over nutzt dafür die IP Adressierung. Abbildung 4.3 und Abbildung 4.4 verdeutlichen das Weiterleitungs-Schema der jeweiligen Verfahren.

Mesh-Under: Da innerhalb eines Mesh-Under Netzwerkes das Routing für die IP Schicht transparent geschieht, stellen sich Mesh-Under Netzwerke als ein gemeinsa-

Standard Abkürzung	Protokoll-Name	Funktion
6LoWPAN	IPv6 over Low-Power Wireless Personal Area Networks	Die IETF Spezifikation für Encapsulierung und Compression von IP version 6 Paketen über Standard IEEE 802.15.4 Low-Rate Wireless Personal Area Networks (LR-WPANs).
AMQP	Advanced Message Queuing Protocol	Offenes Standard Application Layer Protokoll für Message-Oriented Middleware. Die definierten Funktionen von AMQP sind Nachrichten-Orientierung, Queuing, Routing (inkl. Point-to-Point und Publish-and-Subscribe), Zuverlässigkeit und Sicherheit – üblicherweise durch die Verbindungsserver implementiert.
CoAP	Constrained Application Protocol	CoAP ist ein Request/Response Application Layer Protokoll, das für den Einsatz in ressourcen-beschränkten Internet-Geräten wie Sensor Knoten gedacht ist. CoAP wurde so designed, dass es sich für eine vereinfachte Integration mit der Web Infrastruktur leicht in HTTP übersetzen lässt.
DDS	Data Distribution Service	Ein dezentralisiertes Messaging Protokoll, um intelligente Maschinen via Peer-to-Peer Kommunikation zu integrieren (M2M).
JMS	Java Message Service	Ein asynchrones API für zuverlässige Kommunikation zwischen zwei oder mehr Client Geräten (M2M).
MQTT	Message Queue Telemetry Transport	Publish/Subscribe Messaging Modell. Es passt für Verbindungen zwischen Außenstandorten, bei denen ein geringer Code Umfang erforderlich ist und/oder Netzwerk Bendbreite eingeschränkt oder kostenintensiv ist.
RESTful HTTP	HTTP auf Basis REST	Request/Response Client-Server Protokoll; besonders sicher, wenn im IoT Gerät nur ein Client implementiert wird, so dass es nur Verbindungen initiieren, aber keine eingehenden Verbindungen annehmen kann. Wird zum Beispiel bei Smart Homing im Smart Energy Profile 2 genutzt (entwickelt von Wi-Fi Alliance, ZigBee Alliance, HomePlug Alliance und HomeGrid Alliance)
XMPP	Extensible Messaging and Presence Protocol	Offene Technologie für Echtzeit-Kommunikation, kommt in einer Reihe Applikationen zum Einsatz, stellt generalisiertes Routing für XML Daten bereit. Skaliert sehr hoch, z.B. im Consumer Umfeld bei Waschmaschinen, Trocknern, Kühlschränken etc.
WebSocket	WebSocket Protokoll	Leistet full duplex Client-Server Kommunikation auf Basis einer einzelnen TCP-Verbindung. Es ist Teil der HTML5 Spezifikation und vereinfacht die Komplexität einer bidirektionalen Web-Kommunikation und ihres Managements deutlich.

Abbildung 4.2: Übersicht über IoT Protokolle

mes IP Subnetz dar. Die IP Routing Funktion innerhalb eines solchen Netzwerkes ist ausschließlich in einem Border-Router am Übergang zum Internet implementiert. Somit arbeitet das gesamte 6LoWPAN Funknetzwerk als eine gemeinsame Broadcast Domäne, die immanent das Funktionieren einiger IPv6 Protokoll-Mechanismen gewährleistet, welche Broadcast/Multicast-Mechanismen vorsehen wie zum Beispiel das Verfahren zur Vermeidung doppelter Adressen. Die hier gesendeten Nachrichten müssen an alle Teilnehmer des Netzes gesendet werden, was durch das Mesh-Under Routing Schema sichergestellt ist. Nachteilig ist die Generierung einer vergleichsweise hohen Netzwerklast durch geflutete Pakete. Mesh-Under bietet sich daher in lokal begrenzten und kleinen Netzwerken an. In Mesh-Under Netzwerken werden Fragmente bis zum Zielknoten weitergeleitet und erst dort zusammengesetzt, da Fragmentierung eine Funktion der IP-Schicht ist.

Route-Over: Route-Over Netzwerke implementieren das Routing in der IP Schicht, daher ist jeder Hop ein IP-Router. Das bedeutet aber auch, dass jeder Hop im Netzwerk über die Funktionalität eines IP Routers, wie z.B. Neighbor Discovery, verfügen muss. Route-Over ermöglicht somit die Nutzung von IP Funktionen wie IPv6 Routing, Dienste für Management und Konfiguration. Die Verwendung von IP Routing bedingt auch Unabhängigkeit von den unteren Schichten, somit vereinfacht es die Integration in leistungsfähige-

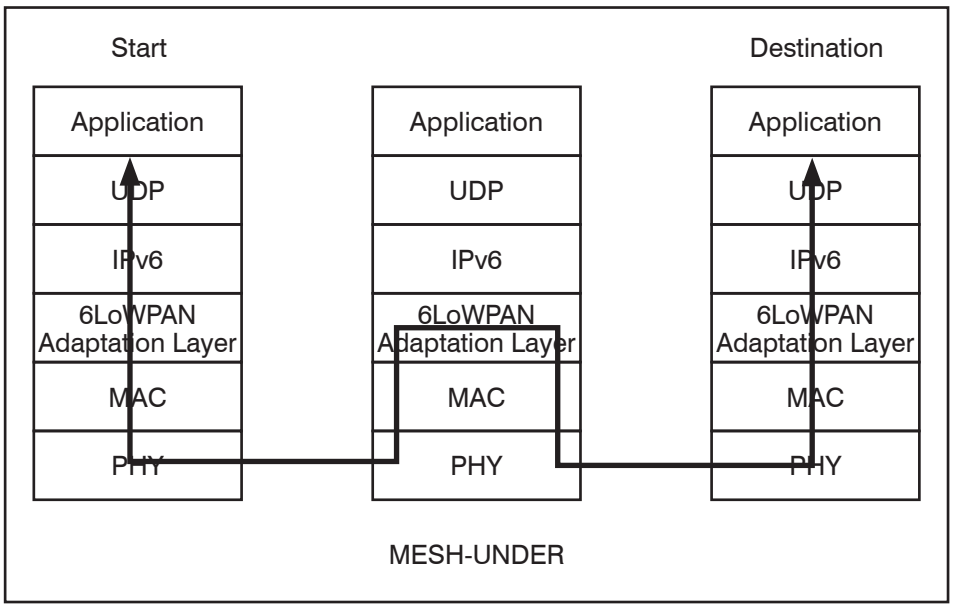


Abbildung 4.3: 6LoWPAN Routing Mesh-Under
Quelle: Grundlagen Enrico Lehmann: 6LoWPAN; dresden elektronik ingenieurtechnik gmbh 2012

re Netzwerke. Zudem werden Nachrichten nicht über Broadcast geflutet, sondern gezielt zu Knoten innerhalb der Funkreichweite gesendet. Route-Over Netzwerke leiten bei Fragmentierung jedes Fragment nur bis zum nächsten Hop weiter. Dort werden alle Fragmente zusammengesetzt, dann wird das Gesamtpaket ausgewertet, um den nächsten Zielknoten zu ermitteln. Bei Route-Over Netzwerken muss also jeder Hop alle Fragmente speichern, das bedeutet: er muss über genügend Ressourcen verfügen.

6LoWPAN verwendet den Mesh-Under Ansatz.

Zusammengefasst hat 6LoWPAN folgende Charakteristiken:

- geringe Sendezeit pro Nachricht
- Nachrichten so klein wie möglich
- immanentes Routing (Mesh-Under)
- angepasstes Protokollformat (Enkapsulierung, Headerkompression)
- geringe Bandbreite und lange Delays

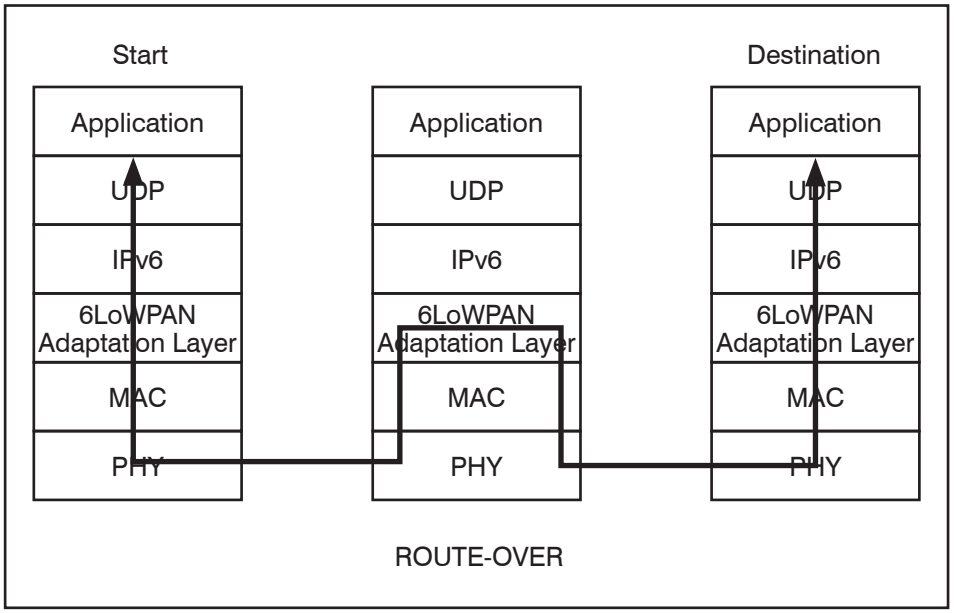


Abbildung 4.4: 6LoWPAN Routing Route-Over
Quelle: Grundlagen Enrico Lehmann: 6LoWPAN; dresden elektronik ingenieurtechnik gmbh 2012

AMQP - Advanced Message Queuing Protocol

AMQP entstand im Banken-Umfeld und ist besonders auf die Abarbeitung von Warteschlangen und die Bereitstellung von Routing Funktionen fokussiert. Dieses Protokoll kann Tausende von zuverlässigen Transaktionen in einer Warteschlange abarbeiten. Es ist eine auf Nachrichten ausgerichtete Middleware, die Transaktions-Nachrichten zwischen Servern sendet. Kernfunktion von AMQP ist es, keine Nachrichten zu verlieren, das heißt verlustfrei zu arbeiten.

Die Kommunikation verläuft von so genannten Publishern zu Austausch-Knoten (Exchanges) und von den dortigen Warteschlangen zu den Subscribern. In allen Fällen basiert die Kommunikation auf TCP und leistet somit eine strikte zuverlässige Punkt-zu-Punkt Verbindung. Endpunkte / Clients müssen den Erhalt jeder Nachricht quittieren. Ihrer Entstehung aus dem Bankenumfeld geschuldet, sorgt die AMQP Middleware dafür, dass alle Nachrichten mittels Tracking nachverfolgt und gesichert abgeliefert werden, sogar über Ausfälle und Reboots hinweg.

CoAP - Constrained Application Protocol

Obwohl Web Protokolle für IoT Geräte verfügbar und nutzbar sind, sind sie für viele IoT Anwendungen viel zu aufwändig. An dieser Stelle kommt das CoAP Protokoll ins Spiel – wie der Name schon sagt, ist es für Systeme nutzbar, die sehr restringierte Ressourcen haben wie niedriger Energiebedarf und Netzwerke mit starken Bandbreitenbeschränkungen, zum Beispiel Wireless Sensor Knoten in einem WSN-Netz.

CoAP ist ein so genanntes RESTful Protokoll, seine Semantik ist an HTTP ausgerichtet und unterstützt ein Eins-zu-Eins-Mapping mit HTTP, sowohl von CoAP zu HTTP als auch umgekehrt. So ist es für die Nachrichten-Konvertierung von und nach HTTP optimiert.

CoAP wird beispielsweise von Geräten genutzt, die aus der Umgebung Energie gewinnen oder batteriebetrieben arbeiten. Einige Eigenschaften von CoAP:

- Es setzt auf UDP auf
- Daher sind einige TCP Funktionen auf der CoAP Schicht nachgebildet, zum Beispiel kennt CoAP zu bestätigende (Confirmable) und nicht zu bestätigende (non-confirmable) Nachrichten
- Anfragen (Requests) und Antworten (Responses) werden asynchron mittels CoAP Nachrichten ausgetauscht
- Header Overhead und Parsing Komplexität sind minimiert
- Alle Header, Funktionen und Status-Codes sind binär codiert, um Overhead einzusparen
- Anders als bei HTTP, ist die Möglichkeit, CoAP Antworten im Cache zu halten, nicht abhängig von der Anfrage-Methode, sondern vom Antwort-Code
- CoAP erfüllt alle Anforderungen eines extremen, das heißt äußerst schlanken "Lightweight" Protokolls und unterstützt Dauer-Verbindungen.
- Insgesamt ist CoAP, insbesondere auf Basis eines Web-Hintergrunds, relativ leicht implementierbar.

MQTT - Message Queue Telemetry Transport

MQTT ist ein Open Source Protokoll für Systeme mit beschränkten Ressourcen in Netzen mit niedriger Bandbreite und hohem Delay. Daher ist es besonders bandbreiten-effizient, Daten-agnostisch und beinhaltet eine ständige Session-Überwachung. Der Code-Umfang ist minimal, somit minimiert CoAP die Ressourcen-Anforderungen in den IoT-Geräten, stellt aber gleichzeitig einen zuverlässigen Dienst sicher und liefert zumindest ansatzweise Quality-of-Service Funktionalität.

MQTT zielt auf sehr große Netze mit sehr vielen sehr kleinen Geräten ab, die von einem Backend-Server über Internet überwacht und kontrolliert werden müssen. Es ist vollständig Client-Server-orientiert, das heißt es gibt bei MQTT keine Peer-Kommunikation zwischen IoT-Geräten. Insbesondere wird kein Multicasting an Geräte-Gruppen unterstützt.

MQTT ist eine extrem einfaches Protokoll mit nur ganz wenigen Kontroll-Optionen.

XMPP - Extensible Messaging and Presence Protocol

XMPP entstand ursprünglich aus dem UC-Umfeld, um nahtlose peer-to-peer UC-Interaktion und Kommunikation zwischen Menschen zu ermöglichen, ins-

besondere für Chat (Instant Messaging) und Erreichbarkeits-Dienste: Dies war viele Jahre lang der Fokus der XMPP Protokoll-Suite. Durch Gründung der XSF wurde die Kommunikation via XMPP offen und kontrollierbar gehalten.

Auf der M2M Seite gab es lange Zeit nichts Vergleichbares, und da XMPP sich als "Lightweight Middleware" und als generalisiertes Routing von beliebigen XML-Daten etabliert hat, ist es auch in den IoT-Markt hineingewachsen. Es skaliert sehr hoch und eignet sich damit für IoT-Szenarien im Consumer Umfeld mit Waschmaschinen, Trocknern, Kühlschränken und ähnlichen Geräten.

Abkürzungen

6LoWPAN	IPv6 over Low power Wireless Personal Area Network
A/V	Audio / Video
ABB	Asea Brown Boveri
ACL	Access Control List(e)
ALE	Alcatel Lucent Enterprise
ALG	Application Layer Gateway
AMQP	Advanced Message Queuing Protocol
ANSI	American National Standards Institute
ANT	Trademark Dynastream (ANT Protokoll)
API	Application Programming Interface
ARM	Acorn RISC Machine (Prozessoren)
ARM	Architectural Reference Model (EU IoT-A)
AT&T	American Telephone & Telegraph
B2B	Business to Business
B2BUA	Back-to-Back User Agent
BAN	Body Area Network
BLE	Bluetooth Low Energy
BRI	Basic Rate Interface
BYOD	Brind Your Own Device
CAC	Call Admission Control
CAGR	Compound Annual Growth Rate
CAPEX	CAPital EXpenditure
CES	Consumer Electronics Show
CoAP	Constrained Application Protocol
CoRE	Constrained RESTful Environments
CPU	Central Processing Unit
CRM	Customer Resource Management
DASH7	D7A Dash7 Alliance Protocol
DC	Data Center
DDoS	Distributed Denial of Service
DDS	Data Distribution Service
DEC	Digital Equipment Corporation
DMZ	Demilitarized Zone
DoD	Department of Defense
DoS	Denial of Service
DSP	Digital Signal Processor
DTLS	Datagram Transport Layer Security
EDGE	Enhanced Data Rates for GSM Evolution
EMC	Egan,Marino, Connelly und Curley ("EMC2") Corporation
ERP	Enterprise Resource Planning
ESBC	Enterprise SBC
EtherCAT	Ethernet for Control AutomationTechnology
ETSI	Euopean Telecommunications Standards Institute
E-UTRA	Evolved UMTS Terrestrial Radio Access
FG	Functional Group
FMC	Fixed Mobile Conversion
FW	Firewall
GE	General Electric
GSM	Global System for Mobile Communications
GUI	Graphical User Interface
GW	Gateway
HA	High Availiability
HAN	Home Area Network
HART	Highway Addressable Remote Transducer
HMR	Header Manipulation Rules
HTML	Hypertext Markup Language
HTTP	Hyper Text Transfer Protocol
IaaS	Infrastructure as a Service
IBM	International Business Machines Corporation
IBM	International Business Machines
ICE	Interactive Connectivity Establishment
ICT	Informations and Communications Technology
ID	Identifikator
IDC	International Data Corporation
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IFTTT	If-This-Then-That
IIC	Industrial Internet Consortium
IIoT	Industrial Internet of Things
IIRA	Industrial Internet Reference Architecture
IIS	Industrial Internet System
IM	Instant Messaging
IMS	IP Multimedia Subsystem
IoT	Internet of Things
IP	Internet Protocol
IPsec	IP Security
IPSO	IP Smart Objects
IPv6	Internet Protocol Version 6
IPX	Internetwork Packet eXchange
IRF	Intelligent Resilient Framework (HP)
ISA	International Society of Automation 8isa!==9
ISDN	Integrated Services Digital Network
IS-IS	Intermediate System-to-Intermediate System Protocol
ISO	International Organization for Standardization
ISP	Internet Service Provider
ISUP	ISDN User Part
IT	Informations-Technologie
ITSP	Internet Telephony Service Provider
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union – Telecommunication Standards
JMS	Java Message Service
JSON	JavaScript Object Notation
L2/L3	Layer-2/ Layer-3
LACP	Ling Aggregation Control Protocol
LAG	Link Aggregation Group (IEEE 802.3ad)
LAN	Local Area Network
LB	Load Balancing
LCR	Least Cost Routing
LED	Light Emitting Diode
LLN	Low Power and Lossy Network
LoPWAN	Low Power Wireless Area Network
LPWA	Low Power Wide Area
LTE	Long Term Evolution
LTE-A	LTE-Advanced
LWL	Lichtwellenleiter
M2M	Machine to Machine
MAC	Media Access Control
M-Bus	Meter-Bus (Feldbus)
MCU	Micro Controller Unit
MITRE	Massachusetts Institute of Technology Research Establishment
MOM	Message-Oriented Middleware
MoR	Mid of Row
MP	Multiprotocol / Multipath
MPLS	Multi Protocol Label Switching
MPP	Massively Parallel Processing
MPU	Micro Processor
MQTT	Message Queue Telemetry Transport
MRP	Metro Ring Protocol
ms	Millisekunden
NAC	Network Access Control
NAT	Network Address Translation
NEC	Nippon Electric Company
NETCONF	Network Configuration
NFC	Near Field Communication
NFV	Network Function Virtualisation
NIC	Network Interface Card (Coupler)
NNI	Network to Network Interface
OCSP	Online Certificate Status Protocol
OFDM	Orthogonal Frequency-Division Multiplexing
OMG	Object Management Group
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
OT	Operational Technology
OTS	Off the Shelf
PAN	Personal Area Network
PBX	Private Branch eXchange
PC	Personal Computer
PCRF	Policy an Charging Rules Function

PoC	Proof of Concept
POP	Point of Presence
PRI	Primary Rate Interface
PSTN	Public Switched Telephony Network
PSU	Power Supply Unit
PYANG	in Python geschriebenes YANG
QoS	Quality of Service
QSFP	Quad SFP
QSIG	Q-interface SIGnalling protocol
REST	Representational State Transfer
RFC	Request For Comment; TCP/IP Standard-Dokument
RFC	Request for Comment
RMON	Remote Network Monitoring MIB (SNMP)
ROLL	Routing Over Low power Lossy networks
RSA	Rivest, Shamir, Adleman
RSTP	Rapid Spanning Tree Protocol
RTC	Real Time Communications
RTCP	Real Time Control Protocol
RTC-Web	Real-Time Communication - Web
RTOS	Real-Time Operating System
RTP	Real-time Transport Protocol
SAP	SystemAnalyse und Programmentwicklung
SBC	Session Border Controller
SDK	Software Development Kit
SDN	Software-Defined Networking
SDP	Session Description Protocol
SEP	Stable Election Protocol
SFP	Small Form-Factor Pluggable
SIMPLE	SIP for Instant Messaging and Presence Leveraging Extensions
SIP	Session Initiation Protocol
SIP-I	SIP - ISUP Interworking
SIPREC	SIP RECording
SLA	Service Level Agreement
SMCP	Short Message Control Protocol
SNA	Systems Network Architecture
SOAP	Simple Object Access Protocol
SOC	System On a Chip
SP	Service Provider
SPB	Shortest Path Bridging
SPBM	Shortest Path Bridging MAC
SPBV	Shortest Path Bridging VID
SPOF	Single Point Of Failure
SQL	Stuctured Query Language
SRTP	Secure RTP
SS7	Signaling System #7 / Signalisierungssystem Nummer 7
STUN	Simple Traversal of UDP through NAT
TCP	Transmission Control Protocol
TCSPI	Telephony Conferencing Service Provider Interface
TDM	Time Division Multiplexing
TE	Traffic Engineering
TISPAN	Telecommunications and Internet converged Services and Protocols for Advanced
TK	Telekommunikation
TLS	Transport Layer Security
TLV	Type – Length – Value
TRILL	TRansparent Interconnection of Lots of Links
TTL	Time To Life
UC	Unified Communications
UCC	Unified Communications and Collaboration
UDP	User Datagram Protocol
UHA	Ultra High Available
ULP	Ultra Low Power
UMTS	Universal Mobile Telecommunications System
UNI	User to Network Interface
URI	Universal Resource Identificator
USB	Universal Serial Bus
VDI	Verein Deutscher Ingenieure
VDOS	Video Denial of Service
VDX	Virtual Document eXchange
VID	VLAN ID
vLAG	Virtual Link Aggregation Group
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNI	VXLAN Network Identifier
VoIP	Voice over IP
VPN	Virtual Private Network
VSL	Virtual Switch Link (Cisco)
VSS	Virtual Switching System
VXLAN	Virtual Extensible VLAN
VXLAN GPE	Generic Protocol Extension for VXLAN
W	Watt
WAN	Wide Area Network
WEF	World Economic Forum
WLAN	Wireless LAN
WSN	Wireless Sensor Network
WYSIWYG	What You See Is What You Get
XML	eXtensible Markup Language
XMPP	eXtensible Messaging and Presence Protocol
XNS	Xerox Network Systems
YANG	Yet Another Next Generation

Links

www.ietf.org
www.uidcenter.org

Literatur

- EU FP7, Francois Carrez (Editor): Internte of Things – Architecture IoT-A, D1.5 – Final architectural reference model fort he IoT v3.0; 15.07.2013

- Session Boder Controllers: A Primer; Oracle White Paper 2013

- Market Guide for Enterprise SBC; Gartner, Juni 2014

- John Hardwick: Session Border Controllers, Enabling The VoIP Revolution; Data Connection Whitepaper, 2005

Im nächsten Teil lesen Sie:

- IoT Roadmap und Trends

Standpunkt

Schluss mit lustig: Eine umfassende und verbindliche Cyber-Sicherheitsstrategie muss her

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.

Auch wenn es sich am Ende nur als Kollateralschaden herausgestellt hat, der Angriff auf die Router der Telekom, der am 28. November ca. 900.000 Router zeitweise außer Kraft gesetzt hat [1], gibt mehr als zu denken, und es muss über Konsequenzen nachgedacht werden.

Bei diesem Angriff ist nach aktuellem Kenntnisstand folgendes passiert: Derzeit werden eine Vielzahl von Systemen im Internet (und nicht nur die betroffenen Router der Telekom) im Minutentakt auf Port 7547 angegriffen. Über diesen Port erfolgt normalerweise die Fernwartung von Routern für den Internetzugriff durch den jeweiligen Internet Service Provider über das standardisierte Protokoll TR-069. Dabei versucht der Angreifer eine spezielle (seit mehreren Wochen bekannte) Schwachstelle von gewissen Zyxel-Routern auszunutzen, um auf dem hier verwendeten Linux-Betriebssystem einen Trojaner zu installieren, der den Router zu einem willenlosen Mitglied eines Botnet macht. Nur waren die angegriffenen Router der Telekom von einem anderen Hersteller und setzten auch ein anderes Betriebssystem ein. Die Schwachstelle, die der Angreifer eigentlich ausnutzen wollte, gibt es hier nicht. Trotzdem reicht ein mehrfacher Angriffsversuch aus damit die betroffenen Router ihre Arbeit einstellen, und aus dem eigentlichen Angriffsversuch ist als Kollateralschaden ein großflächiger Denial of Service (DoS) geworden.

Es ist davon auszugehen, dass die aktuell laufenden Angriffe auf den TR-069-Port von einem Botnet aus infizierten Routern ausgehen, das verdächtige Ähnlichkeiten zum Mirai Botnet hat, welches aus dem Internet of Things (IoT) für den kürzlich erreichten Distributed-DoS-Rekord im Terabit-Bereich verantwortlich war. Die Tatsache,

dass das Mirai Botnet inzwischen bereits eine Handelsware auf dem Cyber-Crime-Marktplatz ist [2], zeigt die hiervon ausgehende Gefahr besonders plakativ. Damit ist klar: Das IoT hat sich erschreckend schnell zu einer größten Gefährdung des Internets entwickelt!

Analysiert man den Vorfall, fällt zunächst auf, dass ein effektives Schwachstellenmanagement diesen Vorfall wahrscheinlich vermieden hätte, denn das Problem war schon länger bekannt und der genutzt Port hätte nicht vom gesamten Internet aus frei zugreifbar sein müssen. Dies hätte jedoch nicht die Ursache, nämlich den Angriffsversuch selbst verhindert und genau hier liegt das Problem, denn die Systeme im IoT, von denen Angriffe ausgehen können, bleiben uns noch länger erhalten. So wichtig ein Schwachstellenmanagement als einer der Kernprozesse der Informationssicherheit ist, wir müssen an die Ursachen ran.

Wir benötigen für Geräte, die an das Internet angeschlossen werden, dringend verbindliche Standards und entsprechende Gütesiegel bzw. Zertifikate hinsichtlich Softwarequalität und Informationssicherheit sowie eine gemeinsame, übergreifende Cyberstrategie. Diese Strategie muss umfassend sein und nicht nur die skizzierten Angriffe aus dem IoT betrachten, sondern beispielsweise auch die systematische Beeinflussung von Meinungen durch Social Media Bots.

Dies hilft aber nichts, wenn nicht auch seitens der Gesetzgebung eingegriffen wird. Der international anerkannte Sicherheitsexperte Bruce Schneier hat die Angriffe aus dem IoT mit einer Umweltverschmutzung verglichen, der nur mit einer konsequenten Regulierung begegnet werden kann [3]. Dabei sind nicht nur die Hersteller und Dienstanbieter, sondern auch alle Internetnutzer zu einer Verantwortlichkeit zu verpflichten, denn die Botnets, die uns aus dem IoT im Moment besonders ärgern, haben unter anderem auch ihre Wurzeln in durch den Nutzer nicht geänderten Standardpasswörtern.

Inzwischen sind auch bei uns entsprechende Stimmen aus der Politik laut geworden und die im November von der Bundesregierung beschlossene „Cyber-Sicherheitsstrategie für Deutschland 2016“ ist ein Licht am Horizont. Nur ist es bei Cyber Crime auch hier wie mit der Umweltverschmutzung, die nicht vor Landesgrenzen halt macht. Wenn wir nicht dauerhaft mit den zuletzt vorgekommenen Angriffen (und viel Schlimmerem) leben wollen, brauchen wir eine internationale Regulierung des Cyber-Raums und entsprechende Abkommen, was leider in der aktuellen politischen Lage alles andere als realistisch ist.

Verweise

[1] Siehe z.B. http://www.spiegel.de/netzwelt/gadgets/telekom-hacker-angriff-nicht-die-telekom-router-waren-das-ziel-a-1123805.html und https://www.telekom.com/de/medien/details/mythos-offene-schnittstelle-was-wirklich-geschah-445232

[2] Siehe https://www.bleepingcomputer.com/news/security/you-can-now-rent-a-mirai-botnet-of-400-000-bots/

[3] Siehe https://www.schneier.com/essays/archives/2016/11/testimony_at_the_us_.html

Zweitthema

Das PSTN geht – die Vielfalt kommt

Fortsetzung von Seite 1

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

Um jetzt beim Beispiel Fax zu bleiben, gibt es dazu verschiedene Möglichkeiten der Realisierung:

1. ITU T.38
2. ITU T.37
3. oder aber Wandlung des analogen Signals in ein digitales, zum Beispiel mit G.711 codiertes, Paket

Um nun ein Fax fehlerfrei von Provider A nach Provider B zu übertragen, müssen beide auf ein einheitliches Verfahren zurückgreifen. Dieses Verfahren kann

1. durch eine regulatorische Richtlinie definiert werden (mit der Einschränkung, dass auf wesentliche Neuerungen eventuell zu spät reagiert wird, da die Änderung einer solchen Richtlinie in diversen Gremien oder durch Gutachten bestätigt werden muss)

2. aber auch eine Absprache zwischen allen Netzbetreibern sein, die einem verbindlichen Charakter entspricht, was nicht weniger aufwendig erscheint und daher meist erst einmal nur im nationalen Rahmen erfolgt.

(Um Ihnen ein Gefühl für die Zeitspanne eines weltweiten Standardisierungsprozesses zu geben, möchte ich in diesem Zusammenhang auf das ITU-T Dokument Q.3401: NGN NNI verweisen, welches am 09.03.2007 aufgelegt und bis heute nicht verabschiedet wurde.)

Wie Sie an diesem einen Beispiel sehen können, ist die Umstellung auf eine All-IP Plattform neben allen technischen Problemen auch eine organisatorische Herausforderung.

Doch zurück zu unserem Fax. Nachdem jetzt hoffentlich klar geworden ist, dass Fax Übertragung nicht gleich Fax Übertragung ist, schauen wir uns nun die unterschiedlichen Verfahren mit ihren Vor- und Nachteilen an.

Die ITU hat in diesem Zusammenhang zwei Verfahren standardisiert, die wir heute als T.37 und T.38 kennen. Beide Varianten sollen eine Übertragung des analogen Fax-Signals über ein paketorientiertes Netzwerk ermöglichen.

Das Protokoll T.37 findet dabei leider in der allgemeinen Betrachtung wenig Gehör, was eigentlich sehr schade ist, handelt es sich doch um eine TCP Übertragung, die auf dem SMTP Protokoll beruht.

Die Vorgehensweise dabei ist, dass ein Fax Gateway die empfangenen Daten nach T.30 sammelt und diese dann als E-Mail Anhang (TIFF Datei) an das Zielsystem versendet (Store and Forward). Durch den Rückgriff auf SMTP und TCP ist dabei sichergestellt, dass alle Daten beim Empfänger ankommen.

Leider gibt es nur eine geringe Verbreitung von T.37 Lösungen, die aber natürlich auch die Frage aufwerfen: Warum nicht direkt das Dokument per E-Mail versenden?

T.38 hingegen setzt auf eigenes Protokoll, das Internet Facsimilé Protocol (IFP). Vereinfacht gesagt wird auch hier das Fax in ein Bild umgewandelt, nur dass die Bitabfolge jetzt direkt in Echtzeit übertragen wird und nicht wie bei T.37 erst zwischengespeichert werden muss. IFP verhält sich dabei ähnlich wie RTP. Dies bedeutet, das Protokoll nutzt keine „well known Ports“, sondern diese werden beim Verbindungsaufbau mittels des SDP Protokoll ausgetauscht und sind Session spezifisch.

Die Übertragung kann sowohl über TCP als auch über UDP erfolgen.

Das Verfahren wird als IFT Internet Facsimile Transfer bezeichnet und ist im ITU Dokument T.38 von 11/2015 näher beschrieben.

Das IFP Paket Format besteht aus 2 Feldern:

- dem T30_INDICATOR TYPE, der u.a. die Art des modulation trainings definiert (von ITU-T V.27 2400 bis ITU-T V.33 14 400)

- und dem eigentlich Datenanteil T30_DATA mit folgenden Werten: ITU-T V.21 Channel 2 bis ITU-T V.33 14 400

Die weiteren Ausführungen der ITU gehen jedoch davon aus, dass die Übertragung in der Regel mittels UDP erfolgen. Um dabei auftretende Paketverluste zu kompensieren sieht der Standard deshalb die Einführung von Redundancy Messages innerhalb des Datenanteils vor.

Durch den Rückgriff auf UDP als Transportprotokoll besteht jedoch die latente Gefahr, dass Pakete im Netzwerk verloren gehen, da es keine Transportsicherung wie bei TCP gibt.

Was im Sprachumfeld noch toleriert werden kann, führt bei einem Fax unweigerlich zu fehlenden Zeichen oder Informationen, die ein Dokument letztendlich unlesbar machen.

SEQUENCE NUMBER (45)	PRIMARY MESSAGE	REDUNDANCY MESSAGE 1	REDUNDANCY MESSAGE n

Abbildung 1: Standard

Aber auch unsere Faxgeräte reagieren auf fehlende Pakete sehr empfindlich. Gerät der Paketfluss ins Stocken, weil Pakete im Datennetz gepuffert werden, geht unser Fax davon aus, dass die Übertragung unterbrochen wurde und beendet die Kommunikation mit einer Fehlermeldung. Dies wiederum liegt an der Funktionsweise des analogen Faxes, welches von einem getakteten Empfang von Signalen ausgeht, welche aufgrund der Pufferung jedoch ausbleiben.

Sollten Sie jetzt der Meinung sein, na gut, dann codieren wir eben die analogen Signale in digitale G.711 Informationen, so seien Sie gewarnt. Es ist durchaus zu erwarten, dass die Netzbetreiber zur Bandbreitenoptimierung in ihrem Backbone effizientere Codierungsverfahren wie z. B. Opus einsetzen, um das ineffektive G.711 zu ersetzen. In der Folge wird das generierte G.711 Paket in ein Opus Paket umcodiert. Dabei kommt es unweigerlich zu Signalverfälschungen, welche vom Faxgerät nicht mehr erkannt werden und wiederum zum Faxabbruch führen.

Das Grundproblem, das sich hier zeigt, ist:

> *Man versucht einen analogen Dienst in das digitale Zeitalter herüber zu retten, was - wie man erkennen kannn - kläglich scheitert.*

Nachdem nun die technischen Probleme geklärt sind, möchte ich zusätzlich die oft erwähnte rechtliche Bedeutung des Faxes beleuchten, in der oft erklärt wird, dass ein Fax der Schriftform entspricht. Dazu ein Auszug aus einem Statement, das ich bei it-recht-kanzlei.de gefunden habe. (siehe Abbildung 2)

Wie aus §126 a BGB hervorgeht, können Dokumente, die der Schriftform bedürfen, durchaus über den elektronischen Weg ausgetauscht werden, so sie den elektronisch signiert sind, jedoch nicht mittels Fax.

Aber wo wir gerade schon bei den guten alten PSTN Diensten sind, so müssen wir auch einen neuen Blick auf die Sonderanschaltungen werfen.

Warum lieben Sonderanschaltungen analoge Anschlüsse? Weil sie eine Phantomspeisung mitbringen, also man auch dann noch eine Meldung absetzen kann, wenn es zu einem Stromausfall kommt. Daher wurde die Meldung eines großen deutschen Netzbetreibers mit Wohlwollen aufgenommen, als dieser zusagte auch weiterhin analoge Telefonanschlüsse (inkl. Phantomspeisung) zur Verfügung zu stellen. Hierzu muss erwähnt werden, dass dies nur in den Gebieten garantiert werden kann, in denen der Netzbetreiber den Netzausbau selbst verantwortet. In anderen Gegenden kann dies ganz anders aussehen, so dass heute nicht garantiert werden kann, dass ein vollwertiger Analoganschluss deutschlandweit verfügbar sein wird.

Erklärungen per E-Mail, Telefax oder Computerfax entsprechen daher in Regel nicht der Schriftform.

- Erklärungen per Telefax: Erklärungen per Telefax entsprechen nicht der Schriftform, denn das Fax dient lediglich der Übermittlung. Der Empfänger erhält eine Unterschrift nur in Form einer Kopie, nicht das zur Wirksamkeit der Erklärung erforderliche Original.

- Erklärungen per E-Mail: Auch E-Mails entsprechen nicht der Schriftform. Denn E-Mails sind nur über das Internet übertragbare Nachrichten, die lediglich dann das Schriftformerfordernis erfüllen, wenn ein Ausdruck der E-Mail mit einer Unterschrift versehen ist.

Die schriftliche Form kann allerdings gemäß §§ 126 Abs.3, 126 a BGB durch die elektronische Form ersetzt werden.

Das elektronische Dokument muss dazu mit einer so genannten „qualifizierten elektronischen Signatur“ im Sinne des Signaturgesetzes versehen sein (§ 126 a BGB) und der Erklärungsempfänger muss mit der elektronischen Form einverstanden sein. Handelt es sich um einen Vertrag, müssen die Vertragsparteien jeweils ein gleichlautendes Dokument wirksam elektronisch signieren.

Ist die Schriftform nicht Wirksamkeitsvoraussetzung, sind Erklären per Telefax oder per E-Mail wirksam, auch mündliche Erklärungen. Aus Beweisgründen kann bei wichtigen Erklärungen aber z.B. ein per Einschreiben versandter, unterschriebener Brief oder bei Verträgen die Unterschriften der Vertragspartner dennoch sinnvoll.

Abbildung 2: Quelle: **http://www.it-recht-kanzlei.de/gesetzliche-schriftform.html**

Für die Zukunft aber ist es nicht ausgeschlossen, dass auch der lokale MSAN mittels Batteriepufferung Störungen im Stromnetz kompensieren kann.

Die Verfügbarkeit der Stromeinspeisung wird dabei nicht über den lokalen Netzzugangspunkt (MSAN) realisiert, sondern durch den BGN, der - wie früher die Ortsvermittlungsstelle - gegen Stromausfälle abgesichert ist.

Jedoch sind für die beliebten Sonderanschaltungen wie BMA, EMA und ÜMA die analogen PSTN Zugänge keine Pflicht mehr. Seitens des VdS wurde mit der Verabschiedung der Richtlinie 2471 (A13+A14) der Weg frei gemacht für Netzzugänge, die auf IP Basis zu realisieren sind:

> Der Primärweg ist dabei über IP (ADSL/VDSL, FTTH, usw.) und der sekundäre Pfad über eine Mobilfunkschnittstelle (GSM) abzubilden.

Im Zuge der Umsetzung der VdS Richtlinie muss explizit daraufhin gewiesen werden, dass für den lokalen Betrieb der genannten Meldeanlagen der Betreiber für eine Notstromversorgung mittels USV zuständig ist und nicht der Netzbetreiber oder Leitungsanbieter.

In diesem Zusammenhang möchte ich hier noch einmal darauf hinweisen, dass viele Dienste sich besser des Datennetzes bedienen als weiterhin auf die klassischen ISDN oder Analogschnittstellen zu bauen.

Geräte wie EC-Cash Terminals, Geldautomaten oder Ticketdrucker arbeiten auf Basis von digitalen Informationen und sind in der Lage über Datenleitungen mit einer viel höheren Bandbreite zu kommunizieren, was wiederum Transaktionen schneller und effektiver macht. Es macht keinen Sinn und wird zukünftig die Fehleranfälligkeit sogar erhöhen, wenn man diese Geräte weiterhin als analoge oder ISDN Endpunkte einbindet.

Auch Betreiber von ISDN basierten TK-Anlagen werden zum Handeln gezwungen, so sie weiterhin PMX Anschlüsse betreiben wollen oder müssen.

Zwar stellen fast alle Netzbetreiber ihren Kunden ISDN Gateways zur Verfügung, die sogar ein oder zwei PMX Anschlüsse zulassen. Hat man jedoch Bedarf nach mehr, kann es zu erheblichen Problemen kommen.

Das PSTN geht – die Vielfalt kommt

Diese Probleme liegen im Unterschied der zugrundeliegenden Übertragungstechnik: Die eingesetzte Paketvermittlung kennt im Gegensatz zur Kanalvermittlung keine Taktung. Dies bedeutet, dass die bisher seitens des Netzbetreibers zur Verfügung gestellte externe Taktung nicht mehr existiert und auch nicht bereitgestellt werden kann, da Datennetze diese nicht benötigen.

Werden jetzt mehrere PMX Gateways parallel genutzt, so hat jedes dieser Gateways einen eigenen Takt, der mit dem Takt der TK Lösung synchron sein muss.

Dieser Umstand führt dazu, dass nur PMX Gateways eingesetzt werden können, die zunächst intern ihren Takt synchronisieren, um sich dann im Anschluss mit der TK-Anlage zu verbinden. Das wird jedoch nicht von allen Gateway Lösungen unterstützt, so dass hier erhebliche Probleme zu erwarten sind.

Ein weiterer Punkt, der an dieser Stelle erwähnt werden muss, ist die Art der Bereitstellung einer Anbindung an das öffentliche Kommunikationsnetz. Wurden bisher einzelne Anschlüsse vermarktet, reden wir jetzt über einen Anschluss, der mehrere parallele Verbindungen zulässt.

So können heute schon auf einem asymmetrischen VDSL Zugang bis zu 164 parallele Telefonkanäle realisiert werden. Für Sie als Kunden bedeutet dies ein Umdenken bei der Planung von PSTN Anschlüssen. Haben Sie bisher z.B. für Sonderanschaltungen eine dedizierte Analog- oder ISDN-Leitung beauftragt, so müssen Sie jetzt nur noch dafür sorgen, dass auf der vorhandenen Anbindung ausreichend Kapazität für diese Sonderanschaltung zur Verfügung steht.

Eine weitere, neue Leitung wird nicht mehr benötigt.

Auch die bisher bekannte Staffelung der ISDN Kanäle in 2er oder 30er Schritten wird ersatzlos gestrichen. Es gibt nur noch einen Datenzugang mit der Bandbreite „x“ Mbit/s plus einer Anzahl „y“, von möglichen Gesprächskanälen. Die Variablen „x“ und „y“ sind nur von den vor Ort zu realisierenden technischen Gegebenheiten und dem geschäftlichen Bedarf abhängig.

So werden wir in Zukunft einzelne Gesprächskanäle auch dynamisch hinzubuchen können, falls die vertraglich vereinbarte Kanalanzahl nicht ausreichen sollte.

Sicher ist, dass es in der Zukunft möglich sein wird, maßgeschneiderte Lösungen zur Kommunikationsanbindung zu realisieren, die weit besser auf die Bedürfnisse der Kunden hin optimiert sind als dies heute mit ISDN geschehen kann.

Noch allerdings ist der Markt mitten im Umbruch, gerade die großen Netzbetreiber haben aktuell nicht alle nötigen Produkte am Start. Vieles ist noch Stückwerk, wie die mangelnde Innovation bei den Produkten. Sicher die bisher bekannten Leistungsmerkmale des ISDN Zuganges können in weiten Bereichen auch mittels IP umgesetzt werden, aber gerade neue Dienste sind stand heute noch nicht zu erkennen.

Dabei bietet sich das verwendete SIP Protokoll geradezu an neue Mehrwertdienste im Markt zu platzieren.

- Wo sind die Angebote, die HD Audio und Video anbieten?
- Welcher Provider bietet WebRTC basierte Kollaboration und Chat Plattformen als Mehrwertdienst zum SIP Trunk?
- Wer hält eine Lösung bereit um Föderationen zwischen Unternehmen zu vereinfachen?

All diese Fragen sind bisher nicht in Produkte eingeflossen, obwohl der Markt erkennbar danach verlangt.

Aber nicht nur die Provider müssen sich dringend ihren Hausaufgaben stellen, auch die Regulierungsbehörden haben noch Nachholbedarf.

Als Beispiel sei hier nur das Thema Notruf zu nennen. Zwar gibt es seit dem Juni 2011 eine technische Richtlinie Notruf, die bis heute jedoch nur den Bereich der ISDN basierten Netze verbindlich regelt.

Um Ihnen einen Einblick in die aktuelle Situation zu geben hier einige Auszüge aus der TR Notruf der Bundesnetzagentur:

1. Die TR Notruf legt unabhängig von den in Ursprungs- und Transitnetzen verwendeten Übertragungs- und Vermittlungstechniken die technischen Einzelheiten von Notrufverbindungen zu den im Einsatz befindlichen Notrufabfragestellen fest

2. **Notrufabfragestellen sind zurzeit ausschließlich mit Netzzugängen in ISDN-Technik ausgestattet**

3. Die TR Notruf legt die technischen Eigenschaften dieser Notrufanschlüsse fest

4. Sie gibt das Verfahren und die verschiedenen Formate zur Übertragung der Standortangabe als Anschrift oder in der Form einer Beschreibung mit geografischen Koordinaten vor

5. Die Standortangaben sind seit 23. Dezember 2012 zu übertragen

Gerade zu bedenklich ist dabei die Position 2 in der Auflistung. Trotz der Ankündigung aller Provider bis 2018 ISDN als Zugangstechnik abzuschalten, hat man es bisher nicht geschafft einen neuen, IP-basierten Standard für die Leitstellen zu verabschieden.

Zwar beteuert man von Seiten der Gremien, dass man eine finale Entscheidungsvorlage auf den Weg gebracht hat, jedoch steht immer noch nicht fest, wann eine Revision der TR Notruf verabschiedet wird.

Das PSTN geht – die Vielfalt kommt

Hinzu gesellt sich die Einsicht, das vielen Kommunen und Betreibern von Notrufabfragestellen anscheinend nicht klar ist, welche Folgen und Probleme ein Weiterbetrieb einer ISDN basierten Infrastruktur an einem IP basierten Netzzugang verursachen wird. Hier werden anscheinend notwendige Ausgaben in die Infrastruktur auf die lange Bank geschoben, in der Hoffnung das es schon irgendwie funktionieren wird.

Um dies zu unterstreichen hier ein weiterer Passus aus der Richtlinie:

6.3 Technologiespezifische Anforderungen an Notrufverbindungen

6.3.1 Notrufverbindungen im ISDN
Anforderungen an Notrufverbindungen im ISDN sind im Anhang N3 beschrieben.

6.3.2 **Notrufverbindungen in IP-Netzen**
Die Festlegung der Anforderungen erfolgt in einer künftigen Ausgabe der TR Notruf.

(Information: Anhang N -> Normativer Charakter)

Fakt ist jedoch auch, dass jeder, der eine Telekommunikationseinrichtung betreibt, die über einen Zugang zum nationalen öffentlichen Telefonnetz verfügt, verpflichtet ist einen Notruf zu unterstützen. Dies beinhaltet auch bei einer IP Anbindung den Provider darüber zu informieren, wo der Notruf initiiert wurde:

8.2 Aufgaben der Betreiber von Telekommunikationsnetzen

8.2.1 Mitwirkung bei der Ermittlung des Standortes des Notrufenden
Auf Anforderung des Telefondienste Anbieters des Notrufenden **ist der Erbringer von Vorleistungen verpflichtet, an der Ermittlung des Standortes mitzuwirken.** Nutzt der verpflichtete Vorleistungserbringer seinerseits Vorleistungen, so muss er beim Erbringer dieser Vorleistung die Standortdaten anfordern

Der Erbringer der Vorleistung ist verpflichtet, die Standortdaten in Abhängigkeit vom Netzzugang, d.h. entweder Festnetzanschluss oder Mobilfunkanschluss, von dem die Notrufverbindung eingeleitet wurde, unverzüglich an den Anfragenden zu übermitteln. Nach Empfang der Anfrage sind die Standortdaten innerhalb von 1 Sekunde an die anfragende Stelle zu übermitteln.

Die technische Schnittstelle zur Anforderung der Daten über den aktuellen Standort des Notrufenden ist beispielhaft in Anhang I4 beschrieben.

(Information: Anhang I -> Informativer Charakter)

Hier hilft aktuell nur der direkte Kontakt zum Provider um mit ihm ein Verfahren zu bestimmen, wie Geo-Daten oder Ortsinformationen parallel zu einem Notruf ausgetauscht werden können.

Der Regulierer gibt stand heute nur Empfehlungen, aber keine feste Regel vor.

Wie Sie sehen, ergeben sich zukünftig eine Reihe von Änderungen, denen jedoch heute schon eine ganze Reihe von technischen Alternativen und Empfehlungen gegenüberstehen, so dass sich auch in Zukunft alle bisherigen Anschaltungen adäquat erbringen lassen.

ComConsult Veranstaltungskalender

Lokale Netze für Einsteiger, 13.02. bis 17.02.2017 in Aachen

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,-- netto

IP-Wissen für TK-Mitarbeiter, 20.02. bis 21.02.2017 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,-- netto

RZ-Kopplung: Georedundanz für Rechenzentren, 13.03.2017 in Berlin

Die gestiegene Bedeutung von zentralen IT-Systemen für Unternehmen und gesetzliche Vorgaben erfordern geo-redundante Standorte von Rechenzentren. Für die Bereitstellung und den Betrieb der Rechenzentrums-Kopplung wird besonderes Know-how und strategische Planung benötigt. In diesem Seminar werden die aktuellsten Technologien und Anforderungen vorgestellt und ein optimales Gesamtkonzept beschrieben.
Preis: € 1.090,-- netto

Aufbau und Management von Internet-DMZ und internen Sicherheitszonen, 13.03. bis 15.03.2017 in Berlin

Die IT-Sicherheit für die Internet DMZ und internen Sicherheitszonen werden in diesem Seminar von Experten aus der Praxis vorgestellt und anschaulich erklärt. Verschiedene IT-Architekturen und Konzepte werden analysiert und auf ihre Praxistauglichkeit untersucht. Die Umsetzung anhand konkrete Projektbeispiele runden die Schulung ab. Preis: € 1.890,-- netto

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen, 13.03. bis 15.03.2017 in Köln

Dieses Seminar vermittelt alle notwendigen Projektschritte zu einer erfolgreichen Umsetzung von VoIP Projekten. Diese erstrecken sich über die Einsatz- und Migrations-Szenarien, die einsetzbaren Basis-Technologien und Komponenten und die erweiterten TK-Anwendungen wie IVR, UM oder UC. Es werden Bewertungskriterien für eine TK-Lösung und eine Übersicht über den bestehenden TK-Markt mit allen etablierten Hersteller vorgestellt.
Preis: € 1.890,-- netto

Netzzugangskontrolle: Technik, Planung und Betrieb, 13.03. bis 15.03.2017 in Berlin

Dieses 3-tägige Seminar vermittelt den aktuellen Stand der Technik der Netzzugangskontrolle (Network Access Control, NAC) und zeigt die Möglichkeiten aber auch die Grenzen für den Aufbau einer professionellen NAC-Lösung auf. Schwerpunkt bildet die detaillierte Betrachtung der Standards IEEE 802.1X, EAP und RADIUS. Dabei wird mit IEEE 802.1X in der Fassung von 2010 und mit IEEE 802.1AE (MACsec) auch auf neueste Entwicklungen eingegangen.
Preis: € 1.890,-- netto

TCP/IP-Netze erfolgreich betreiben, 13.03. bis 15.03.2017 in Aachen

IP ist die Grundlage jeden Netzes. Die Protokolle TCP und UDP bilden die Basis jeder Anwendungskommunikation. Es werden zudem Kenntnisse über Routingprotokolle, DHCP, DNS benötigt. Dieses Seminar vermittelt praxisnah das notwendige Wissen.
Preis: € 1.890,-- netto

Vertragsgestaltung und rechtssichere Organisation von Cloud Services für Nichtjuristen, 03.04. bis 04.04.2017 in Bonn

Dieses Seminar erklärt, wie Sie die Auslagerung Ihrer Private Cloud vertraglich absichern und warum Sie das unbedingt machen sollten.
Preis: € 1.590,-- netto

Virtualisierungstechnologien in der Analyse, 03.04. bis 04.04.2017 in Bonn

Im Zuge stetig zunehmender Konsolidierung ist Virtualisierung längst zum Standard in jedem Rechenzentrum geworden. Doch der Blick hinter die Kulissen offenbart einen rapide wachsenden Komplexitätsgrad, dessen Beherrschung ein tieferes Verständnis dieser Technologie erfordert. In diesem Seminar werden die Zusammenhänge zwischen Server, Netzwerk und Storage im Umfeld der Virtualisierung analysiert.
Preis: € 1.590,-- netto

Kommunikation über Private WAN und Internet, 03.04. - 04.04.2017 in Bonn

Dieses Seminar vermittelt die Erfahrungen aus den jüngsten Projekten mit dem Fokus Konzeption und Ausschreibung von WANs. Teilnehmer dieses Seminars profitieren von langjährigen Erfahrungen der Vortragenden im WAN-Bereich, kombiniert mit dem großen Erfahrungsschatz von ComConsult bei der Lösung von Problemen und der Lokalisierung von Fehlern in standortübergreifenden Netzen. Ferner werden Erfahrungen bei der Gestaltung sinnvoller Service Level Agreements (SLA) im WAN-Betrieb in diesem Seminar vermittelt.
Preis: € 1.590,-- netto

Zertifizierungen

ComConsult Certified Network Engineer

Lokale Netze für Einsteiger
13.02. - 17.02.17 in Aachen
08.05. - 12.05.17 in Aachen
18.09. - 22.09.17 in Aachen

TCP/IP-Netze erfolgreich betreiben
13.03. - 15.03.17 in Aachen
29.05. - 31.05.17 in Aachen
09.10. - 11.10.17 in Bremen

Internetworking
03.04. - 07.04.17 in Aachen
19.06. - 23.06.17 in Göttingen
13.11. - 17.11.17 in Aachen

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

ComConsult Certified Trouble Shooter

Trouble Shooting in vernetzten Infrastrukturen
02.05. - 05.05.17 in Aachen
26.09. - 29.09.17 in Aachen

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

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

ComConsult Certified Voice Engineer

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen
13.03. - 15.03.17 in Köln
15.05. - 17.05.17 in Düsseldorf
16.10. - 18.10.17 in Frankfurt

Session Initiation Protocol Basis-Technologie der IP-Telefonie
05.04. - 07.04.17 in Bonn
29.05. - 31.05.17 in Frankfurt
08.11. - 10.11.17 in Stuttgart

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

Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter
20.02. - 21.02.17 in Bonn
02.05. - 03.05.17 in Düsseldorf
18.09. - 19.09.17 in Düsseldorf

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

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

Impressum

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

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

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

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