ComConsult Research

Der Netzwerk Insider

Juli 2016

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

Software-Defined Wide Area Network

von Dr. Behrooz Moayeri

Das Attribut „Software-Defined“ wird vor immer neue Begriffe gesetzt. Einer dieser Begriffe ist WAN (Wide Area Network). Software-Defined WAN ist der neue Trend im Design standortübergreifender Netze. Dieser Beitrag geht auf diesen Trend ein. Dabei orientieren wir uns an den von der Open Networking User Group (ONUG) aufgestellten Kriterien für Software-Defined WAN.

Integration von WAN und Internet

Die wichtigste Eigenschaft von Software-Defined WAN ist die Integration von WAN und Internet. In einem Insider-Beitrag vom Mai dieses Jahres wurde bereits auf eine solche Integration eingegangen [1]. Durch die kombinierte Nutzung eines klassischen WAN und des Internet können Unternehmen verschiedene Ziele erreichen, darunter:

- Entlastung der relativ teuren Ressource WAN durch Verlagerung von besonders verkehrsintensiven Anwendungen wie Video und Web Surfing in das Internet
- Erhöhung der Verfügbarkeit des WAN durch Internet Backup
- Optimierung der Verkehrsströme bei Zugriff auf externe Clouds, indem der Pfad direkt von jedem Unternehmensstandort aus zu einer öffentlichen Cloud führen kann statt über den Umweg des unternehmenseigenen Rechenzentrums.

weiter auf Seite 5

Zweitthema

Internet of Things – die vierte industrielle Revolution Teil 1

von Dipl.-Inform. Petra Borowka-Gatzweiler

IoT – das Internet of Things wird unter dem deutschen Marketing-Begriff Industrie 4.0 vermarktet. Was verbirgt sich dahinter? Hat IoT Revolutions-Potenzial für die Netzwerk-Technologie? Wo steht der IoT-Markt, Zeichnen sich bereits erkennbare Architekturen und Standards ab? Der nachfolgende Beitrag setzt sich mit den genannten Fragen auseinander.

Schöne neue Welt

Die Musik des Weckers holt Sheila um 07:00h MESZ aus dem Schlaf. Die Rollos an den Fenstern muss sie nicht mehr hochziehen, denn 15 Minuten nach dem Start der Weckmusik heben sie sich automatisch. Abhängig von der Weckzeit hat sich 30 Minuten vor dem Wecken die Heizung hochgefahren und Küche und Bad von der Nachtabsenkung auf angenehme 22 Grad erwärmt. Das Wohnzimmer bleibt noch in der Nachtabsenkung, denn Sheila nutzt es morgens nicht, wie die Raumkamera in 4 Monaten Baselining festgestellt hat.

weiter auf Seite 16

Geleit

IPv6: Wenn man nicht hinsieht, ist es auch nicht da

auf Seite 2

Standpunkt

Widerstand ist zwecklos: Sicherheitskomponenten in der Cloud

auf Seite 14

Sonderveranstaltung

Das PSTN stirbt: Die neue Kommunikation mit SIP/IP

ab Seite 12

Aktuelles Seminar

Die neue EU-Datenschutzgrundverordnung

ab Seite 4

Zum Geleit

IPv6: Wenn man nicht hinsieht, ist es auch nicht da

Ja, es gibt Probleme, die kann man durch Aussitzen lösen. Bei IPv6 wird das jedoch genau so wenig funktionieren wie bei einem Wasserfleck an der Wand: je länger man ihn ignoriert, desto größer wird nur das Problem.

Welche Gefahren gibt es, wenn man IPv6 ignoriert?

Was ist nun mit dem Wasserfleck an der Wand, der immer größer wird? Wo liegen die Gefahren, wenn man IPv6 einfach im Alltag ignoriert? Oder ist das nur Panikmache derer, die IPv6 unbedingt durchsetzen wollen?

Welche Gefahren es für wen gibt, ist von der eigenen Infrastruktur, den eingesetzten Komponenten und Betriebssystemen, aber auch vom Internetprovider abhängig. Darum will ich hier nur drei Beispiele aufzeigen, die nicht zwingend jeden treffen, alle aber bereits so eingetreten sind:

1. **Sicherheit**
   Der aktive Dual-IP-Stack moderner Betriebssysteme erlaubt es mit Bordmitteln gängiger Linux-Distributionen einem Rechner ein aktives IPv6 Netz vorzugaukeln (Stichwort: Router Advertisments + NAT64, ggf. noch DNS). Damit kann man jeglichen Verkehr über den eigenen Rechner leiten, indem man vorgibt, der aktive IPv6 Router zu sein. Ein Man-in-the-Middle-Angriff wie er im Buche steht.

   Wenn man IPv6 ignoriert, wird man das höchstwahrscheinlich gar nicht mit bekommen, da ja alles funktioniert.

   Wenn man jedoch selbst IPv6 eingeführt hat, dann sollte man auch ein entsprechendes Sicherheitskonzept erarbeitet haben. Im eigenen Netz schützen RA-Guards auf Layer 2 Switchen vor solchen Angriffen, wie es die DHCP-Guards bei IPv4 tun.

2. **Tunnel**
   Eine Alternative zum Ignorieren ist das Deaktivieren von IPv6. Auch das hat ein Kollege von mir versucht: mit gemischtem Erfolg.

   Er war der Meinung, IPv6 wäre an den langsamen Internetverbindungen schuld (wie sich rausstellte war es eine geänderte Update-Regel, die die

   Internetleitung regelmäßig überlastete). Also schaltete er damals bei seinem Windows 7 Rechner den IPv6 Stack einfach aus. Das Resultat war, dass auf der Firewall plötzlich IPv6 Adressen auftauchten, die wir gar nicht vergeben hatten.

   Was war passiert? Mit dem Abschalten des IPv6 Stacks auf dem Interface aktivierte Windows einen virtuellen 6to4 Adapter und versuchte einen Tunnel aufzubauen.

   Ein anderer, mit Troubleshooting befasster Kollege erzählte, dass er auch schon aktive ISATAP-Tunnel in Unternehmen entdeckt hat, von denen niemand etwas wusste.

   Solange die Firewalls ordnungsgemäß konfiguriert sind, sollten solche Tunnel kein weiteres Problem für die Sicherheit darstellen. Das Problem liegt im Wort „solange“: denn wenn ein Unternehmen nicht mal weiß, dass es ISATAP aktiviert hat, wie kann es dann sicher sein, dass die Firewalls ordnungsgemäß konfiguriert sind?

3. **„Schattenbetrieb“**
   Alle Betriebssysteme kommen heute mit aktivierten Dual-IP-Stack. Empfängt ein Client keine Router Advertisements, so resultiert daraus nicht, dass der IPv6 Stack deaktiviert wird, vielmehr bleibt die Kommunikation auf die Link-Lokale IPv6 Adresse beschränkt. Mit dieser kann er aber ohne Probleme innerhalb seines Layer-2 Netzes kommunizieren.

   Wer jetzt glaubt, dass er das nicht täte, da diese Adresse schließlich quasi unbekannt ist, weil sie beispielsweise nicht im DNS eingetragen wird, irrt. Dafür sorgen einige Betriebssysteme selbst, bei Windows der Computerbrowser, bei OS X der Bonjour-Dienst.

   Aber auch Agenten-basierte Software kann die Link-Lokalen Adressen nutzen. Bevor wir selbst mit IPv6 aktiv angefangen haben, wurde IPv6 bereits von einer Datensicherungssoftware genutzt. Diese kopierte die Daten von den Servern und sicherte sie damals auf Band. Das genutzte Protokoll war IPv6, die genutzten IP Adressen waren Link-Local.

   Die Gefahr besteht darin, dass man im Falle eines notwendigen Troubleshootings mit einem Protokoll konfrontiert wird, das man bislang glaubte ignorieren zu können. Im Fehlerfall ist es dann aber zu spät sich einzuarbeiten.

Was ist die Grundvoraussetzungen für eine erfolgreiche Migration

Die eigentliche Frage ist jedoch: ist IPv6 und die Migration dorthin überhaupt ein so großes Problem wie vielfach angenommen?

Dr. Moayeri brachte es unlängst auf den Punkt: mehr und mehr gewönne er den Eindruck, dass es sich bei der Dual-Stack-Umstellung so verhalte wie mit der Jahr-2000-Umstellung: problemloser als befürchtet.

Ich möchte nicht falsch verstanden werden, man beachte den Komparativ: „problemloser“ heißt nicht „problemlos“. Aber die erwarteten Schreckensszenarien blieben bislang aus.

Für eine erfolgreiche, problemlose Umstellung sind zwei Kenntnisse ausschlaggebend:

1. Die Kenntnis, wo man ist
2. Die Kenntnis, wo man hin will

Ersteres bedeutet, dass man für die Migration sehr genau wissen muss, wie das eigene Netz aufgebaut ist, welche Software im Unternehmen eingesetzt wird und welche Prozesse unternehmenskritisch sind. Zweiteres bedeutet, dass man viel Zeit in die Planung eines IPv6 Projektes stecken sollte. Das umfasst auch

Schwerpunktthema

Software-Defined Wide Area Network

Fortsetzung von Seite 1

Dr.-Ing. Behrooz Moayeri hat viele Großprojekte mit dem Schwerpunkt standortübergreifende Kommunikation geleitet. Er gehört der Geschäftsleitung der ComConsult Beratung und Planung GmbH an und betätigt sich als Berater, Autor und Seminarleiter.

Ein Grundmerkmal von Software-Defined WAN, nämlich Nutzung von WAN und Internet im Modus aktiv-aktiv, ist in der Abbildung 1 dargestellt.

Im Design gemäß der Abbildung 1 kommt der Komponente, die zwischen dem LAN einerseits und den standortübergreifenden Netzen WAN und Internet andererseits eingesetzt wird, eine Schlüsselrolle zu. Diese Komponente muss einen Teil des Verkehrs über das WAN und einen anderen Teil über das Internet übertragen. Der Modus „aktiv-aktiv“ bedeutet, dass die Netzlast auf das WAN und das Internet aufgeteilt wird.

Es kann verschiedene Kriterien für die Lastverteilung geben. Am geeignetsten ist die Unterscheidung zwischen verschiedenen Applikationen. Die Komponente am Übergang zwischen lokalem und standortübergreifendem Netz („Edge“) muss die Datenpakete zu Anwendungen zuordnen und für verschiedene Applikationen unterschiedliche Routen verwalten können. Lange bevor der Begriff Software-Defined WAN zum ersten Mal aufgetaucht ist, nannten Netzspezialisten die applikationsabhängige Weiterleitung von Paketen Policy-Based Routing (PBR).

Bei der Internet-Nutzung ist zu berücksichtigen, dass über das offene Medium Internet mehr Angriffe drohen als über ein privates WAN. Die schon seit Jahren etablierte Antwort auf diese Herausforderung ist Verschlüsselung. Denkbar ist zum Beispiel, dass die Edge-Komponente über das Internet einen VPN Tunnel zum Rechenzentrum (RZ) aufbaut. Dieser Weg zum RZ existiert dann parallel zum Weg über das WAN. Mit dem verschlüsselten Tunnel wird sichergestellt, dass im Internet der Datenverkehr nicht abgehört oder verfälscht werden kann.

Es gibt neben VPN noch andere Möglichkeiten zur sicheren Kommunikation über das Internet. Zum Beispiel können Applikationen für Verschlüsselung sorgen. In solchen Fällen können die Daten auch direkt über das Internet fließen, ohne dafür einen VPN-Tunnel nutzen zu müsse. Ein solcher Fall ist eine Videokonferenz unter Nutzung des Standards H.235. Viele der heute verfügbaren Videokonferenzlösungen nutzen diesen Standard zur Verschlüsselung und Authentisierung.

Ein anderer wichtiger Aspekt bei der Integration von WAN und Internet ist die Absicherung des einen Pfades durch den

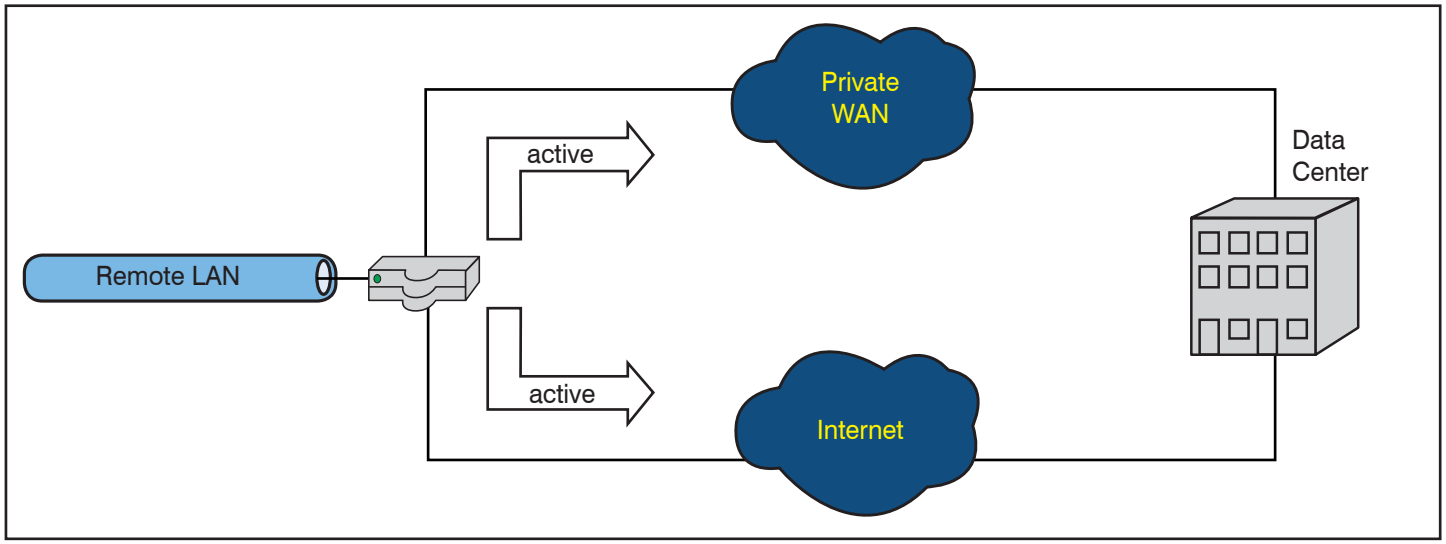

Abbildung 1: Nutzung von WAN und Internet im Modus aktiv-aktiv

anderen. Dynamische Routing-Mechanismen können dafür sorgen. Zum Beispiel kann ein Automatismus für die Umschaltung vom WAN auf ein Internet-VPN genutzt werden. Eine bestimmte Applikation kann das WAN nutzen, solange es verfügbar ist. Fällt die Route über das WAN weg, wird auf das Internet-VPN ausgewichen.

Die gleichzeitige Nutzung von WAN und Internet für die standortübergreifende Kommunikation trägt dem Umstand Rechnung, dass diese beiden Medien unterschiedliche Eigenschaften aufweisen und die verschiedenen Eigenschaften unterschiedliche Wichtigkeit für Applikationen haben. Zum Beispiel kann für eine bestimmte Applikation besonders wichtig sein, dass es möglichst keine Paketverluste gibt. Der Verkehr einer solchen Anwendung kann über das WAN übertragen werden. WAN Provider bieten oft Garantien hinsichtlich Begrenzung von Paketverlusten an. Solche Garantien gibt es auch für die Begrenzung der Paketlaufzeiten und Laufzeitschwankungen.

Andererseits kann die Internet-Verbindung eine wesentlich höhere Bitrate als die WAN-Verbindung aufweisen. Generell gilt, dass Übertragungskapazität in einem privaten WAN teurer als im Internet ist. Weist eine bestimme Anwendung eine besonders hohe Netzlast auf, kann sie das Internet nutzen, statt die teure WAN-Verbindung zu belegen. Ein Beispiel ist der Zugriff auf das World-Wide Web. Immer mehr Webseiten enthalten Video- oder sonstiges voluminöses Bildmaterial. Dem Autor sind Umgebungen bekannt, in denen 70 bis 80 Prozent der WAN-Kapazität durch Internet-Nutzung belegt werden. Da nicht jeder Standort mit einem eigenen Internetanschluss ausgestattet ist, muss der Internet-Zugriff der Standorte ohne eigenen Internetanschluss über das WAN und Standorte mit Internetanschluss erfolgen, in der Regel Rechenzentren. Neben der Belegung teurer Ressourcen kann ein solches Szenario andere Probleme verursachen. Insbesondere in einem globalen WAN können die Antwortzeiten von Internetzugriffen durch den Umweg über das WAN spürbar verlängert werden. Außerdem kann ein Nutzer auf Webseiten landen, die nicht auf seine Sprache und sein Herkunftsland ausgelegt sind.

Wird ein Standort über die Edge-Komponente direkt mit dem Internet verbunden, ist zu klären, wie das Standortnetz vor Angriffen aus dem Internet geschützt werden kann. Die Beschränkung jeglicher Internet-Kommunikation auf verschlüsselten Verkehr in einem VPN-Tunnel ist eine mögliche Variante. Diese Variante weist jedoch den Nachteil auf, dass die Kommunikation mit Zielen im Internet immer den Umweg über das VPN und den zentralen VPN-Standort nimmt.

Eine andere Variante besteht darin, dass der Zugriff auf das öffentliche Web am VPN-Tunnel vorbei führt und den direkten Weg nimmt. Diese Variante heißt Split Tunnel. Dadurch entstehende Risiken können reduziert werden, wenn der Internet-Zugriff über eine Web Security Cloud erfolgt. Eine solche Cloud bietet Funktionen wie Content Filtering und Schutz vor schadensstiftender Software.

Nutzung physischer und logischer Komponenten

Jeder, der bereits Erfahrungen beim Rollout von WAN-Lösungen hat, kennt die logistischen Herausforderungen bei der Lieferung, Aufstellung und Konfiguration von WAN-Komponenten an entfernten Standorten. Wird proprietäre Hardware als WAN Edge Device genutzt, müssen die WAN-Komponenten oft aufwändig ausgeliefert und installiert werden. Dies ist häufig nicht nur bei der Erstinstallation erforderlich, sondern auch bei Änderungen. Zum Beispiel kann die Erhöhung der Bitrate an einem WAN-Anschluss den Einsatz neuer Hardware erfordern. Auch das Hinzufügen neuer Funktionen wie WAN-Optimierung oder Verschlüsselung kann mit Hardware-Änderung einhergehen.

Um diesen Aufwand zu reduzieren, kann man statt proprietärer Hardware Standard-Hardware nutzen. Die WAN-Komponente kann eine virtuelle Maschine auf Basis von Standardhardware sein. WAN Edge Devices oder, wie Provider sie nennen, Customer Premises Equipment (CPE), benötigen heute oft keine anderen Netzschnittstellen als Ethernet. Insofern lässt Standard-Hardware bezüglich Ausstattung mit Netzschnittstellen nichts vermissen. Jede Hardware unterstützt Ethernet.

Abbildung 2 zeigt die Nutzung von physischen und logischen CPE-Komponenten in einem WAN. Das virtuelle CPE nutzt dabei eine Standard-x86-Plattform. Die Änderung einer Edge-Komponente wird dadurch erleichtert. Funktionen können „Software-Defined“ hinzugefügt werden.

Die Nutzung von Standard-Hardware erleichtert auch die Ersatzteilbeschaffung. Standardhardware ist in der Regel schneller zu besorgen als proprietäre Hardware.

In bestimmten Szenarien kann der Einsatz physischer CPE-Komponenten weiterhin erforderlich sein. Zum Beispiel können WAN-Schnittstellen wie DSL oder LTE in Nutzung sein, für die Spezialhardware eingesetzt werden muss. Daher kann es in einem Software-Defined WAN eine Mischung von physischen und virtuellen CPE-Komponenten geben.

WAN-Steuerung durch Anwendungen

Im Zusammenhang von Software-Defined Network (SDN) wird häufig diskutiert, wie Anwendungen das Verhalten des Netzes steuern können. Manche Ansätze von SDN sehen vor, dass über das sogenannte Northbound Interface Applikationen das Netz steuern. Diese Steuerung erfolgt meistens über eine zentrale Instanz, genannt Controller. Der Controller unterhält neben dem Northbound Interface zu Anwendungen sogenannte Southbound Interfaces zu den Netzkomponenten. Über das Southbound Interface steuert der Controller das Verhalten der Netzkomponenten.

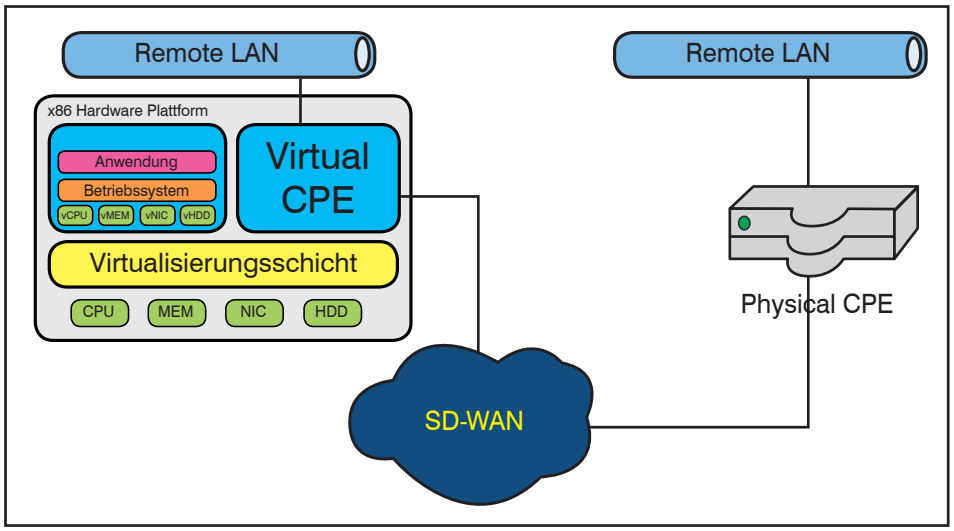

Abbildung 2: Nutzung physischer und logischer WAN-Komponenten

Zweitthema

Internet of Things – die vierte industrielle Revolution

Fortsetzung von Seite 1

Dipl.-Inform. Petra Borowka-Gatzweiler leitet das Planungsbüro UBN und gehört zu den führenden deutschen Beratern 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.

Das vor dem Aufstehen automatisch gesteuerte Hochfahren der Heizung findet nicht nur in Sheilas Wohnung statt, sondern auch bei allen anderen Bewohnern von Smart City, die um 07:00h aufstehen und eine Gasheizung haben. Die dadurch entstehende Leistungsspitze wird durch intelligente Zuschaltungen des regionalen Energieversorgers vorausberechnet, da die Smartmeter aller Haushalte halbstündlich den aktuellen und erwarteten Energiebedarf an das EVU-RZ (in der Cloud) übermitteln. Dadurch müssen keine nennenswerten Überkapazitäten bereitgestellt werden, sondern kann gezielt der aktuelle Gasbedarf ins Versorgernetz eingespeist werden.

Mit dem Frühstückskaffee in der Hand setzt sich Sheila ihre VR-Brille auf und checkt die seit gestern eingegangenen Chats-Anfragen, Videoclips und Projektnotizen (ihre Mutter hat noch mit Email gearbeitet…). Besonders wichtige Chats und Videoclips beantwortet sie sofort.

Nach dem Frühstück steigt Sheila in ihr Elektro-Fahrzeug, um ins Büro zu fahren. An jeder Ampel ist die Straße mit Qualcomm Halo Bodenplatten-Induktionsschleifen ausgestattet, ihr BMW hat eine DIN A4 große Induktions-Spule, über die er beim Halten an der Ampel Strom nachlädt (s.a. "Laden ohne Leiden", Die Welt, 19. Juni 2016). Die geladene Strommenge wird über einen Chip im Auto ermittelt, der beim Nachladen auch den genutzten Energieversorger erkennt. Im Minuten-Takt übermittelt er die von Sheilas Fahrzeug entnommene Strommenge an das RZ des Cloud-Anbieters, der für alle EVUs der Region die Abrechnungs-Auswertungen aller Verbraucher-Chips bereitstellt. Die übermittelten Daten werden sofort in eine Trend-Analyse-App eingespeist, die den Strombedarf des nächsten 5 Minuten-Intervalls anhand des aktuellen Verkehrsaufkommens berechnet. Sheila bekommt monatlich oder vierteljährlich eine Abrechnung, der – auf Wunsch – detailliert zu entnehmen ist, wann ihr Auto bei welchem EVU wieviel Stromleistung bezogen hat. Ist die Ampel rot, hält ihr Wagen mit Autostop 1,5m hinter dem vor ihr stehenden Auto an, 2 Sekunden bevor die Ampel auf Grün wechselt, startet sich der Motor wieder.

Am Bürostandort angekommen, steigt Sheila vor dem Parkplatz aus und startet das autonome Einparken über ihr Smartphone. Sheilas Auto parkt selbständig ein und zwar so, dass es passgenau über der Induktionsschleife des Parkplatzes zu stehen kommt, um mit dem optimalen Wirkungsgrad nachzuladen.

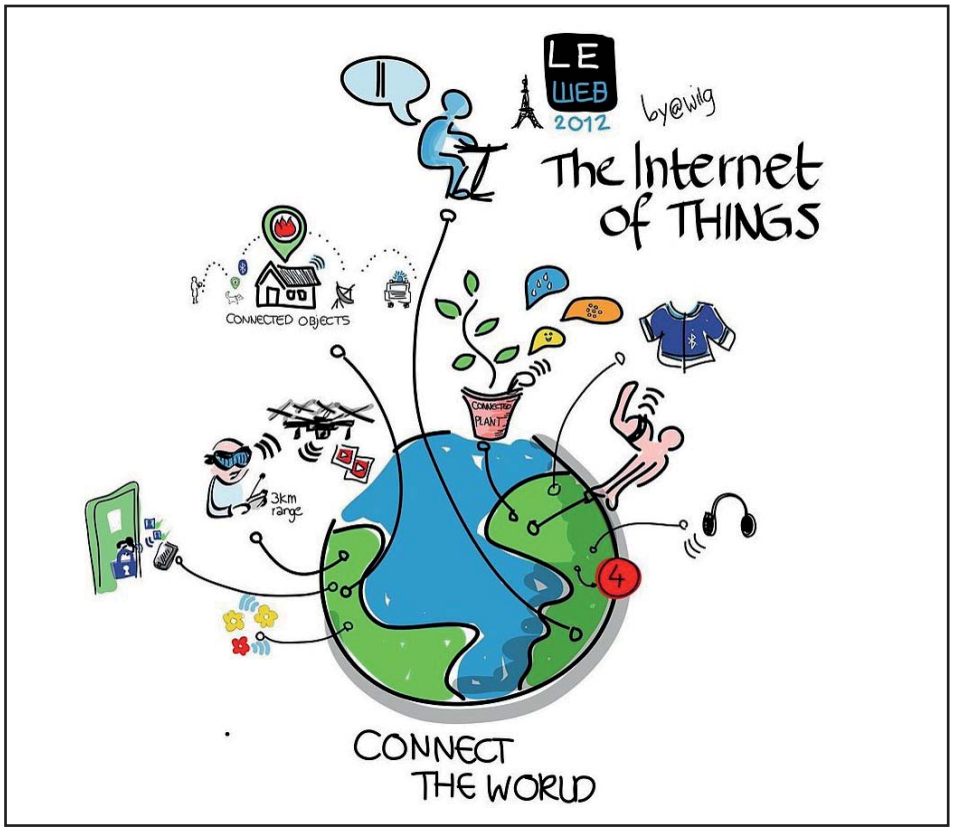

Abbildung 1: Die Vernetzung der Welt

Internet of Things – die vierte industrielle Revolution

Pure Vision? Science Fiction? Nein – die komplette Geschichte kann sich in fünf Jahren als Pilot und in 15 Jahren als Massenmarkt so ereignen: mit Internet of Things, der globalen Vernetzung aller "Objekte" (siehe Abbildung 1):

- Smart Metering
- Smart Home
- Smart City
- Smart Farming
- Smart Retail

1. Was ist Internet of Things?

Internet of Things (IoT) oder noch umfassender Internet of Everything (IoE) wird auch als vierte industrielle Revolution (Industrie 4.0) bezeichnet. Von der Industrialisierung mit Wasser- und Dampfkraft über Elektrizität hin zur digitalen IT und Fertigungs-Automatisierung geht der Weg jetzt über die Vernetzung aller „Dinge“ in Richtung Cyberspace und Cyber-Physikalische Systeme.

Internet of Things ist das Netzwerk physischer Objekte – Geräte, Fahrzeuge, Gebäude und andere Gegenstände – in diese eingebettet sind Elektronik, Software, Sensoren, Aktoren und Netzwerk-Konnektivität, die diese Objekte in die Lage versetzt, Daten zu sammeln und auszutauschen (Wikipedia)

"Manche versetzt das in Euphorie, andere in Angst und Schrecken. Manchen öffnet es die Augen, andere wollen sich davor verschließen. An der Botschaft jedoch ist kein Vorbeikommen: Unsere Lebens- und Arbeitswelten verändern sich dramatisch. Sie entfernen sich vom Manuellen und tauchen immer tiefer ein in die digitale Vernetzung" (Die Welt, 25. April 2016, Sonderausgabe Industrie 4.0, Seite I). (siehe Abbildung 1.1)

Internet of Things betrifft die verschiedensten, wenn nicht alle Bereiche unseres Lebens und Arbeitens und wird diese revolutionieren. Abbildung 1.2 zeigt Beispiele aus den Bereichen

- Welt-Index
- RFID, Logistik-Tracking
- Fernsteuerung (Remote Control)
- M2M und
- Metering, Objektsteuerung

Welt-Index (Orange): stellt eine Vorstufe von IoT dar. Alle Gebäude sind im weltweiten Internet erfasst und beschrieben (Geo-Tagging, GPS, Google Earth). In der erweiterten IoT-Ausbreitung sind alle Objekte der Welt mit ihrer Geo-Positionierung erfasst und online dargestellt. Es gibt jedoch noch keine Kommunikation mit ihnen.

Logistik-Tracking, RFID (Lila): Objekte werden mit einem (weltweit eindeutigen) RFID Tag versehen, der jede ihrer Bewegungen nachvollziehbar macht und über den sie online dargestellt werden. Es gibt jedoch noch keine Kommunikation mit ihnen. Beispiele sind Paket-Tracking, Barcodes, Nearfield Communication.

Remote Control (Rot): Objekte sind über einen Chip mit ihrer Geoposition im Netz erfasst, gestohlene Objekte wie zum Beispiel Autos oder Schlüssel können nachverfolgt werden. Diese Objekte sind mit dem Internet verbunden und kommunizieren mit Menschen: Sie nehmen Aktionsbefehle entgegen und liefern Informationen über sich selbst (beispielsweise ihre Geoposition, wenn sie gestohlen wurden).

Machine to Machine (Grün): Objekte kommunizieren untereinander, wenn bestimmte (Trigger)-Bedingungen eingetreten sind. Im Smart Farming fordern Pflanzen selbständig Wasser von den Bewässerungs-Systemen an, wenn sie "durstig" sind.

Steuerung durch intelligente Objekte (Blau): Alarme werden je nach gemessenen Umgebungs-Bedingungen dynamisch früher oder später aktiviert. Zum Beispiel Weck-Alarme können bei schlechtem Wetter oder hohen Verkehrslasten, unvorhergesehenen Stau-Bedingungen früher aktiviert

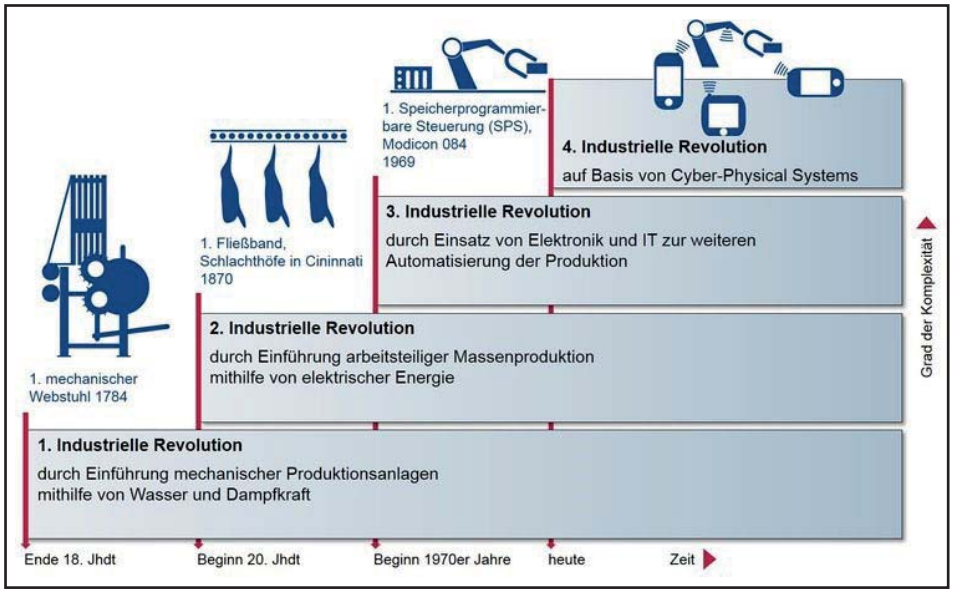

Abbildung 1.1: Industrielle Revolutionen

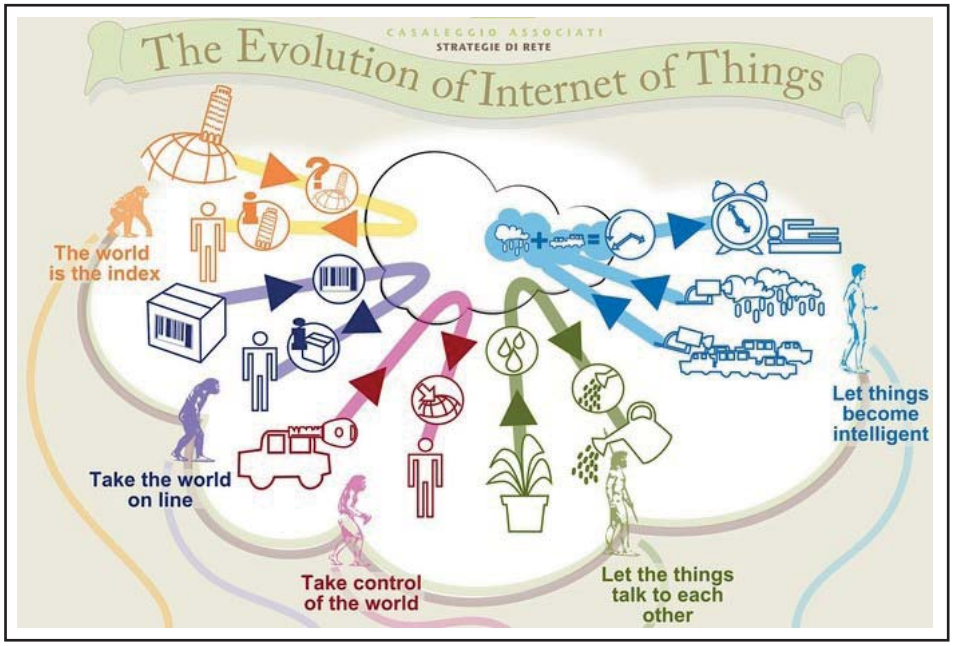

Abbildung 1.2: Einsatzbereiche für IoT