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

die Tests von relevanten Funktionen und Protokollen auf Netzwerkseite sowie Funktionstests bei der Software, sobald diese umgestellt werden soll. Die Umstellung selbst ist dann, je nach Komplexität der Umgebung, vergleichsweise einfach.

In der Tat zeigt sich bei laufenden Projekten, wie wichtig eine Bestandsaufnahme und ein sorgsam geplantes Vorgehen sind. Selbst komplexe Umgebungen mit vielen Standorten können so entspannt migriert werden.

Welche Wege wurden bislang erfolgreich umgesetzt

Der Grund für die Bedeutung von Bestandsaufnahme und Planung liegt darin, dass es keinen allgemeingültigen Migrationspfad gibt. Jedes Unternehmen muss seinen eigenen finden, der zu seinen Bedürfnissen passt. Dazu drei kurze Beispiele sollen das verdeutlichen:

1. **Migration zu Dual-IP in kleinen Umgebungen**
   In kleinen Umgebungen ist es möglich eine zügige Migration hin zu Dual-IP vorzunehmen. Die Anzahl der notwendigen Maßnahmen ist ebenso überschaubar wie die der eingesetzten Hard- und Software. So haben wir bei ComConsult Research diesen Schritt schon vor Jahren hinter uns gebracht. Natürlich gab und gibt es dabei kleine Holpler. Da das Fachpersonal jedoch vor Ort ist und ohne Anträge angesprochen werden kann, werden diese meist schnell beseitigt. Diese Migration haben wir auch auf große Teile unseres Internet-Angebotes übertragen und sind ohne Zwischenschritt direkt zu Dual-IP migriert.

2. **Migration mittlerer Umgebungen direkt zu IPv6-only**
   Ein größeres Partnerunternehmen migriert seine Clients direkt zu IPv6-only. Dabei setzen sie auf NAT64, um Clients, die sich in bereits auf IPv6 umgestellten Bereichen finden, an das restliche Netz anzuschließen. Begonnen wurde natürlich mit unkritischen Bereichen. Die Rückmeldungen sind durchweg positiv.

3. **Schrittweise Migration großer Netze**
   Große Unternehmen migrieren zunächst ihre Netzwerk-Infrastruktur. Dabei muss darauf geachtet werden, dass am Ende keine schwarzen Löcher überbleiben. Also Bereiche, in denen IPv6 nicht geroutet wird. Wie zügig das abläuft, ist davon abhängig wie homogen das Netz aufgebaut ist. Je individueller jeder Standort designt, je mehr Komponenten aus Zukäufen im Netz vorkommen, desto aufwendiger wird die Umstellung. Desto notwendiger wird eine detaillierte Planung des Vorgehens.

Fazit

Wer wie zu Bundeswehrzeiten ein Maßband in der Schublade hat, von dem er jeden Tag einen Zentimeter bis zur Rente abschneidet, der kann IPv6 weiterhin ignorieren und seinen Nachfolgern überlassen. Alle anderen jedoch tun gut daran, sich mit der Technik vertraut zu machen. Sei es auch nur, um den Gefahren zu begegnen, die durch den Nicht-Einsatz von IPv6 entstehen. Besser ist jedoch, den Wasserfleck jetzt anzugehen, bevor sich Schimmel bildet und er zu einem ernsten Problem für das Unternehmen wird.

Ihr
Markus Schaub

Seminar

IPv6 Grundlagen
28.11.-29.11.16 in Bonn

IPv6 betreiben, bedingt IPv6 verstehen. In diesem Seminar werden die Grundlagen des neuen IP Protokolles verständlich und praxisnah vermittelt. Die Schulung richtet sich gleichermaßen an Planer, Betreiber, Administratoren und Software-Entwickler.

IPv6 ohne die notwendigen Grundlagen zu planen oder gar zu betreiben, entspricht einem Blindflug ohne Flugerfahrung: zu groß sind die Unterschiede zwischen den Versionen 4 und 6. Diese erstrecken sich nicht nur auf die Adresslänge. Vielmehr findet ein Paradigmenwechsel auf vielen Ebenen statt: den Adressen, dem Protokoll und den Funktionen. Nur wer diese Unterschiede im Detail kennt, kann sein IPv6 Netz sinnvoll planen, betreiben und im Zweifelsfall die Fehler finden. Dieses Seminar steigt tief in die neue Technik ein, zeigt die Unterschiede auf und erläutert die Bedeutung für die Praxis.

IPv6 bringt als Seminar einige spezielle Rahmenbedingungen mit sich:
- Die Teilnehmer haben unterschiedliche Vorkenntnisse zu IPv4
- Es gibt Sonderthemen, die nicht alle Teilnehmer betreffen
- In der Umsetzung des Gelernten entstehen schnell weitere Fragen

Um dem gerecht zu werden, haben wir dieses Seminar in vier Teile aufgeteilt. Damit integrieren wir Videos, Präsenzschulung und Webinare in einem Seminar. Diese Aufteilung orientiert sich an den neuesten Erkenntnissen der Forschung und ermöglicht sowohl einen optimalen Lernerfolg für die Teilnehmer als auch eine Anpassung an die unterschiedlichen Anforderungen der Teilnehmer:

1. Vorbereitung
2. Präsenzschulung
3. Spezialthemen und Vertiefung

Referent: Markus Schaub
Preis: € 1.790,- netto

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

Aktuelles Seminar

Die neue EU-Datenschutzgrundverordnung 21.09.16 in Frankfurt

Die ComConsult Akademie veranstaltet am 21.09.16 ihr Seminar "Die neue EU-Datenschutzgrundverordnungt" in Frankfurt.

Am 25.05.2016 ist ein neues einheitliches Datenschutzrecht in der Europäischen Union in Kraft getreten. Die Verordnung wurde am 27.04.2016 verabschiedet und am 04.05.2016 im Amtsblatt der EU veröffentlicht. Bis zur einheitlichen Anwendung der Vorschriften gibt es noch eine Übergangsfrist bis zum 25.05.2018. Die Zeit ist jedoch knapp, um sich auf die tiefgreifenden Änderungen des Datenschutzrechts und vor allem die neue Haftung für Auftragsdatenverarbeiter und die Erhöhung der möglichen Bußgelder von 300.000 Euro auf 20 Mio. Euro vorzubereiten. So wird es gravierende Änderungen bei der Verarbeitung von sensiblen Daten und bei der grenzüberschreitenden Datenverarbeitung geben. Firmen außerhalb der EU, insbesondere aus den USA, müssen sich auf eine erhebliche Ausweitung des Anwendungsbereichs einstellen. Die Aufsichtsbehörden verhängen erste erhebliche Bußgelder nach dem Ende von Safe Harbour, ob das Nachfolgeabkommen EU US Privacy Shield in Kraft tritt, steht nach der Ankündigung der irischen Datenschutzbehörde, zum EuGH zu gehen und dem Widerstand des EU-Datenschutzbeauftragten noch in den Sternen.

Das deutsche Datenschutzgesetz wird nur noch solche Themen behandeln, die den Mitgliedsstaaten in der Verordnung als Regelungsbereiche überlassen wurden, z.B. die Frage, wie die Pflicht eines betrieblichen Datenschutzbeauftragten geregelt wird.

Informieren Sie sich frühzeitig über die geplanten Regelungen, damit Sie jetzt schon wissen, was auf Ihr Unternehmen zukommt.

- Entwicklung des Datenschutzes
- Entstehung der Verordnung
- Datenschutz ab 2018
- Direkt in allen Mitgliedsstaaten gültige Verordnung statt nur indirekt gültiger Datenschutz-Richtlinie 95/46/EG
- Einheitliche Datenschutzvorschriften in der EU
- Erweiterung von EU-Vorschriften auf Auftraggeber in Drittstaaten
- Konzentration der Aufsicht für Organisationen auf die nationale Datenschutzbehörde des Mitgliedsstaates des Hauptsitzes
- Recht auf Vergessen werden
- Recht auf Datenübertragbarkeit
- Notifizierung von Datenschutzverletzungen
- Definition von Binding Corporate Rules
- Datenschutzrechtliche Zustimmung nur noch explizit möglich
- Datenschutz bei Kindern
- Verarbeitung von sensiblen Daten wird untersagt (ausgenommen explizit erwähnte Ausnahmen)
- Dokumentationspflicht in den Unternehmen
- Datenschutzkonzept
- Sicherheitskonzept
- Ggf. Pflicht des Auftraggebers zur Erstellung einer Datenschutz-Folgenabschätzung nach Artikel 33 statt Vorabkontrolle
- Einrichtung verpflichtender Datenschutzbeauftragter (neue Grenzen)
- Datenschutz durch Technik
- Pflicht zur Überprüfung der verwendeten technischen Mittel zum Schutz der Daten
- Prüfung des gesamten Lebenszyklus der Daten von der Entstehung bis zur Löschung
- Meldung von Sicherheitsvorfällen
- Datenschutzaudit
- Aufgaben Datenschutzbeauftragter

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Die neue EU-Datenschutzgrundverordnung

Ich buche das Seminar
Die neue EU-Datenschutzgrundverordnung

☐ 21.09.16 in Frankfurt
zum Preis von € 1.090,-- netto

☐ Bitte buchen Sie mir ein Hotelzimmer

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

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

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

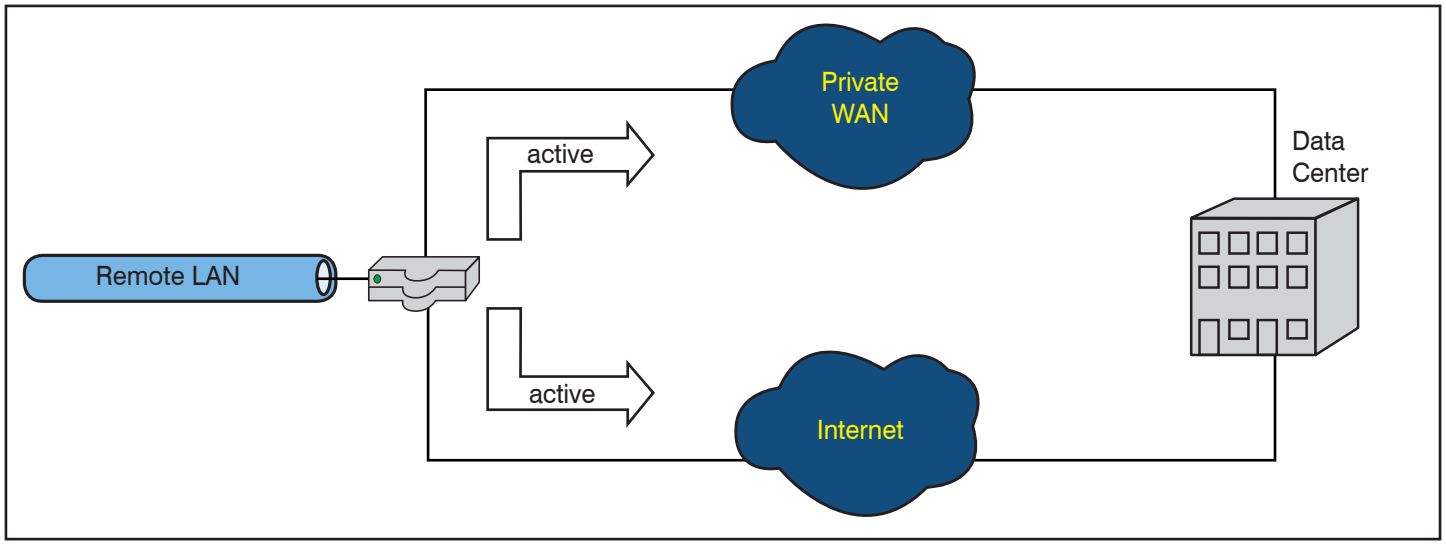

Abbildung 1: Nutzung von WAN und Internet im Modus aktiv-aktiv

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.

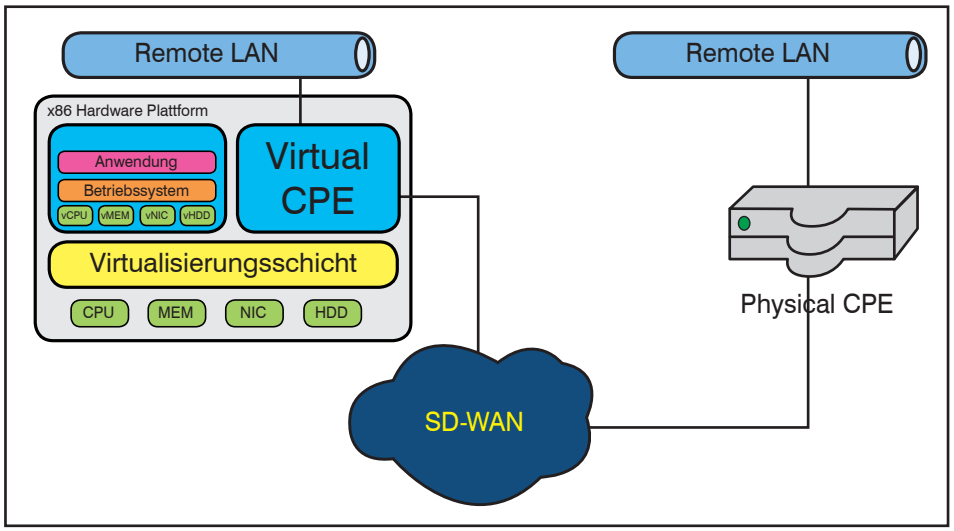

Abbildung 2: Nutzung physischer und logischer WAN-Komponenten

Software-Defined Wide Area Network

In einem Beitrag vom Juni dieses Jahres wurde darauf eingegangen, warum die Steuerung von Unternehmensnetzen problematisch sein kann [2]. Gleichwohl kann in bestimmten Fällen die Steuerung des WAN durch Anwendungen sinnvoll sein.

Ein relativ einfaches Modell der WAN-Steuerung durch Anwendungen wird bereits seit Jahren praktiziert, ohne dass dafür der Begriff Software-Defined WAN genutzt wird. Im WAN wird häufig Quality of Service (QoS) genutzt. QoS im WAN sieht in der Regel vor, dass der Verkehr in verschiedene Klassen unterteilt wird. Das WAN behandelt verschiedene Verkehrsklassen unterschiedlich. Zum Beispiel können die WAN-Komponenten dafür sorgen, dass die zu einer Echtzeitanwendung gehörenden Pakete sonstigen Verkehr überholen und somit schneller am Ziel sind. Die Zugehörigkeit zu einer Verkehrsklasse kann entweder von Netzkomponenten anhand bestimmter Merkmale (IP-Adressen, TCP/UDP-Ports) erkannt oder von Anwendungen vorgegeben werden. Das erstere Modell ist manchmal nicht möglich. Netzkomponenten fehlt häufig der Einblick in die Mechanismen der Anwendungen. Zum Beispiel können Anwendungen dynamische TCP/UDP-Portnummern verwenden. Ferner kann es sein, dass ein Gerät mit ein und derselben IP-Adresse Daten sendet, die unterschiedlichen Verkehrsklassen zuzuordnen sind. In solchen Fällen ist es hilfreich, wenn die Anwendung selbst die Pakete klassifiziert und entsprechend markiert. Dann können sich Netzkomponenten nach diesen Markierungen richten und zum Beispiel die Pakete anhand solcher Markierungen in unterschiedliche Warteschlangen einordnen.

Natürlich ist dies auch eine Frage der Vertrauensstellung. Wer Endgeräte und Anwendungen manipulieren kann, wäre damit auch in der Lage, das Verhalten des Netzes zu steuern. Daher setzt die WAN-Steuerung durch Anwendungen voraus, dass die Endgeräte und damit die Anwendungen einer vertrauenswürdigen administrativen Hoheit unterliegen.

Ist diese Bedingung erfüllt, kann die Steuerung des WAN durch Anwendungen nicht nur hinsichtlich QoS erfolgen. Auch Policy-Based Routing kann sich nach denselben Markierungen richten. Pakete einer bestimmten Verkehrsklasse können über das private WAN geleitet werden, während andere Markierungen zum Routing über das Internet führen.

Ein weiteres Beispiel sind Managementanwendungen. Solche Anwendungen können speziell für das WAN konzipiert

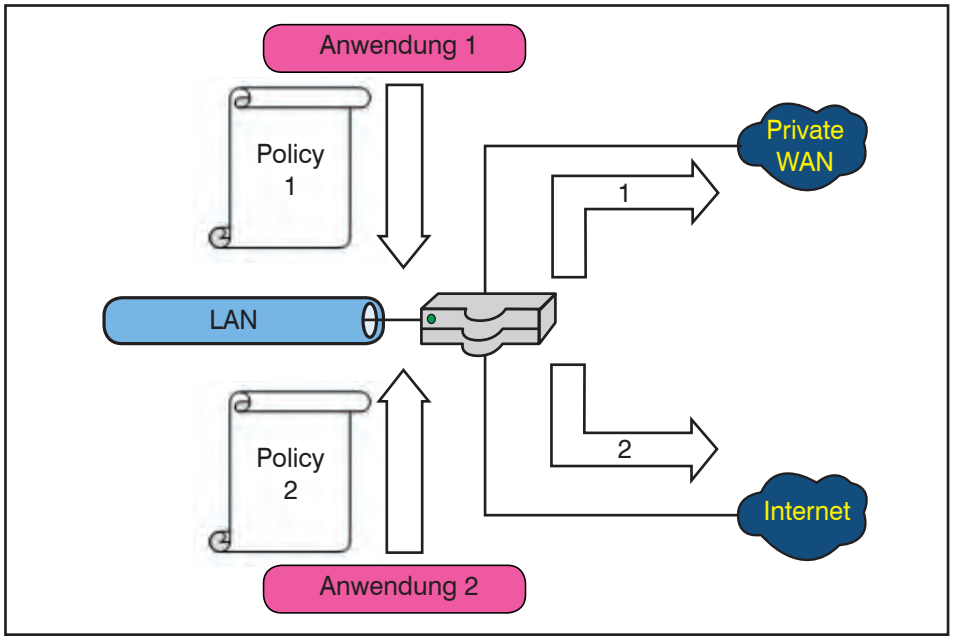

Abbildung 3: WAN-Steuerung anhand der Richtlinien von Anwendungen

oder Teil umfangreicherer Lösungen für die Bereitstellung von Diensten und Applikationen sein.

Abbildung 3 stellt vereinfacht dar, wie Anwendungen in einem Software-Defined WAN die Edge Devices durch Vorgabe von Richtlinien (Policies) steuern können.

Wie aus der Abbildung 3 hervorgeht, geben die Anwendungen 1 und 2 dem WAN Edge Device zwei verschiedene Richtlinien vor. Die WAN-Komponente kann zum Beispiel anhand dieser Richtlinien den Verkehr der Anwendung 1 über das WAN und den Verkehr der Anwendung 2 über das Internet führen. Die Vorgabe der Richtlinien kann anhand einfacher Mechanismen wie Markierungen im IP Header, speziell im Feld Differentiated Services (DS), erfolgen.

Visualisierung, Sicherheit, QoS

Wie erwähnt schließt Policy-Based Routing auch QoS ein. QoS gilt ohnehin als ein Merkmal von Software-Defined WAN. Natürlich gilt die Einschränkung, dass das Internet kaum QoS-Mechanismen unterstützt. QoS-Parameter können im besten Fall für die „letzte Meile“ zwischen dem Kunden und dem Internet Service Provider (ISP) vereinbart werden. Selbst das scheitert oft daran, dass ein ISP nicht bereit ist, auf der eigenen Plattform individuelle Einstellungen für Kunden vorzunehmen.

So ist QoS-Unterstützung im Software-Defined WAN oft gleichbedeutend damit, dass Bestandteil des Software-Defined WAN auch eine private WAN-Struktur ist. Diese muss anders als das Internet QoS unterstützen.

Zusätzlich müssen auch die WAN-Edge-Komponenten QoS unterstützen. Gerade auf der letzten Meile kann es Engpässe geben. Deshalb muss das Edge Device in der Lage sein, Pakete zu priorisieren und bei Engpässen der WAN-Zuleitung Pakete höherer Priorität mit Vorrang übertragen.

Daher kommt man im Software-Defined WAN an gewissen intelligenten Funktionen der Edge Devices nicht vorbei. Wenn diese aber die Intelligenz besitzen, die für QoS erforderlich ist, können sie gleich weitere Funktionen wahrnehmen.

Dazu gehören wie bereits erwähnt Sicherheitsfunktionen. Neben Verschlüsselung und VPN-Tunnelbildung über das Internet können Sicherheitsfunktionen im Software-Defined WAN auch die Abwehr von Denial of Service, Firewalling und Intrusion Prevention umfassen. Weil die Edge-Komponenten im Software-Defined WAN das interne Netz neben dem privaten WAN auch mit dem Internet verbinden, kommt den Sicherheitsfunktionen der CPE-Komponente große Bedeutung zu.

Zusätzlich kann die Intelligenz von WAN-Edge-Komponenten für die Visualisierung des WAN-Verkehrs genutzt wird. Jedem Netzexperten sind Standards für die Nutzung von Netzkomponenten zur statistischen Auswertung des Verkehrs bekannt, beispielsweise NetFlow, sFlow oder IPFIX. WAN-Edge-Komponenten können Daten über die übertragenen Pakete sammeln und gemäß einem dieser Standards zen-

tralen Instanzen zukommen lassen. Statistiken über den Datenverkehr im Netz kommen der vorausschauenden Netzplanung, der Fehlersuche und Sicherheitsprüfungen zugute. Insbesondere Letzteres liegt im Trend. Statistische Aufbereitungen von Verkehrsdaten können die Erkennung von Anomalien erleichtern und somit einen Beitrag zur Abwehr von Angriffen leisten. Nicht von ungefähr beobachten wir im Markt, wie zum Beispiel Netflow-Analysatoren in Sicherheitslösungen eingebunden werden. Ein Security Information and Event Management (SIEM), das auch die statistische Analyse von Verkehrsdaten einschließt, kann diese Analyse mit anderen Informationen wie zum Beispiel Logs von Sicherheitskomponenten korrelieren.

Abbildung 4 stellt die Nutzung der Intelligenz im WAN Edge für Visualisierung, Sicherheit und QoS dar. Voraussetzung dafür sind natürlich neben den erforderlichen Funktionen der CPE-Komponenten auch Softwarewerkzeuge, die an zentraler Stelle die Daten sammeln und auswerten bzw. für die Verteilung von Richtlinien im Netz sorgen.

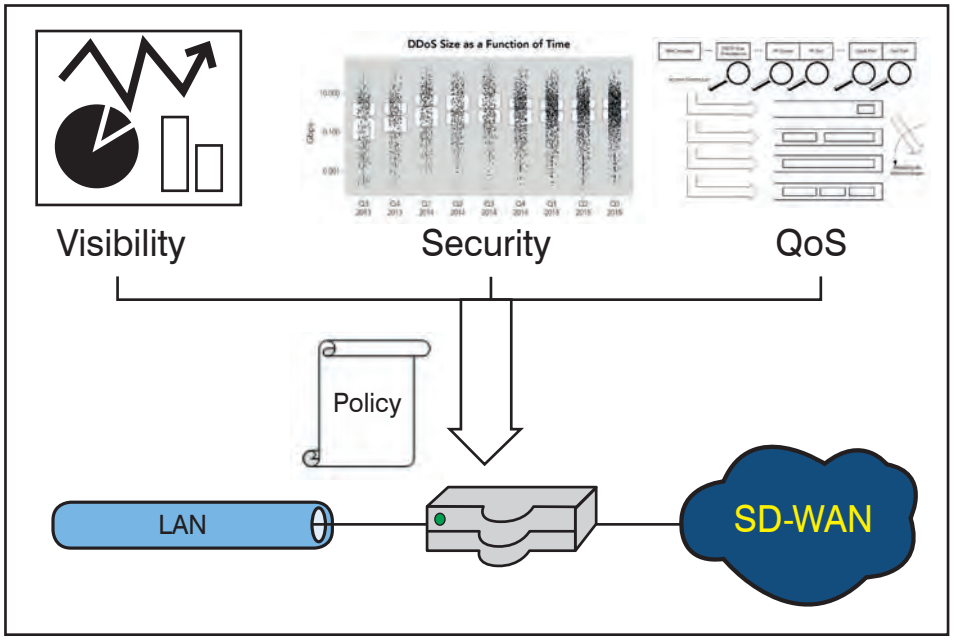

Abbildung 4: Nutzung der Intelligenz im WAN Edge für Visualisierung, Sicherheit und QoS

Hochverfügbarkeit im Software-Defined WAN

Eingangs haben wir bereits die Erhöhung der Verfügbarkeit als eine der Hauptmotivationen für Software-Defined WAN erwähnt. Man kann sich das Software-Defined WAN als eine Art Overlay-Struktur vorstellen. Diese Struktur ist eine logische Instanz, die als solche zentral konfiguriert wird und die Ressourcen physischer Strukturen nutzt, die sie überlagert (daher der Begriff Overlay). Andere Beispiele für Overlay-Strukturen sind virtuelle Maschinen bzw. virtuelle Speichermedien. Virtuelle Maschinen sind logische Konstrukte, die auf verschiedenen physischen Instanzen residieren können. Sie können von einzelnen Hardware-Komponenten unabhängig sein. Dadurch können sie auch bei Ausfall der Hardware weiter funktionieren, indem sie einfach eine andere Hardware nutzen.

Gleiches gilt für logische Speicherbereiche. Überlagert man physische Speichermedien mit logischen, kann man hochverfügbare Speichermedien als logischen Speicher organisieren. Logischer Speicher kann mehrere Speichermedien nutzen und Daten zwischen diesen replizieren. Fällt ein physischer Speicher aus, nutzt der logische Speicher andere physische Speicher im Verbund.

Der Ansatz ist auf das Netz übertragbar. Ein Overlay-Netz ist ein logisches Konstrukt. Es nutzt physische Netze, ist aber von einzelnen physischen Pfaden unabhängig. Fällt ein Pfad aus, funktioniert das logische Konstrukt weiter, indem es auf andere Pfade ausweicht.

Beim Software-Defined WAN nutzt das logische Konstrukt in der Regel ein privates WAN und das Internet. Das einfachste Modell dafür ist älter als der Begriff Software-Defined WAN und besteht aus Internet-VPN-Backup für ein WAN.

Wie bereits erwähnt geht aber Software-Defined WAN weiter. Es sieht die gleichzeitige Nutzung von privatem WAN und Internet als Übertragungsmedien vor. Damit bietet Software-Defined WAN keine reine Hochverfügbarkeitslösung, sondern eine solche im Modus aktiv-aktiv. Die Netzlast wird auf die verschiedenen Medien WAN und Internet verteilt.

Eine schematische und vereinfachte Darstellung dieses Mechanismus gibt die Abbildung 5 wieder.

Wie in der Abbildung 5 dargestellt kann eine Lösung für Software-Defined WAN auch Load Balancing zwischen dem privaten WAN und dem Internet einschließen. Dabei angewandte Kriterien können komplexer als Policy-Based Routing anhand einer reinen Applikationserkennung sein.

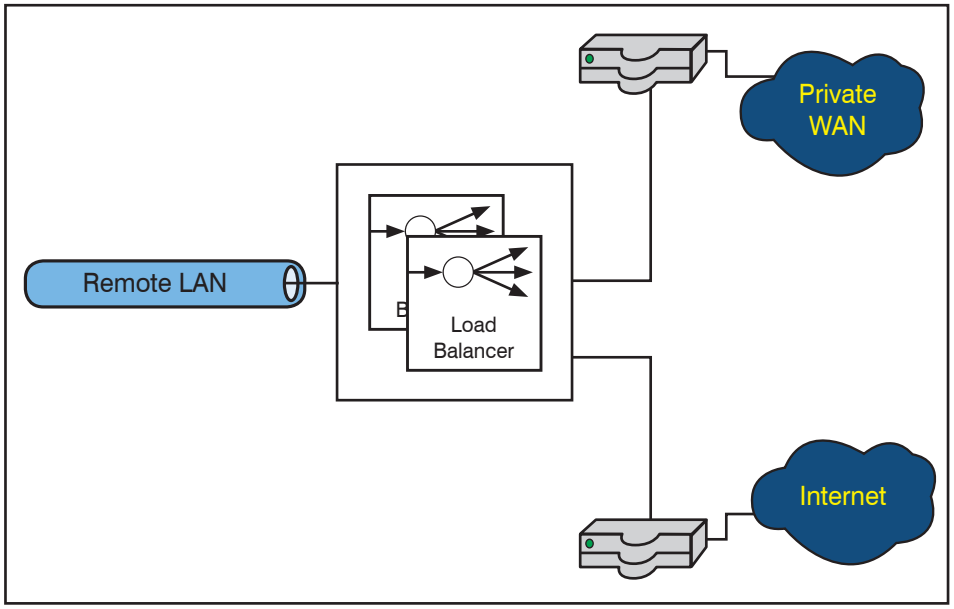

Abbildung 5: Hochverfügbarkeit im Software-Defined WAN

Load Balancing kann es auch ohne Hochverfügbarkeit geben. Datenströme einer bestimmten Anwendung können zum Beispiel ausschließlich über das Internet übertragen werden. Fällt der Internetweg aus, sind die entsprechenden Applikationen nicht verfügbar. Denkbar ist das Szenario, dass zum Beispiel Videokonferenzen nur über das Internet möglich sind.

Angesichts der wachsenden Bedeutung der standortübergreifenden Kommunikation für die Arbeitsfähigkeit von Unternehmensstandorten sucht jedoch eine zunehmende Zahl von Unternehmen eine Hochverfügbarkeitslösung für das eigene WAN. Da die hochverfügbare Auslegung des privaten WAN oft mit einer wesentlichen Erhöhung der Kosten verbunden ist, kann die Kombination aus WAN und Internet eine angemessene Antwort auf diese Anforderung sein.

Daher kommt es auf die dynamischen Mechanismen an, die bei Ausfall eines der Pfade die Nutzung des jeweils anderen einfädeln. Dynamische Routing-Protokolle können dazu genutzt werden. Mit zusätzlichen Maßnahmen wie Bi-Directional Forwarding Detection (BFD) kann die Umschaltung zwischen verschiedenen Pfaden beschleunigt werden.

In der Planung jeder Hochverfügbarkeitslösung durch Nutzung von WAN und Internet ist zu berücksichtigen, dass die häufigsten Ausfallursachen im WAN auf der Strecke zwischen dem Point of Presence (PoP) des Providers und dem Kundenstandort geortet werden. Vom PoP aufwärts (Richtung Backbone-Plattform des Providers) werden in der Regel redundante Strukturen (kanten- und knotendisjunkt) genutzt.

Eine Hochverfügbarkeitslösung bestehend aus WAN und Internet ist nur dann von hoher Wirkung, wenn für WAN und Internet nicht dasselbe Kabel oder dieselbe Trasse genutzt wird. Insofern löst das Software-Defined WAN nicht das Problem eines Gebäudes, das mit dem Rest der Welt über einen einzigen physischen Weg verbunden ist. Fällt dieser Weg aus, ist das Gebäude vom Rest der Welt abgeschnitten.

Abhilfe können doppelte Hauseinführungen, kantendisjunkte Kabelführung auf öffentlichem Grund und Anschluss an verschiedene PoPs des oder der Provider leisten. Ist dies nicht möglich oder unbezahlbar, bleibt immer noch der Funkweg, entweder über Mobilfunk (insbesondere wenn die Versorgung mit hoher Bitrate zum Beispiel über LTE gegeben ist) oder andere Varianten wie Richtfunk.

Die Kombination aus der WAN-Plattform des einen mit der Internet-Plattform des anderen Providers kann für mehr Verfügbarkeit sorgen. Entscheidend ist, dass die beiden Plattformen möglichst vollständig unabhängig voneinander sind. Oft nutzen verschiedene Provider in der letzten Meile die Dienste desselben Carriers. Für international agierende Unternehmen ist es daher wichtig sicherzustellen, dass die Kombination aus WAN und Internet an einem bestimmten Standort auch auf der letzten Meile mehr Diversität bedeutet. In diesem Zusammenhang ist die Informationspolitik der Provider von großer Bedeutung. Unternehmen müssen von Providern Informationen darüber einfordern, über welche Wege ihre Standorte mit der Netzplattform des Providers verbunden sind. Zu diesen Informationen gehört auch die genaue Streckenführung.

Layer-2-WAN

Die meisten Weitverkehrsnetze sind Gebilde auf der Ebene der Protokollschicht 3, d.h. der Netzwerkschicht und konkret der Ebene des Internet Protocol (IP). Dies gilt nicht nur für das Internet, sondern auch für die meisten privaten WAN-Plattformen wie zum Beispiel Multi-Protocol Label Switching (MPLS).

Als Eigenschaft eines Software-Defined WAN gilt die Unterstützung von Layer-2-Verbindungen über das WAN neben der klassischen Layer-3-Verbindung. Ein Software-Defined WAN, das sowohl Layer-3- als auch Layer-2-Verbindungen unterstützt, ist in der Abbildung 6 dargestellt.

Neben den klassischen Layer-3-Varianten sind auch Layer-2-Plattformen als private WAN verfügbar. Auch wenn MPLS als de facto Standard für private WAN eine Layer-3-Plattform ist, können verschiedene Techniken für Layer-2-WAN genutzt werden. Eine Variante nutzt MPLS und heißt Virtual Private LAN Service (VPLS). Andere Layer-2-WAN-Verfahren sind Shortest Path Bridging (SPB) und Ethernet over Optical Transport Network (OTN).

Da ein Software-Defined WAN eine Overlay-Struktur darstellt, die das Internet und das private WAN überlagert, ist es naheliegend, für die Layer-2-Overlay-Bildung ein einheitliches Verfahren zu nutzen, welches sowohl über jedes private WAN als auch über das Internet funktionieren kann.

Das physische Medium Internet ist und bleibt ein Layer-3-Medium. Insofern muss ein Layer-2-Protokoll wie Ethernet im Internet Tunnelmechanismen nutzen. Ein Beispiel für eine Technologie, die diese Anforderung erfüllt, ist OpenVPN. Wie aus der Bezeichnung hervorgeht, handelt es sich dabei um eine frei verfügbare Lösung. Die Tunnelbildung bei OpenVPN erfolgt mittels Secure Socket Layer (SSL) bzw. Transport Layer Security (TLS). Sowohl Client-to-Site- als auch Site-zu-Site-Anbindungen sind mit OpenVPN möglich.

Eine andere Frage ist, welche Motivation es für Layer-2-Verbindungen über das WAN geben kann. Häufig wird als Einsatzgebiet dafür die Bildung von Layer-2-Strukturen im RZ-Bereich genannt, die

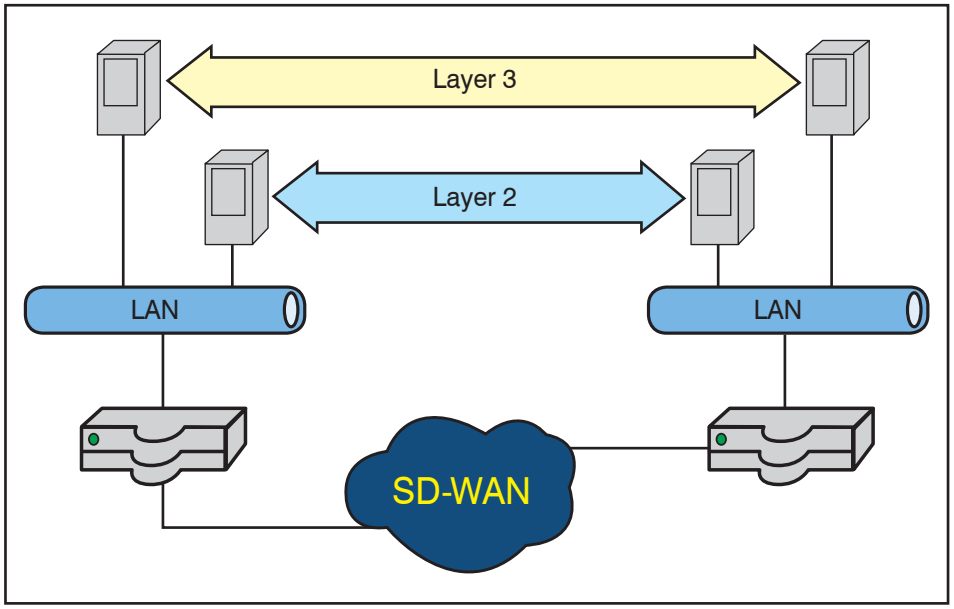

Abbildung 6: Layer-2- und Layer-3-Verbindungen über Software-Defined WAN

für die Verlagerung virtueller Maschinen erforderlich sind. Mittlerweile unterstützen jedoch führende Anbieter von Virtualisierugslösungen wie Microsoft und VMware auch die Nutzung von Layer-3-Netzen zwischen den Virtualisierungshosts. Die Layer-2-Overlays werden dann auf anderer Ebene gebildet, nämlich zwischen den Hypervisor-Instanzen.

Einige Unternehmen legen Wert darauf, die Hoheit über die Routing-Instanzen im WAN zu behalten und mit Providern keine Routing-Informationen austauschen zu müssen. Dieser Anforderung wird ein Provider nur mit einer Layer-2-Platform gerecht. Dies kann ein weiterer Grund für den Einsatz eines Layer-2-WAN sein.

Reporting

Unternehmen richten steigende Anforderungen an WAN Reporting, zum Beispiel zu folgenden Zwecken:

- Kontrolle von Service Level Agreements (SLAs) einschließlich Parameter wie Verfügbarkeit
- Netzlastanalyse für Kapazitätsmanagement einschließlich Reaktion auf Engpässe und Identifikation der Ursachen hohen Ressourcenverbrauchs
- Erkennung von Anomalien
- Untersuchung von Fehlern und Problemen

Das Software-Defined WAN mit seinen intelligenten Komponenten bietet wie bereits erwähnt die Basis der Datensammlung, die als Grundlage von Reports genutzt werden kann.

Reports sind auf verschiedenen Ebenen erforderlich:

- Site Level: Es kann notwendig sein, Reports über die WAN-Anbindung einzelner Standorte zum Beispiel mit der Verfügbarkeit und Auslastung einer solchen Anbindung zu erstellen.
- Application Level: Das Netzverhalten einer bestimmten Anwendung kann von Interesse sein. Zum Beispiel kann es für die Optimierung einer Applikation relevant sein zu erfahren, wie sich Maßnahmen auf der Ebene der Applikation auf die Netzlast im WAN auswirken.
- VPN Level: In einem mandantenfähigen WAN können verschiedene VPNs gebildet werden. Reports auf VPN-Ebene können erforderlich sein, um jedem Mandanten den entsprechenden Report bieten zu können.

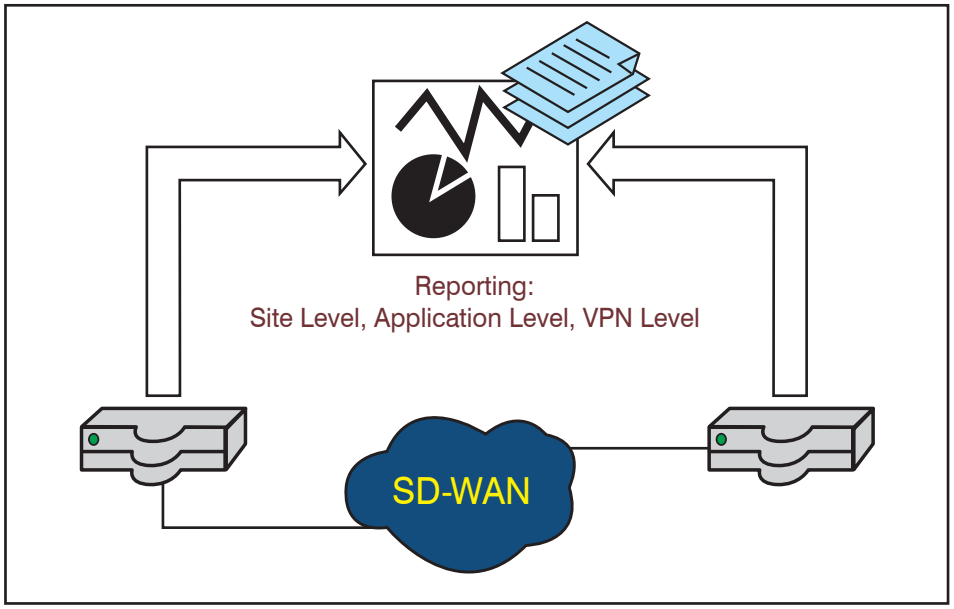

Abbildung 7: Reporting im Software-Defined WAN

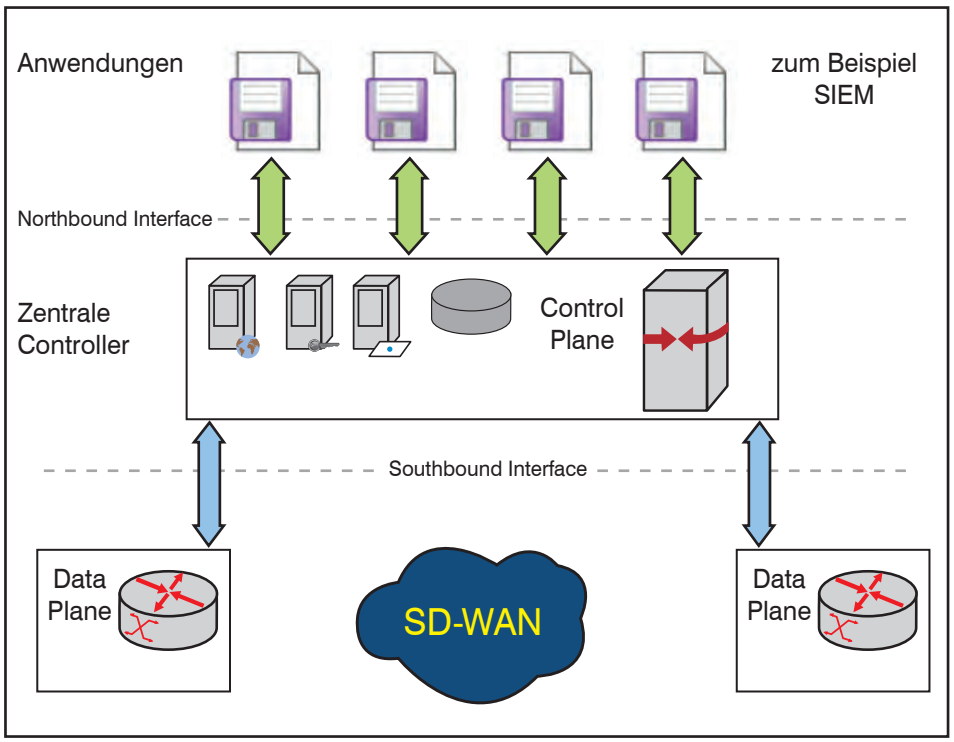

Abbildung 8: Northbound Interface

Neben den Datensammelfunktionen der WAN-Edge-Komponenten benötigt man daher eine Reporting-Lösung, die die von den WAN-Komponenten gelieferten Daten auswertet und in Reports zusammenfasst. Eine solche Lösung ist in der Abbildung 7 angedeutet.

Northbound Interface

Im Zusammenhang mit der richtlinienbasierenden WAN-Steuerung haben wir bereits das Northbound Interface erwähnt, das von Applikationen für die Steuerung des Netzes genutzt werden kann.

Im Zusammenhang mit Software-Defined WAN sind Ansätze denkbar, die das Northbound Interface analog zum Ansatz OpenFlow über eine zentralisierte Control Plane zur Verfügung stellen. Eine Motivation hierzu ist die Nutzung standardisierter Schnittstellen, die es ermöglichen, Lösungen für die Netzsteu-

erung nach eigenen Bedürfnissen zu erweitern.

Inwieweit sich die Nutzung von offenen Controller-Lösungen mit standardisierten Schnittstellen im Bereich Software-Defined WAN durchsetzen wird, ist noch abzuwarten. Außer den Service-Providern hat kaum ein Unternehmen die personellen Ressourcen, das Know-how und die strategische Ausrichtung, die erforderlich sind, um die WAN-Steuerung mit eigener Programmierleistung an individuelle Bedürfnisse anzupassen. Die meisten Unternehmen bevorzugen fertige Lösungen, die sie ohne großen Anpassungsaufwand einsetzen können.

Das Northbound Interface zur Steuerung des Software-Defined WAN ist in der Abbildung 8 dargestellt. Wie bereits im Zusammenhang mit Sicherheitsanforderungen an das Software-Defined WAN erwähnt kann zum Beispiel eine SIEM-Lösung über einen zentralen Controller Informationen über den WAN-Verkehr erhalten und mit anderen Informationen korrelieren, um sicherheitsrelevante Auswertungen durchzuführen. Aber auch Lösungen sind denkbar, die aktiv auf das Netz Einfluss nehmen können. Ein denkbares Beispiel ist ein Intrusion Prevention System (IPS), das bei Erkennung eines Angriffsmusters über den Controller entsprechende Maßnahmen wie die Blockierung oder Umleitung von Datenströmen veranlassen kann.

Zero-Touch Provisioning

Die Eigenschaft von Software-Defined WAN, sowohl physische als auch virtuelle CPE-Komponenten zu unterstützen, wurde bereits erwähnt. Durch den Einsatz von virtuellen Komponenten auf Basis von Standard-Hardware kann der WAN-Betreiber von logistischen Aufgaben im Zusammenhang mit der Auslieferung von proprietärer Hardware entlastet werden. Folglich können WAN-Lösungen schneller und mit geringerem Aufwand realisiert werden.

Hier kommt das Attribut „Software-Defined“ im wahrsten Sinne zur Geltung. Die Trennung der Prozesse für die physische Aufstellung von Komponenten von solchen für die Bereitstellung logischer Funktionen im Software-Defined WAN wird „Zero-Touch Provisioning“ genannt und ist in der Abbildung 9 dargestellt.

Zertifikats- und Schlüsselmanagement

Software-Defined WAN schließt die Nutzung des Internet ein. Wie bereits erwähnt kann es erforderlich werden, dass die WAN-Komponenten den Datenverkehr über das unsichere Internet verschlüsseln.

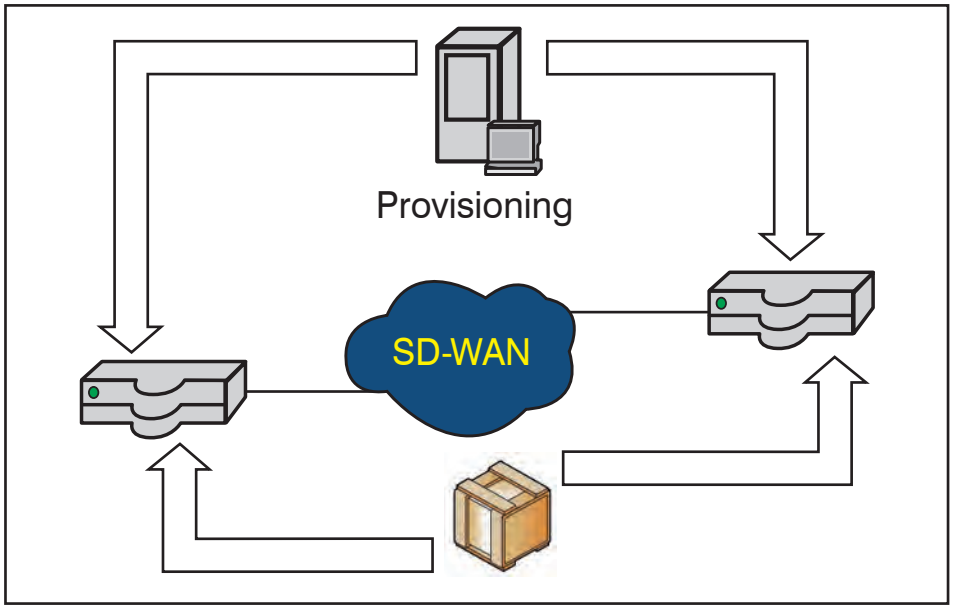

Abbildung 9: Zero-touch Provisioning

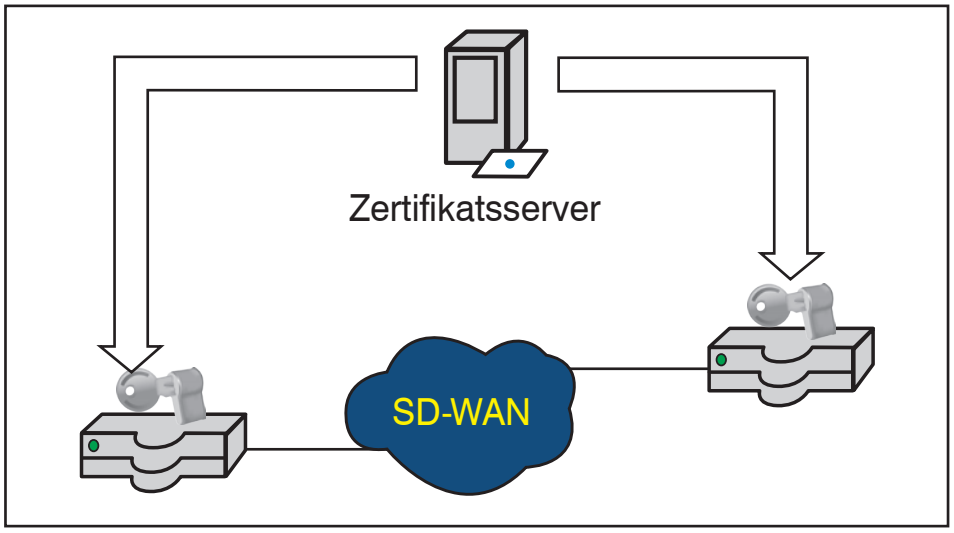

Abbildung 10: Zertifikats- und Schlüsselmanagement

Ein etabliertes Verfahren zur Verwaltung von Schlüsselmaterial ist die Nutzung von Zertifikaten. Komponenten in einem Software-Defined WAN können dieses Verfahren nutzen. Eine zentrale Lösung für die Verwaltung von Zertifikaten ist dazu erforderlich, wie in der Abbildung 10 dargestellt.

Zusammenfassung

Software-Defined WAN ist ein Oberbegriff von Verfahren, die teilweise bereits vor der Einführung dieses Begriffs in Nutzung waren. Wesentliche Eigenschaft von Software-Defined WAN ist die Integration von WAN und Internet. Eine solche Kombination dient dazu, die Verfügbarkeit standortübergreifender Netze zu erhöhen und die wachsenden Leistungs-, Sicherheits- und Effizienzanforderungen an Weitverkehrsnetze zu erfüllen. Der Ansatz dazu ist die Überlagerung des Gesamtkonstrukts aus WAN und Internet mit einer Overlay-Struktur.

Verweise

[1] Moayeri, Behrooz: Redesign von WAN- und Internet-Zugängen, Der Netzwerk-Insider, Mai 2016

[2] Moayeri, Behrooz: Unternehmensnetze folgen nicht immer dem Beispiel der Hyperscaler, Der Netzwerk Insider, Juni 2016.

Sonderveranstaltung

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

Die ComConsult Akademie veranstaltet am 21.09.16 ihre Sonderveranstaltung "Das PSTN stirbt: Die neue Kommunikation mit SIP/IP" in Frankfurt.

Diese Sonderveranstaltung analysiert, wie der Wechsel von PSTN auf All-IP im Unternehmen verläuft. Sie zeigt auf, welche Funktionalität heute erreicht werden kann und mit welchem Aufwand für Anpassung und Fehlersuche zu rechnen ist.

Die Deutsche Telekom hat angekündigt, bis 2018 das klassische PSTN-Netz, respektive analoge und ISDN-Anschlüsse abzuschalten. Dies betrifft alle Unternehmen, die weltweit kommunizieren wollen und müssen.

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

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

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

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

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

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

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

Fax-Anmeldung an ComConsult 02408/955-399

Das PSTN stirbt: Die neue Kommunikation mit SIP/IP

Ich buche das Seminar
Das PSTN stirbt: Die neue Kommunikation mit SIP/IP

☐ 21.09.16 in Frankfurt
zum Preis von € 1.090,--

☐ Bitte buchen Sie mir ein Hotelzimmer

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

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

Standpunkt

Widerstand ist zwecklos: Sicherheitskomponenten in der Cloud??

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

Die Automatisierung für die Einrichtung von Cloud-Diensten erzwingt neue Konzepte, bei denen Sicherheitskomponenten wie Firewalls in Cloud-Architekturen integriert werden. Der Hintergrund ist einfach: Kommunikationsverkehr in der Cloud muss auch in der Cloud gefiltert werden können.

Sichtbar wird dies zunächst bei Plattformen wie OpenStack, die Firewall as a Service (FWaaS) ermöglichen. Wenn per Automatisierung virtualisierte Infrastrukturen eingerichtet bzw. aus Gründen einer besseren Lastverteilung umorganisiert werden müssen, betrifft dies auch Firewalls, für die automatisiert Regelwerke eingerichtet bzw. angepasst werden müssen. Im Extremfall ist die Firewall virtualisierter Bestandteil der Lösung und wird per Automatisierung bei Bedarf als virtuelle Firewall bereitgestellt. Solche Konzepte sind auch unmittelbare Konsequenz von Network Virtualization Overlays (NVOs), die von der zugrundeliegenden physischen Netzinfrastruktur durch Tunnelmechanismen abstrahieren und auf Ebene des Hypervisor logische Netzstrukturen für VMs bereitstellen. Firewalls müssen hier entsprechende Schnittstellen zum Hypervisor haben bzw. (zumindest zu Teilen) Bestandteil des Hypervisor werden, um an den Tunnelendpunkten der Overlay-Struktur den eigentlichen Verkehr filtern zu können. Ein populäres Beispiel ist die VMware NSX Distributed Firewall (DFW), die Bestandteil der VMware NSX Network Virtualization Platform ist.

Solche Konzepte sind Kernelemente eines Software-defined Data Center (SDDC), das seinerseits eine wesentliche Basis für Dienste gleichermaßen in der Private Cloud als auch in der Public Cloud ist. Im Falle einer Public Cloud oder einer Private Cloud bei einem Dienstleister bedeutet dies zwangsläufig, dass Sicherheitskomponenten das eigene Haus verlassen und im Extremfall als Managed Service extern betrieben werden.

Wer nun eine Private Cloud im eigenen Rechenzentrum unterhält, könnte denken, dass man ja nach wie vor jegliche Kontrolle insbesondere über die eigenen Sicherheitskomponenten hat. Dies ist jedoch öfter nicht der Fall:

- Die notwendige Intelligenz von diversen Security-Lösungen kann nicht mehr vollständig lokal gehalten werden, sondern muss kontinuierlich über eine Verbindung zur zentralen Infrastruktur eines Herstellers bzw. Dienstleisters aktualisiert, nachgeladen oder bereitgestellt werden. Im Extremfall sind die lokalen Sicherheitskomponenten nur noch „dumme“ Probes und die eigentliche Intelligenz, die Daten analysiert (z.B. hinsichtlich Anomalien, die vielleicht auf einen zielgerichteten Angriff hindeuten), sitzt irgendwo in der Cloud außerhalb der eigenen Infrastruktur.

- Werkzeuge, die zur Erkennung und Abwehr zielgerichteter Angriffe (Advanced Persitent Threats, APTs) dienen, nutzen inzwischen oft SIEM-Lösungen (Security Information and Event Management) der zweiten Generation, die mit Big Data, d.h. insbesondere mit statistischen Methoden die Vielfalt und Vielzahl an Ereignissen und Protokolldaten zu analysieren, um system- und anwendungsübergreifend Korrelationen und statistische Muster zu erkennen, die auf APTs hindeuten. Woher kommen nun die Parameter für die statistischen Analyse-Modelle (und die Modelle selbst) am besten: Natürlich aus der Cloud.

- Ein weiteres Beispiel in diesem Zusammenhang ist der Schutz vor Angriffen vom Typ Distributed Denial of Service (DDoS). Maßnahmen gegen DDoS in der eigenen Infrastruktur sind oft nicht wirkungsvoll genug, da es bereits in dem Moment, in dem die DDoS-Attacke den eigenen Internet-Zugang erreicht, eigentlich schon zu spät sein kann. Es gibt daher Lösungen, bei denen der eingehende Netzverkehr zunächst über ein Scrubbing Center in der Cloud geleitet wird (siehe z.B. Cloudflare). Im Scrubbing Center kann DDoS-Verkehr erkannt sowie herausgefiltert („abgebürstet“, daher die Bezeichnung) werden und erst dann wird der gereinigte Verkehr in die eigene Infrastruktur geleitet.

Es gibt noch weitere Potentiale: Stellen wir uns ein international operierendes Unternehmen vor. Aufgabe ist die Schaffung eines unternehmensweit standardisierten Internet-Zugangs mit einheitlichen Policies an einem Secure Web Gateway (SWG). Reflexartig wurde hier in der Vergangenheit ein zentraler Internetzugang (der dann natürlich per-se standardisiert ist) gefordert und lokale Internet-Zugänge in den verschiedenen Gesellschaften verteufelt. Der Erfolg solcher Konzepte spricht für sich: Lokale Internetzugänge in Gesellschaften eines Konzerns oder einer Unternehmensgruppe nehmen eher zu als ab, mit der Konsequenz, dass man sich nicht selten von einer Standardisierung immer weiter entfernt. Wie wäre es nun mit einem für alle Clients ortsunabhängig einheitlichen Internetzugang über ein SWG aus der Cloud? Es würde lediglich ein Tunnel über einen beliebigen Internet-Provider zum Cloud Provider benötigt, der das SWG hostet und vielleicht sogar als Managed Service bereitstellt. Damit ist natürlich fast automatisch die Internet-Firewall, über die das SWG auf das Internet zugreift, ebenfalls Bestandteil der Cloud (Konzepte hierzu siehe oben). Insgesamt ist so ein Teil der bis dato lokalen Internet-DMZ in eine Provider Cloud (ggf. sogar in eine Public Cloud) verlagert worden. Dies ist keinesfalls akademischer Natur. Hier sei nur auf den aktuellen Erfolg von zScaler verwiesen.

Natürlich sind die genannten Beispiele von Sicherheitskomponenten und der

Widerstand ist zwecklos: Sicherheitskomponenten in der Cloud

zugehörigen Cloud-Dienste aus einer Sicherheitsperspektive höchst bedenklich, wenn kritische Daten auf diese Weise in die Cloud wandern. Jedoch gibt es auf der anderen Seite einen Sicherheitsgewinn, der vielleicht sogar die damit verbundenen Risiken ausgleicht. Als Beispiel kann der eben genannte standardisierte Internet-Zugang dienen, der einen wesentlichen Gewinn an Informationssicherheit, um den Preis der Auslagerung in die Cloud bedeuten würde.

Es ist also wichtig, hier nicht reflexartig die Cloud zu verteufeln, sondern das Potential insbesondere auch für die Informationssicherheit zu sehen. Es wäre nicht das erste Mal, dass eine eigentlich giftige Substanz in der richtigen Dosierung zur Medizin wird.

Kernelement ist und bleibt dabei stets das Vertrauen in den Cloud Provider und natürlich der entsprechende Nachweis der Vertrauenswürdigkeit. Es gibt mit ISO 27017 “Code of practice for information security controls based on ISO/IEC 27002 for cloud services” zwar inzwischen einen internationalen Standard der ISO-270xx-Serie, der spezifisch für Cloud-Dienste ist und man kann sich als Cloud-Provider sogar nach diesem Standard zertifizieren lassen. ISO 27017 ist jedoch recht allgemein gehalten (und der Detaillierungsgrad der Maßnahmen ist entsprechend grob). Nebenbei bemerkt, auch Google ist nach diesem Standard zertifiziert (siehe **https://cloud.google.com/files/ISO27017_Digital_2016.pdf**). Ob dieser Standard das Vertrauen in Cloud-Dienste signifikant erhöht, wage ich persönlich zu bezweifeln (dieser Standard ist allerdings besser als nichts). In diesem Zusammenhang sei jedoch auf die Initiative „Trusted Cloud“ des BMWi hingewiesen (siehe **https://www.trusted-cloud.de/**), die auch ein eigenes Zertifizierungsprogramm erarbeiten wird. Vielleicht gibt ja hier künftig einen umfassenderen und tiefer gehenden Prüfkatalog für die Cloud-Sicherheit.

Seminar

Aufbau und Management von Internet-DMZ und internen Sicherheitszonen
14.11.-16.11.16 in Bonn

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.

Dieses Seminar analysiert die verschiedenen aktuellen technischen Konzepte und Architekturen für den Aufbau und Betrieb von Internet DMZs und internen Sicherheitszonen. Anhand konkreter Projektbeispiele wird die Umsetzung dieser Konzepte illustriert.

- welche Kernbausteine eines sicheren Internetzugangs notwendig sind
- wie Security Gateways (insbesondere Firewalls) arbeiten, welche Typen es gibt und wie Einsatzszenarien, Aufbau- und Betriebskonzepte aussehen
- wie sich erweiterte Sicherheitsfunktionen wie IPS und Content Security integrieren lassen
- was sich hinter Next Generation Firewalls wirklich verbirgt und wie solche Firewalls arbeiten
- wie mit Virtualisierungstechniken in Internet-DMZs und internen Sicherheitszonen umgegangen werden kann
- wie sich der Aufbau von internen Sicherheitszonen von einer Internet-DMZ unterscheidet und wie mit den hohen Anforderungen an Verfügbarkeit und Leistung umgegangen wird
- wie Internet-DMZs und interne Sicherheitszonen auf eine sichere Weise betrieben werden können und wie dabei Administration, Überwachung und Datensicherung durchgeführt werden können
- wie ein sicherer Fernzugriff aufgebaut werden kann, welche VPN-Technologien aktuell eingesetzt werden und wie typische Einsatzszenarien aussehen
- wie Terminal Server und VDI für einen sicheren Fernzugriff genutzt werden können
- welche Methoden zur Absicherung von E-Mail-Kommunikation und Web-basierten Applikationen existieren
- wie Cloud Computing den Aufbau von Internet-DMZs und internen Sicherheitszonen beeinflusst

Dieses Seminar richtet sich an IT-Sicherheitsbeauftragte, Administratoren, Projektleiter und Verantwortliche für die Architektur, Planung, Einführung und Betrieb von Kommunikationsumgebungen.

Referenten: Dr. Simon Hoff, Dipl.-Math. Simon Wies
Preis: € 1.890,- netto

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

Aktueller Kongress

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

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

Das diesjährige UC-Forum analysiert die herausragenden Trends für UC und VoIP und gibt Empfehlungen für Projekte, Technologie-Auswahl und Investitionen. Das dominante Thema ist weiter hin All-IP, sprich die Abschaltung der ISDN- und PSTN-Infrastruktur. Diese geht einher mit einer Welle neuer Dienste und einer Neugestaltung des Mobilfunks. Gleichzeitig rücken Technologien wie Session Border Controller SBC und auch SIP in den Mittelpunkt. Sie entscheiden mehr oder weniger über die Zukunftsfähigkeit moderner UC-Lösungen.

Dabei darf nicht übersehen werden, dass der Markt weiterhin im Wandel ist. Die Übernahme von Polycom durch Mitel ist dabei nur die Spitze des Eisbergs und ein Vorzeichen weiterer wesentlicher Änderungen. Ohne Zweifel wird die zunehmende Bedeutung von Cloud-basierten UC-Leistungen zu weiteren Verwerfungen führen.

Wir analysieren dementsprechend auf dem UC-Forum 2016 für Sie:

- Wo steht der Markt, wie verändert sich die Position der Hersteller, wer hat im Moment die beste Lösung?

- Session Border Controller: Markt und Technik einer Schlüsseltechnologie
- SIP Connect 2.0: genügt der Standard endlich den Ansprüchen?
- Migration im Enterprise und KMU Umfeld: was hat sich bewährt, was ist kritisch?
- Spezialfälle und Sonderschaltungen: wie funktioniert das? (Beispiele: E-Cash, Gefahrenmeldeanlagen)

Mit den aktuellen Änderungen der Technik ändern sich auch die Arbeitsplätze. Dies generiert neue Chancen für mehr Effizienz bei sinkenden Kosten, aber es generiert auch eine Reihe ernst zu nehmender Probleme. Gerade hier hat Microsoft in diesem Jahr eine Reihe von interessanten Ankündigungen und Produkten lanciert, die wir natürlich genauer analysieren möchten. Zudem sind jetzt auch die WebRTC-basierten Produkte Unify Circuit, Cisco Spark und Mitel MiCollab verfügbar, die ja eine neue Art der Kommunikation und Kollaboration mittels Browser-Technologie ermöglichen. Dieser Entwicklung tragen wir mit unserem Zusatztag am dritten Tag der Veranstaltung Rechnung, für den wir alle relevanten Anbieter auf der Basis eines RFI zu einem Wettbewerb um die beste Lösung einladen. Der Zusatztag **"Was bringt der Arbeitsplatz der Zukunft"** - Neue und aktuelle Kommunikations- und Kollaborations-Lösungen im Vergleich - inkl. Live Demo und Hands On" empfehlen wir jedem Teilnehmer, er kann optional gebucht werden.

Als Sonderthemen haben wir für das diesjährige Forum adressiert:

- IT-Compliance
- SDN in UC Projekten mit Microsoft Skype for Business
- Qualitätssicherung durch VoIP Monitoring

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

Fax-Anmeldung an ComConsult 02408/955-399

ComConsult UC-Forum 2016

Ich buche den Kongress
ComConsult UC-Forum 2016

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

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

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

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

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

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

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.

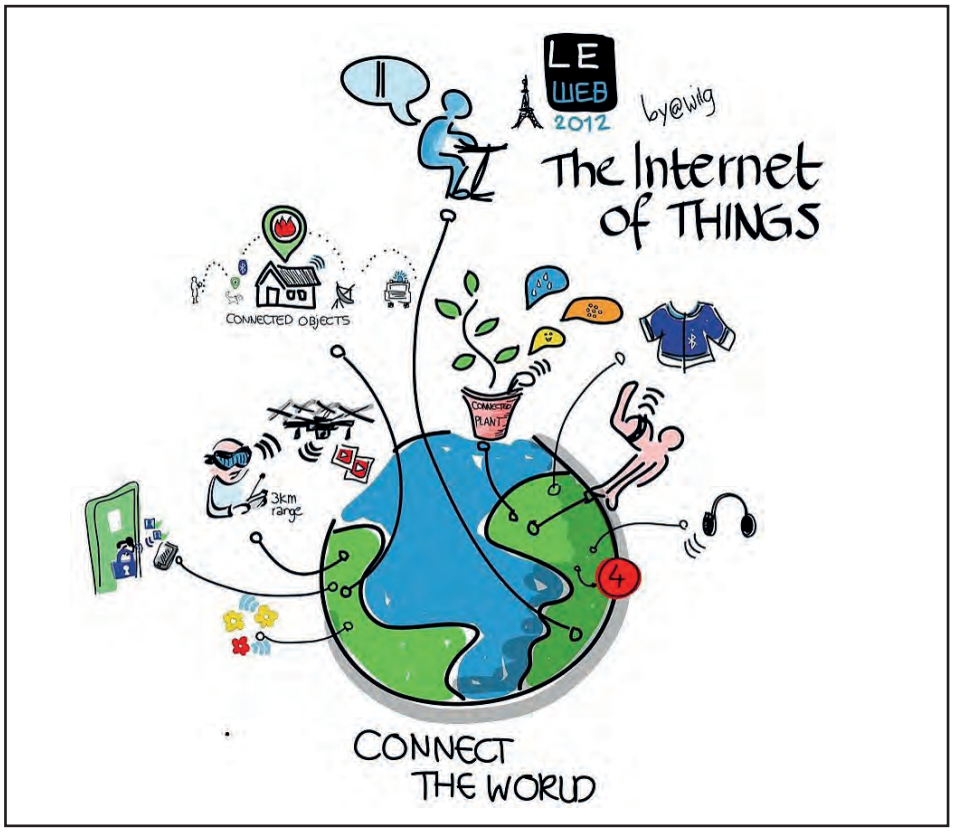

Abbildung 1: Die Vernetzung der Welt

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

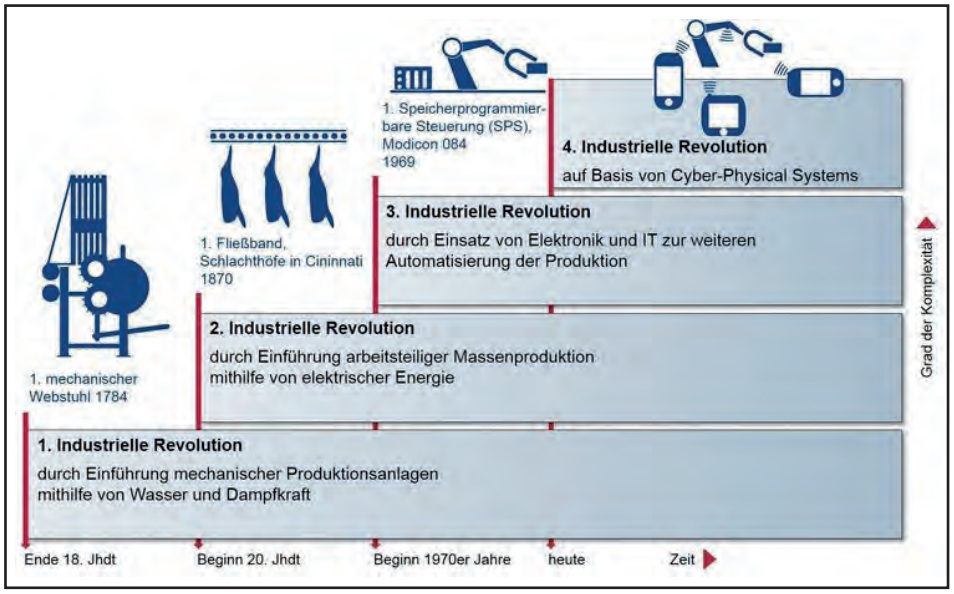

Abbildung 1.1: Industrielle Revolutionen

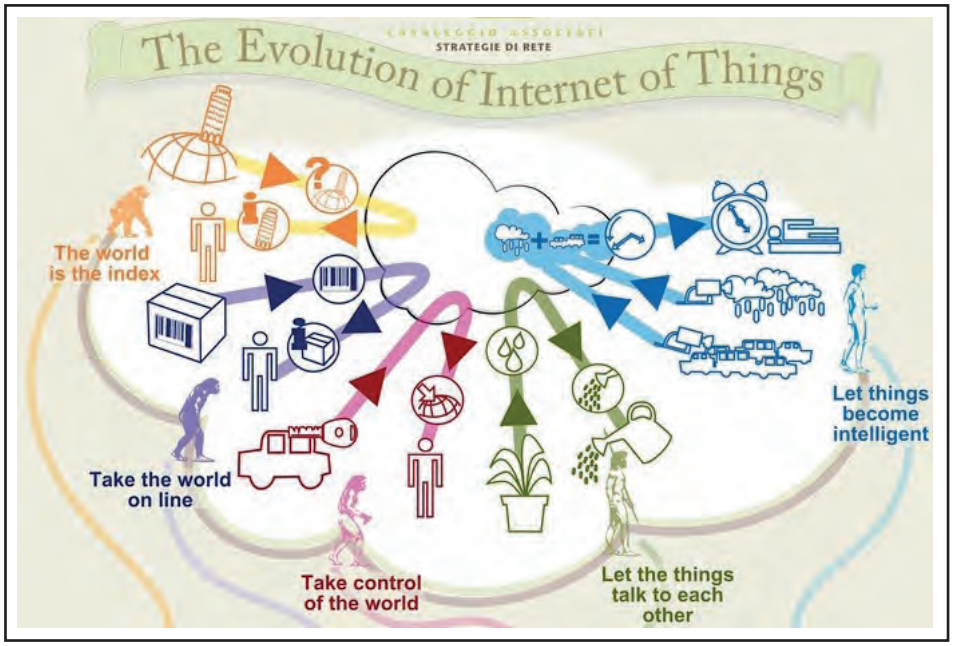

Abbildung 1.2: Einsatzbereiche für IoT

werden. EVU-Leitsysteme werden durch Trendberechnungen auf Basis der abgerufenen Leistungen (Smart-Metering) hinsichtlich ihrer Einspeisungs-Leistung vorausschauend gesteuert. Hier kommunizieren intelligente Objekte mit dem Netz und liefern Informationen, die als "neue Wissensbasis" weiterverarbeitet werden können.

Die oben beispielhaft dargestellten Anwendungsbereiche erstrecken sich über die verschiedensten, um nicht zu sagen fast alle Geschäftsbereiche:

- Gebäude
- Energie
- Verbraucher
- Gesundheit
- Industrie
- Transport
- Einzelhandel
- Öffentliche Sicherheit
- IT und Netze

Markt und Zahlen

Gartner prognostiziert für 2020, dass 25 Mrd. Objekte via Internet vernetzt sein werden, das entspricht im Vergleich zu 2009 einem Faktor 30 (heute sind es 15 Mrd. vernetzte Objekte). Schätzungen von Cisco und Intel gehen sogar von 50 bis 200 Mrd. vernetzten Objekten aus.

Das Marktvolumen für IoT-Dienstleistungen schätzt Gartner auf 69,5 Mrd. USD in 2015 und 263 Mrd. USD in 2020, IDC schätzt sogar 1,7 Bio. USD (ausgehend von 656 Mrd. in 2014). Hierbei werden Verbraucher-Applikationen die Anzahl vernetzter IoT-Geräte zwar weiter in die Höhe treiben, Unternehmen werden jedoch mit IoT den größten Umsatzanteil erzeugen.

Nach einer Telefonica-Untersuchung werden in 2020 werden 90% aller Autos vernetzt sein (ausgehend von 2% in 2012; Quelle: Telefonica). Der Wearable-Markt wird nach IDC von 76,1 Mio. Geräten in 2015 auf 173 Mio. in 2019 anwachsen.

Zum Vergleich der IoT-Dimension: aktuell sind etwa eine Milliarde Menschen vernetzt – und glaubt man Accenture, so verstehen etwa 87% der Mainstream Consumer nicht, was der IoT Markt eigentlich ist.

Statista hat in diesem Jahr Schätzungen veröffentlicht, die sich im Gesamtvolumen etwa mit Gartner decken – das Marktforschungs-Institut geht von 20 Mrd. vernetzten Objekten in 2020 aus (beginnend mit 3,8 Mrd. vernetzten Objekten in 2014). Hierbei ist das Zahlen-Wachstum vernetzter Objekte im Consumer-Bereich mit zwei Dritteln Anteil bei weitem am größten, der kommerzielle, industrie-übergreifende und vertikale Industrie-Markt nimmt den zweiten Platz ein, das vertikale Marktsegment belegt nur ein gutes Zehntel. Die entsprechende Umsatzbetrachtung kommt jedoch zu ganz anderen Ergebnissen: Hier hat der kommerzielle Markt fast die Hälfte des Umsatzanteils, und hiervon wiederum der vertikale Markt einen Löwenanteil von mehr als 60 Prozent. Die Statista-Marktübersichten sind in den Abbildungen 1.3 und Abbildungen 1.4 dargestellt (Quelle: Statista 2016).

Nach einer Untersuchung von CB Insights (November 2015) sind einerseits unter den aktivsten Investoren für IoT-Technologien recht bekannte Namen wie Intel Capital, Qualcomm Ventures, Foundry Group, Cisco Investments und Squoia Capital, andererseits fehlen einige sehr bekannte Namen wie HP und IBM oder NEC.

2. Einige Einsatz-Szenarien mit Internet of Things

Gebäudetechnik

In diesem Bereich gibt es bereits EU-Initiativen zum Smart Metering: 2020 sollen 80 Prozent aller Häuser mit intelligenten Zählern ausgestattet sein (HAN, WAN), 2022 sollen dann die 100 Prozent erreicht werden. In Großbritannien gibt es eine App mit dem Namen HiVE zur Heizungssteuerung: Hierbei werden Boiler und Thermostate über Wi-Fi mit einem Router verbunden und liefern Informationen an den Energieversorger. (siehe Abbildung 2.1)

Mit Google Nest erkennt ein Thermostat, wann er die Wohnung heizen muss:

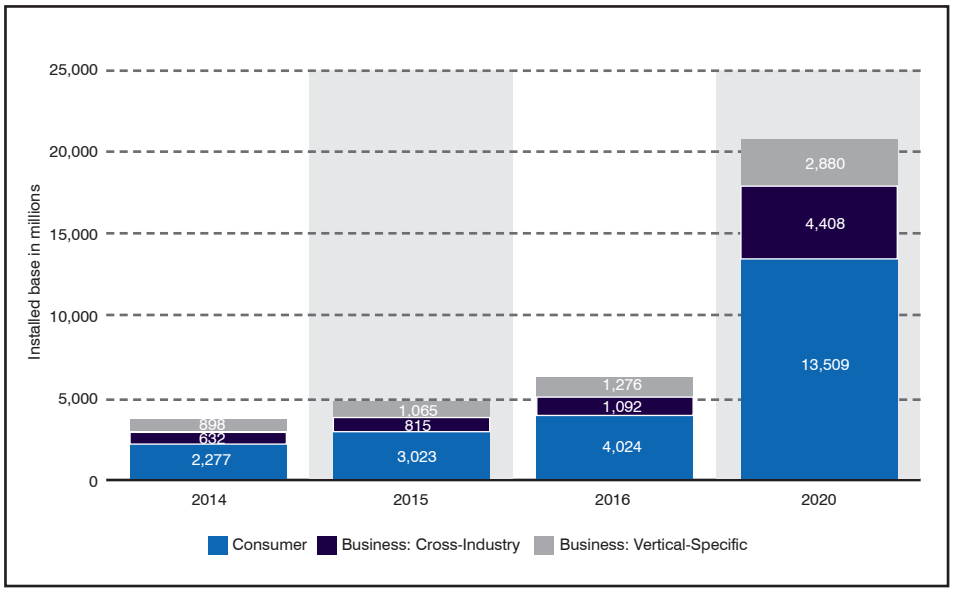

Abbildung 1.3: Anzahl vernetzter IoT Objekte

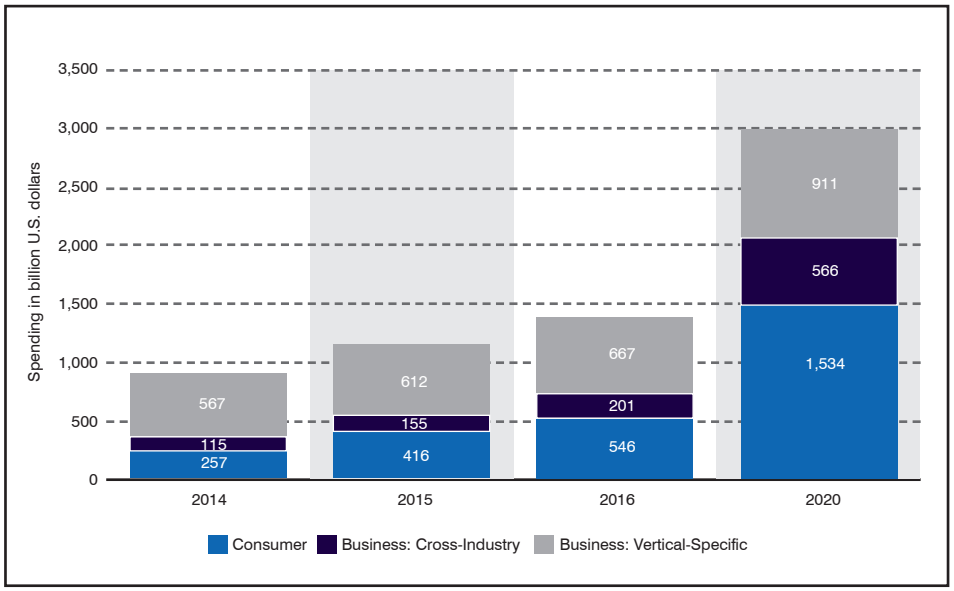

Abbildung 1.4: Umsätze mit IoT

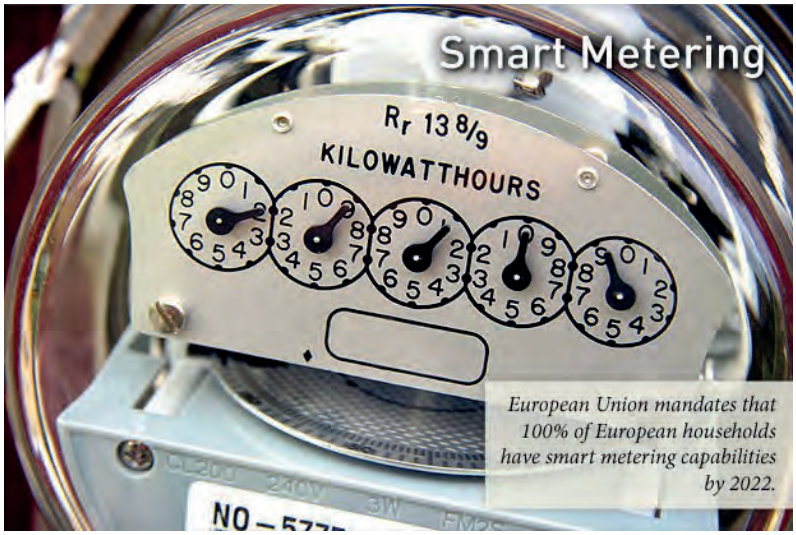

Abbildung 2.1: Smart Metering à la EU

Abbildung 2.2: M2M in der Fertigung

Eub Geofencing-Werkzeug erfasst die Position des Nutzers außer Haus und ermittelt die Wegstrecke sowie die Fahrzeit, die er noch bis nach Hause benötigen wird. Diese Anwendung hat Google jetzt um eine Sprachsteuerung erweitert (Google-Now-App für iOS und Android). Unter dem Logo "Works with Nest" finden sich 3rd Party Erweiterungen, z.B. von Phillips das Hue Beleuchtungssystem; es blinkt, wenn ein Nest-protect Sensor Kohlenmonoxid erkennt.

AV-Systeme mit Überwachungsfunktion für beliebige Haushaltsgeräte könnten Fehlercodes an Hersteller und Versorger melden und Kundendienst-Besuche oder Ersatzteil-Bestellung veranlassen.

Fertigung

Intelligente Fertigungsstraßen, Maschinen und Produkte tauschen miteinander Da-

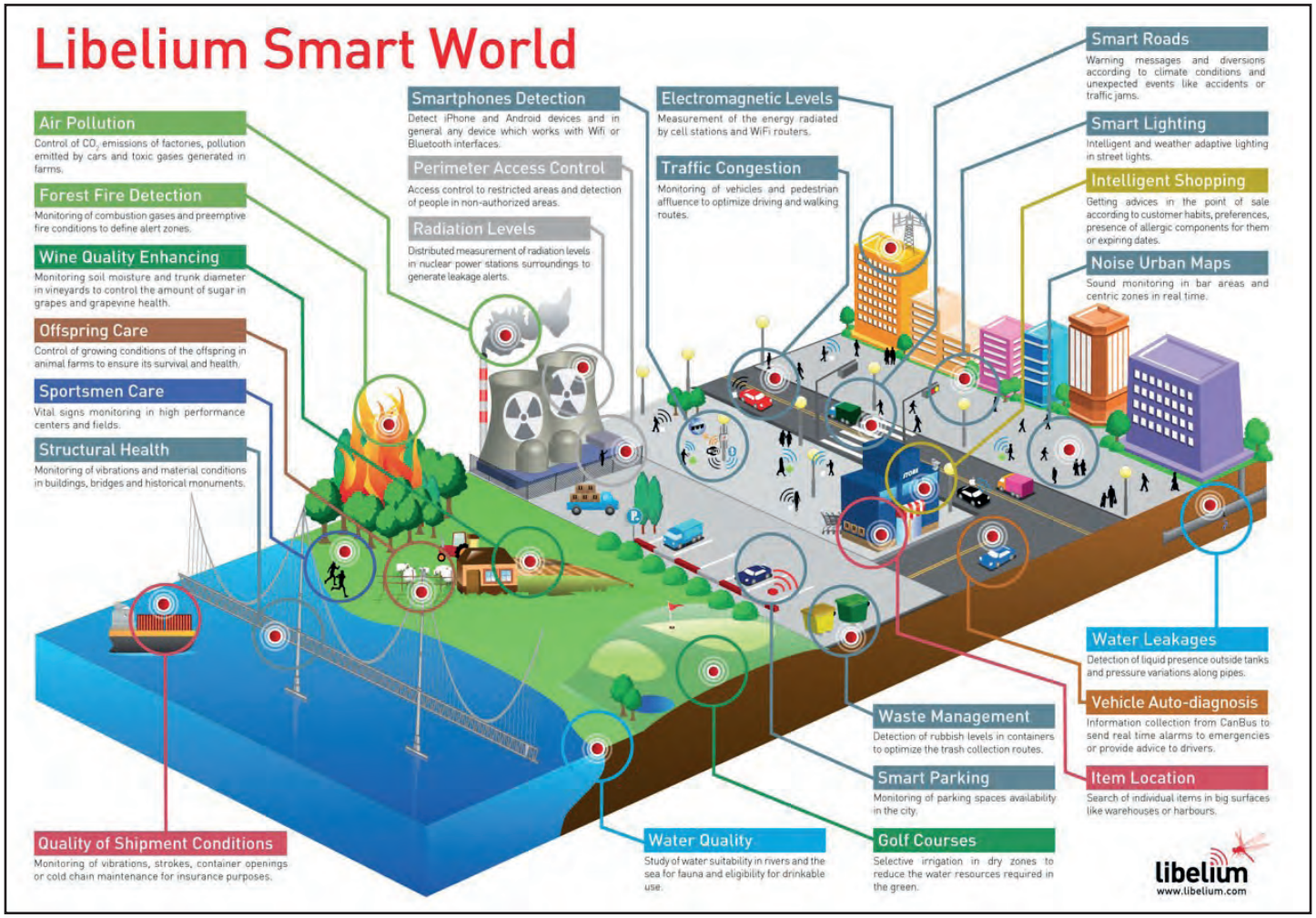

Abbildung 2.3: Internet of Things in der Umwelttechnik

ten aus und steuern den Fertigungsprozess gemeinsam. Smarttags vernetzen dabei die für den Fertigungsprozess notwendigen Bestandteile. Dies führt zu einer effizienteren Anlagenverwaltung, besserer Material-Verfolgung, noch schnelleren Just-in-Time-Prozessen, weniger Fehlern, und last but noch least auch zu weniger Diebstählen. (siehe Abbildung 2.2)

Umwelttechnik und Smart Cities

Vernetzte Sensoren werden Umweltveränderungen erkennen und weitermelden. So können frühzeitige Warnungen vor Erdbeben, Lawinen, Vulkanausbrüchen, Tsunamis erfolgen und bei Bedarf frühzeitig Evakuierungen eingeleitet werden.

Am Flughafen von San Francisco werden beispielsweise Umgebungs-Informationen für Behinderte bereitgestellt: Hier gibt es 500 Signalsender, die mit iOS kommunizieren. Ein iOS Gerät meldet dann eigeninitiativ wichtige Infos wie z.B. nächstgelegene Abflug-Gates, Geldautomaten, Info-Schalter, Steckdosen.

In sehr vielen Bereichen werden Sensor-Netze eine Informationsbasis für Überwachung, Alarme und Steuerung bieten. Dies gilt insbesondere auch im Smart City-Umfeld für Umwelt, Energie, Sport und Verkehr. Hier werden Sensoren die CO^2-, Staub- und toxische Emissionen von Industriebetrieben überwachen. Elektromagnetische Abstrahlungen von Antennen und WiFi Routern werden gemessen und überwacht, gleiches gilt für radioaktive Abstrahlungen von Kernkraftwerken. Schall- und Lärmbelastung kann gemessen und überwacht werden. Wasserrohr-Brüche und überlastete Kanäle führen zu Alarmen. Waldbrände werden frühestmöglich gemeldet. (siehe auch Abbildung 2.3)

Die Verkehrs-Steuerung in überlasteten Städten wird (hoffentlich) wesentlich effizienter. Die Ampelschaltungen werden mit den heranfahrenden und wartenden Autos kommunizieren, Anhalten und Anfahren werden von der Ampelschaltung aus getriggert. Es kann dynamische Staumeldeanzeigen für alle größeren Straßen in allen Fahrzeugen geben. Es kann straßen- und ortsteilbezogene Warnmeldungen bei schlechten Wetter- und Straßenbedingungen geben (zum Beispiel bei Unfallstaus, Starkregen, Glatteis, Überschwemmungen). Freie Parkplätze werden im Auto auf einer Stadtkarte angezeigt.

Gartner prognostiziert, dass 2020 weltweit etwa jedes fünfte Fahrzeug auf der Straße irgendeine Funkverbindung haben wird. Das bedeutet mehr als 250 Millionen vernetzte Fahrzeuge. Diese Vernetzung der

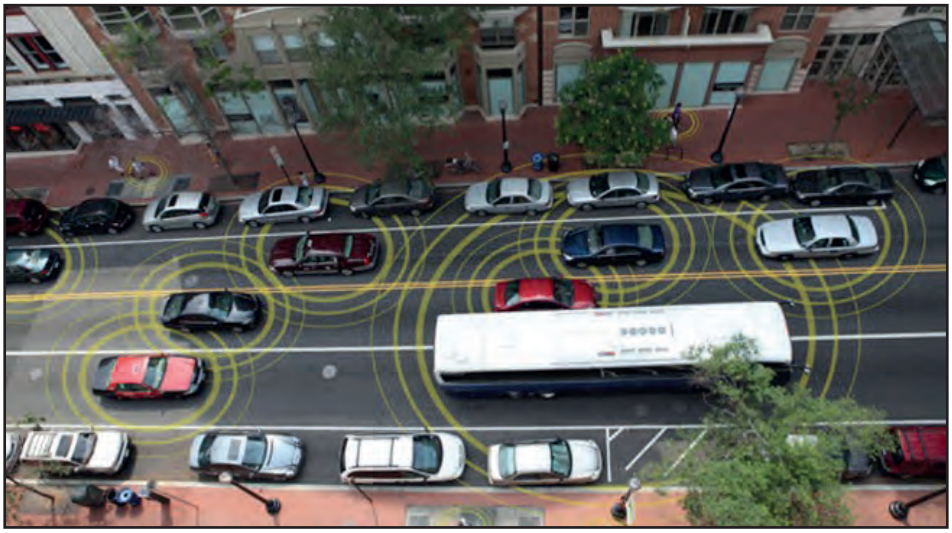

Abbildung 2.4: Verkehrskontrolle durch Fahrzeug-Vernetzung

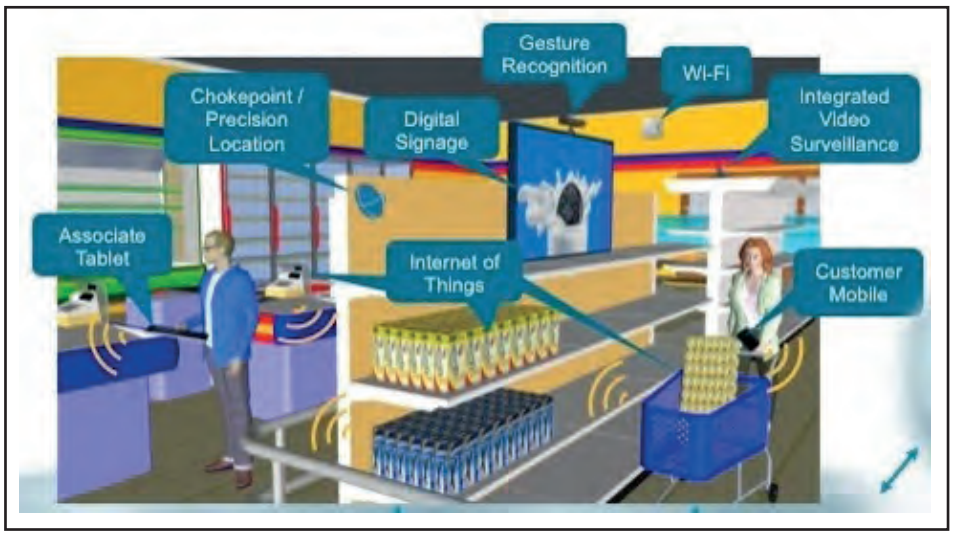

Abbildung 2.5: Internet of Things im Supermarkt

Abbildung 2.6: Wearable-Technologie und Internet of Things zur Gesundheitsüberwachung

Internet of Things – die vierte industrielle Revolution

Fahrzeuge wird als wesentliche Funktionsbereiche Telematik, automatisiertes Fahren, Infotainment und Mobilitäts-Dienste stark beeinflussen. (siehe auch Abbildung 2.4)

Für die Städte werden sich sensorgesteuerte LED-Beleuchtungen etablieren. Jede Straßenlampe wird mit Helligkeits-Sensoren bestückt sein. Die Straßenbeleuchtung schaltet sich dann nicht mehr tageszeitabhängig sondern helligkeits-abhängig ein und wird entsprechend bei etwa vorhandenem Rest-Tageslicht nicht die volle Leuchtkraft aktivieren. Öffentliche Abfalleimer können mit Füllstandsanzeigen ausgestattet werden – wenn sie voll sind, werden sie bedarfsgerecht von einem Roboter geleert.

Im Supermarkt erfasst eine Kamera am Eingang die Kunden per Gesichtserkennung (dagegen können Sie sich im Wesentlichen nur wehren, wenn Sie in einem anderen Supermarkt einkaufen gehen – es wird leider aber keinen Supermarkt mehr ohne Kamera geben… Dagegen können Sie sich dann nur noch wehren, wenn Sie Ihren Salat im eigenen Garten anbauen – natürlich mit Smart Farming). Kameras an den Regalen werden aufnehmen, ob Sie auf die vorgefundenen Produkte erfreut, verärgert oder konsumkritisch reagieren. Alle Waren sind mit RFID Tags versehen. Steht der Ablauf des Mindesthaltbarkeitsdatums bevor, wird der Preis eines Produktes automatisch reduziert. Die Waren, die Sie in Ihren Einkaufswagen geladen haben, werden automatisch erfasst, Sie müssen sie nicht mehr auf ein Band an der Kasse legen. Ihr Kaufverhalten wird ebenfalls erfasst und Ihrem Gesicht zugeordnet. Sofern Sie üblicherweise alle vier Wochen Toilettenpapier kaufen und dies einmal vergessen, könnte die freundliche Dame an der Kasse Sie gezielt daran erinnern. Sie bezahlen nicht mehr mit Bargeld sondern mit Ihrem Mobilgerät oder einer Karte. Ein Smart Market Szenario zeigt Abbildung 2.5.

Gesundheitswesen

Im Gesundheitswesen wird es eine Fülle neuer kleinformatiger und großformatiger Überwachungsgeräte geben. Das ganze "Wearable" Portfolio schlägt hier zu: Blutdruck-Sensoren, Puls-Sensoren, Blutzucker-Sensoren, Schweiß-Sensoren, Schrittzähler und vieles mehr wird in Brustgurten, Manschetten, Klemmen, Kabeln und anderen Kleinteilen eingebaut sein und als BAN (Body Area Network) mit Gesundheitsdiensten, Notdiensten und Patientendatenbanken kommunizieren. (siehe Abbildung 2.6)

Jedes Krankenzimmer ist mit einer Videokamera ausgestattet, die die Krankenbetten im Fokus hat. Im Schwesternzimmer der Krankenstation sind alle Krankenzimmer auf einer großen Wandanzeige zu sehen. Werden dann zum Beispiel nachts mehrere Patientenrufe gleichzeitig ausgelöst, kann die Schwester anhand der Bildanzeige entscheiden, welchem Patienten sie aktuell am dringendsten helfen muss.

In Teil 2 lesen Sie:

- Architektur-Ansätze für Internet of Things
- Die Protokollwelten für Internet of Things

Abkürzungen, Links, Literatur

BAN	Body Area Network
EVU	Energie-Versorgungs-Unternehmen
EU	Europäische Union
HAN	Home Area Network
IDC	International Data Corporation
IoE	Internet of Everything
IoT	Internet of Things
IT	Informations-Technologie
LED	Light Emitting Diode
M2M	Machine to Machine
MESZ	Mittel-Europäische Sommer-Zeit
RFID	Radio Frequency Identitfication
RZ	Rechenzentrum
VR	Virtual Reality
WiFi	Wireless Fidelity

Kongress

ComConsult UC-Forum 2016
21.11. - 23.11.16 in Düsseldorf

Das diesjährige UC-Forum analysiert die herausragenden Trends für UC und VoIP und gibt Empfehlungen für Projekte, Technologie-Auswahl und Investitionen. Das dominante Thema ist weiter hin All-IP, sprich die Abschaltung der ISDN- und PSTN-Infrastruktur. Diese geht einher mit einer Welle neuer Dienste und einer Neugestaltung des Mobilfunks. Gleichzeitig rücken Technologien wie Session Border Controller SBC und auch SIP in den Mittelpunkt. Sie entscheiden mehr oder weniger über die Zukunftsfähigkeit moderner UC-Lösungen.

Dabei darf nicht übersehen werden, dass der Markt weiterhin im Wandel ist. Die Übernahme von Polycom durch Mitel ist dabei nur die Spitze des Eisbergs und ein Vorzeichen weiterer wesentlicher Änderungen. Ohne Zweifel wird die zunehmende Bedeutung von Cloud-basierten UC-Leistungen zu weiteren Verwerfungen führen.

Als Sonderthemen haben wir für das diesjährige Forum adressiert:
- IT-Compliance
- SDN in UC Projekten mit Microsoft Skype for Business
- Qualitätssicherung durch VoIP Monitoring

Moderation: Dipl.-Inform. Petra Borowka-Gatzweiler, Markus Geller, Dipl.-Ing. Dominik Zöller
Preis: € 2.190,- netto* - gültig bis zum 15.09.16 - dann regulär € 2.390,- netto

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

ComConsult Veranstaltungskalender

Lokale Netze für Einsteiger, 19.09.-23.09.16 in Aachen

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

Preis: € 2.490,-- netto

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

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

Preis: € 1.590,-- netto

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

Garantietermin

Diese Sonderveranstaltung analysiert, wie der Wechsel von PSTN auf All-IP im Unternehmen verläuft. Sie zeigt auf, welche Funktionalität heute erreicht werden kann und mit welchem Aufwand für Anpassung und Fehlersuche zu rechnen ist.

Preis: € 1.090,-- netto

Die neue EU-Datenschutzgrundverordnung, 21.09.16 in Frankfurt

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

Preis: € 1.090,-- netto

Datenschutzrecht Update für Nichtjuristen, 27.09.16 in Düsseldorf

Die Veranstaltung beinhaltet einen vertiefenden Einblick in das deutsche und europäische Datenschutzrecht. Teilnehmern soll das Rüstzeug vermittelt werden, um in den grundlegenden datenschutzrechtlichen Fragestellungen eine belastbare rechtliche Ersteinschätzung vornehmen zu können. Zudem werden die Teilnehmer über neueste Entwicklungen auf nationaler und europäischer Ebene informiert.

Preis: € 1.090,-- netto

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

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

Preis: € 2.290,-- netto

Crashkurs IT-Recht für Nichtjuristen, 05.10.16 in Düsseldorf

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

Preis: € 1.090,-- netto

Der Client der Zukunft, 05.10.-06.10.16 in Bonn

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

Preis: € 1.590,-- netto

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

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

Preis: € 1.890,-- netto

Zertifizierungen

ComConsult Certified Network Engineer

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

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

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

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

ComConsult Certified Trouble Shooter

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

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

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

ComConsult Certified Voice Engineer

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

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

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

Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter
19.09. - 20.09.16 in Frankfurt
20.02. - 21.02.17 in Bonn
02.05. - 03.05.17 in Düsseldorf

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

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

Impressum

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

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

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

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

Für unverlangte eingesandte Manuskripte
wird keine Haftung übernommen
Nachdruck, auch auszugsweise
nur mit Genehmigung des Verlages
© ComConsult Research