Februar 2025

ComConsult GmbH
Beratung + Planung + Schulung

Der Netzwerk Insider

Datentreuhänder und die EU-Datenstrategie

von Dr. Kathrin Stollenwerk
Daten sind ein wertvolles Gut, das ist kein Geheimnis mehr. Und wie so häufig gilt auch hier: Die einen haben sie, die anderen wollen sie. Einer Datenweitergabe oder einem Teilen von Daten stehen oft Unklarheiten und Ängste bei den Dateninhabern im Weg. Sobald personenbezogene Daten im Spiel sind, droht die DS-GVO.

Seite 7

Das disruptive Potenzial von Azure Local

von Dr. Behrooz Moayeri
Azure Local hat als RZ-Architektur nach dem Modell der Microsoft-Cloud ein disruptives Potenzial. Mit disruptivem Potenzial meine ich, dass Azure Local eine Reihe von Rechenzentren verändern kann. Ich bin immer skeptisch, wenn ein Hersteller eine proprietäre Architektur entwirft und damit Kunden an sich bindet. Der Markt entwickelt sich jedoch ohne Rücksicht auf meine Skepsis.

Seite 2

Vom Produkt zur Plattform: Wie traditionelle Unternehmen die digitale Transformation meistern können

von Darav Taha
Als Gründer mehrerer digitaler Plattformen sowie als Berater und Trainer für KMUs und große Konzerne zum Thema Marktplätze stoße ich immer wieder auf Verständnisprobleme, wenn es um die Plattformökonomie geht.

Seite 13

Webinar der Woche

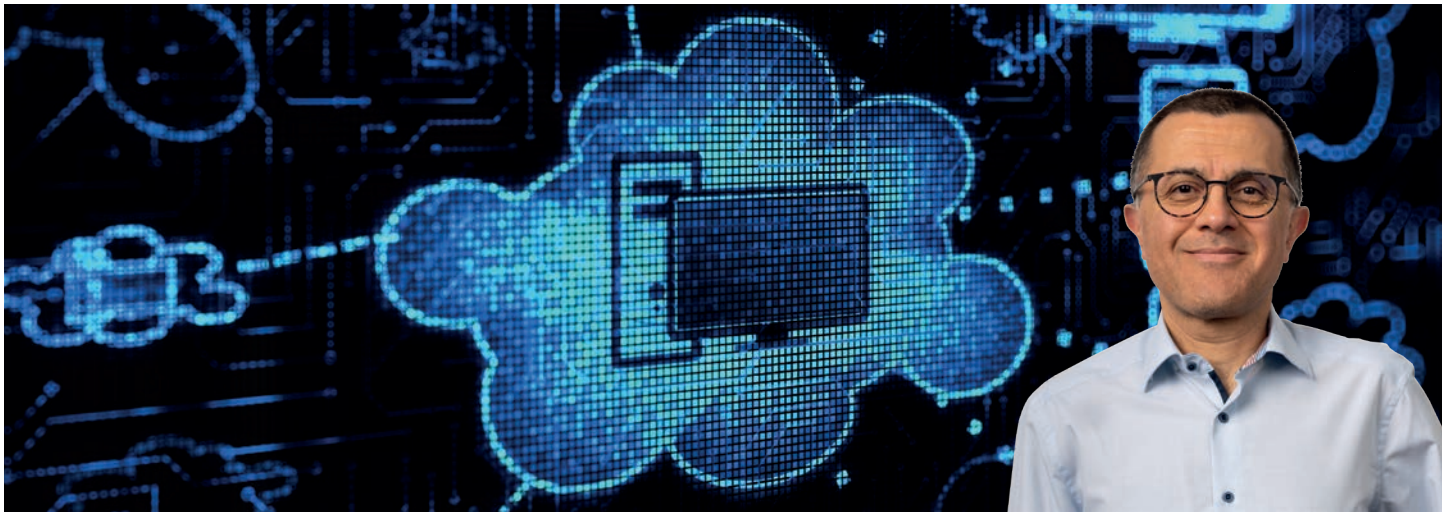
Microsoft Project – mit Plan zur richtigen Lizenz

Seite 24

Was ist das typische WLAN-Problem?

von Dr. Joachim Wetzlar
Jeder von Ihnen hat diesbezüglich seine eigene Erfahrung, vermute ich. Mir fällt auf, dass es in den letzten Jahren oft Anfragen zu Problemen mit Web-Konferenzen gab: Zoom, Teams, WebEx, GoTo Meeting und wie sie alle heißen sind inzwischen aus dem Arbeitsleben nicht mehr wegzudenken. Das ist Fluch und Segen zugleich.

Seite 25



Das disruptive Potenzial von Azure Local

von Dr. Behrooz Moayeri

Azure Local hat als RZ-Architektur nach dem Modell der Microsoft-Cloud ein disruptives Potenzial. Mit disruptivem Potenzial meine ich, dass Azure Local eine Reihe von Rechenzentren verändern kann. Ich bin immer skeptisch, wenn ein Hersteller eine proprietäre Architektur entwirft und damit Kunden an sich bindet. Der Markt entwickelt sich jedoch ohne Rücksicht auf meine Skepsis.

Die wichtigste Herausforderung für RZ-Betreiber

In den letzten Monaten und Jahren habe ich mehr als einmal und auch an dieser Stelle auf ein Problem hingewiesen, das sich nun nach meiner Wahrnehmung zur wichtigsten Herausforderung für RZ-Betreiber entwickelt hat. Ich meine den Fachkräftemangel. Während durch den anhaltenden Digitalisierungstrend einerseits und die immer höheren Anforderungen der Cyber Security andererseits der Aufwand für den Betrieb von Rechenzentren weiter steigt, sorgt der unaufhaltsame demografische Wandel für die Ausdünnung des Personals, das für die Aufrechterhaltung von Rechenzentren samt ihrer Compute-, Storage-, Netz- und Sicherheitskomponenten erforderlich ist.

Es gibt keine Aussicht, dass sich die von den Weather Girls mit „It's Raining Men" besungenen, vom Himmel fallenden Männer bewahrheiten, nicht für IT-Männer und noch weniger für IT-Frauen. Auch hat sich die Hoffnung, Cloud Computing löse das Problem, in den letzten zehn Jahren als trügerisch erwiesen. Genauso aussichtslos oder unzureichend ist das Setzen auf Migrationsströme und die Umschulung von Personal, das die im Niedergang befindlichen Wirtschaftszweige freisetzen.

Deshalb gilt: Die Unternehmen müssen in den kommenden Jahren mit weniger Personal ihre Rechenzentren betreiben, die in den meisten Fällen weder an Komplexität noch an Größe abnehmen.

Weniger ist mehr

Der sich verschärfende Fachkräftemangel im IT-Bereich ist längst bekannt. Deshalb gibt es auch seit Jahren das Versprechen vieler Hersteller, durch Automatisierung den Aufwand für den RZ-Betrieb zu reduzieren. Ein in diesem Zusammenhang immer wieder benutzter Begriff ist Software-Defined Data Center (SDDC). Die Idee dahinter besteht darin, dass die Einrichtung und der Betrieb aller RZ-Ressourcen (Compute, Storage, Netz, Security) mittels einer übergreifenden Software erfolgen.

Erste Schritte in diese Richtung wurden bereits mit der Server-Virtualisierung unternommen. Auch die Virtualisierung von Speicher und Netz wurde von Herstellern ermöglicht. In den meisten Fällen blieben jedoch die sogenannten Silos im RZ-Betrieb bestehen. Die Inbetriebnahme einer Applikation erfordert in der Regel einen Workflow durch die arbeitsteilig zuständigen Silos für Server, Storage, Netz und Security. Virtuelle Maschinen müssen konfiguriert, virtueller Storage muss angelegt, virtuelle Netze gebildet und Firewall-Regeln definiert werden.

Dieser Zustand ist für viele „Kunden" der Rechenzentren unbefriedigend, da er einerseits mit längeren Wartezeiten auf die Realisierung von Anforderungen einhergeht und andererseits im Kontrast zu den mittlerweile allgemein bekannten Abläufen bei der Nutzung von Public Clouds steht. Die Betreiber der Public Clouds befähigen ihre Kunden zur Selbstbedienung. In wenigen Schritten können Cloud-basierende Ressourcen für Compute, Storage und Netz in Betrieb genommen werden, ohne dass man auf fremde Hilfe warten muss. Auch Mikrosegmentierung als wichtiges Sicherheitswerkzeug ist in den Clouds die Regel und nicht die Ausnahme.

Datentreuhänder und die EU-Datenstrategie

von Dr. Kathrin Stollenwerk

Daten sind ein wertvolles Gut, das ist kein Geheimnis mehr. Und wie so häufig gilt auch hier: Die einen haben sie, die anderen wollen sie. Einer Datenweitergabe oder einem Teilen von Daten stehen oft Unklarheiten und Ängste bei den Dateninhabern im Weg. Sobald personenbezogene Daten im Spiel sind, droht die DSGVO. Doch wer darf über Daten verfügen, die keinen Personenbezug besitzen, vielleicht sogar von einer Maschine generiert wurden? Hier möchte die EU mit ihrer Datenstrategie für mehr Klarheit sorgen und so das Datenteilen fördern.

Daten als neuer Rohstoff

Daten sind in heutigen Arbeits- und Geschäftsprozessen ein nicht mehr wegzudenkender Faktor. Sie werden, egal ob personenbezogen oder nicht personenbezogen, überall erzeugt. Mal geschieht dies bewusst, wie bei der Benutzung einer Bonuspunktekarte an der Supermarktkasse, mal eher unbemerkt, beispielsweise durch IoT-Geräte, bei denen dem Nutzenden oftmals gar nicht bekannt ist, welche Flut an Daten durch das Gerät erhoben wird. Hinzu kommen IoT-Geräte in der Produktion, in Land- und Forstwirtschaft und etlichen anderen Bereichen. Was Daten erheben kann, tut dies in der Regel auch.

Bereits 2006 bezeichnete der britische Mathematiker Clive Humby Daten als „das neue Öl“ [1]. Dieses Gleichnis ist in den folgenden zwei Punkten zutreffend: Ähnlich wie Erdöl ein (noch) unverzichtbarer Rohstoff für viele Industriezweige ist, bilden Daten einen essentiellen Rohstoff für innovative Ideen und Wertschöpfung. Ebenso müssen Daten erst eine Auswertung durchlaufen, um einen Mehrwert zu besitzen – ähnlich wie Rohöl, das erst durch Raffinierung zu höherwertigen Produkten wird.

Ein grundsätzlicher Unterschied zwischen Öl und Daten liegt jedoch in der Frage nach dem Eigentümer. Stoßen Sie bei Bohrarbeiten in Ihrem eigenen Garten auf Öl, gehört es leider nicht Ihnen. Für Öl als bergfreier Bodenschatz ist der Besitz im Bundesbergbaugesetz (BbergG) geregelt. Für Daten, die im übertragenen Sinne während des Bohrens von Ihren Bohrgeräten erhoben werden, gibt es hingegen keine gesetzliche Regelung. Denn ein Eigentum an Daten kennt das Bürgerliche Gesetzbuch (BGB) nicht. Dies gilt auch für personenbezogene Daten. Trotzdem sind Daten kein absolutes ‚Freiwild‘, sondern sie bzw. die in ihnen enthaltenen Informationen werden durch verschiedene Gesetze und Verordnungen auf nationaler und europäischer Ebene geschützt. Dies können je nach Ausprägung der Daten beispielsweise die Datenschutzgrundverordnung (DGSVO), das Urheberrecht (UrhG) oder auch das Geschäftsgeheimnisgesetz (GeschGehG) sein.

Maschinengenerierte Daten – wer darf hier was?

Fokussieren wir uns auf maschinengenerierte Daten, helfen die vorgenannten Gesetze nur bedingt weiter. Denn maschinengenerierte Daten haben nicht unbedingt einen Personenbezug und fallen somit nicht in den Geltungsbereich der DSGVO. Ebenso trifft das Urheberrecht nicht auf maschinengenerierte Daten zu, denn „Werke im Sinne dieses Gesetzes sind nur persönliche geistige Schöpfungen“ (§ 2 Abs. 2 UrhG). Dies gilt beispielsweise nicht für Messdaten einer Maschine. Ob solche Messdaten unter das Geschäftsgeheimnisgesetz fallen, ist nicht pauschal zu beantworten. Wer nun also die von einer Maschine erhobenen Daten weiter-

Vom Produkt zur Plattform: Wie traditionelle Unternehmen die digitale Transformation meistern können

von Darav Taha

Der Versuch einer Plattformdefinition

Als Gründer mehrerer digitaler Plattformen sowie als Berater und Trainer für KMUs und große Konzerne zum Thema Marktplätze stoße ich immer wieder auf Verständnisprobleme, wenn es um die Plattformökonomie geht. Viele meiner Kunden können mit dem Begriff wenig anfangen oder verbinden ihn vor allem mit sozialen Medien wie Facebook und Instagram.

Diese eingeschränkte Wahrnehmung erschwert die Diskussion über Plattformmodelle erheblich. Social-Media-Plattformen prägen das allgemeine Verständnis von "Plattformen" vorwiegend aus einer konsumorientierten, medialen Perspektive. Dabei wird häufig übersehen, dass Plattformökonomie weit über die Nutzung von sozialen Netzwerken hinausgeht und vielfältige Geschäftsmodelle ermöglicht – von Marktplätzen über Dienstleistungsplattformen bis hin zu datengetriebenen Ökosystemen.

Folgende Aspekte verdeutlichen den Unterschied zwischen Plattformgeschäftsmodellen und klassischen linearen Geschäftsmodellen:

- **Wertschöpfende Interaktionen:** Plattformen schaffen einen (digitalen) Raum, in dem externe Anbieter und Kunden direkt miteinander interagieren, um Werteinheiten auszutauschen. Diese Interaktionen bilden den Kern der Plattformökonomie.

- **Werteinheiten:** Die ausgetauschten Werte können in verschiedener Form auftreten:
  - Materielle Güter: Wie Bücher, Autos oder Immobilien.
  - Immaterielle Güter: Wie Dienstleistungen, Software oder digitale Inhalte.
  - Soziale Währung: Wie Likes, Kommentare oder Matches auf Plattformen wie Instagram oder Tinder.
  - Vermögenswerte: Wie Aktien, Kryptowährungen oder digitales Buchgeld.

- **Offene Infrastruktur:** Plattformen bieten eine technologiegestützte Infrastruktur, die es Nutzern ermöglicht, schnell und unkompliziert an der Plattform teilzunehmen. Dazu gehören benutzerfreundliche Schnittstellen (Apps, APIs) und skalierbare technische Systeme.

- **Plattform-Governance:** Die Governance einer Plattform legt Regeln und Mechanismen fest, die das Verhalten der Teilnehmer steuern und das Vertrauen innerhalb des Ökosystems sicherstellen. Beispiele hierfür sind Bewertungsmechanismen, Sicherheitsrichtlinien und Zugangsregeln.

Der Cyberrisikocheck: verbesserte Informationssicherheit für Klein- und Kleinstunternehmen

Mit Maren Poppe sprach Christiane Zweipfennig

Cybersicherheit stellt für Unternehmen aller Größen und Branchen eine enorme Herausforderung dar. Gerade bei kleinen Unternehmen, deren Kerngeschäft ohne viele IT-Prozesse auskommt, wird das Thema Informationssicherheit oft vernachlässigt. Um dieser Situation entgegenzuwirken, hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) in Zusammenarbeit mit dem Bundesverband der mittelständischen Wirtschaft (BVMW) und rund 20 weiteren Partnern ein Konsortium gegründet und den Cyberrisikocheck erarbeitet. Veröffentlicht wurde dieser als DIN SPEC 27076 im Mai 2023.

Maren Poppe ist seit vier Jahren im Competence Center IT-Sicherheit bei ComConsult beschäftigt. Während sie anfangs dabei unterstützte, das ComConsult-interne Informationssicherheitsmanagementsystem aufzubauen und die eigene TISAX®-Zertifizierung voranzutreiben, ist heute einer ihrer Arbeitsschwerpunkte das Schreiben von Richtlinien im Rahmen des Aufbaus und Betriebs des Informationssicherheitsmanagements in Kundenprojekten.

Der Cyberrisikocheck dient dazu, Klein- und Kleinstunternehmen bei den ersten Schritten zur Verbesserung ihrer Informationssicherheit zu unterstützen. Warum wurde er entwickelt?

Das BSI hat die Frage analysiert, auf welchem Niveau sich die Informationssicherheit in kleinen Unternehmen unter fünfzig Mitarbeitern und Kleinstunternehmen unter zehn Mitarbeitern befindet. Statistische Erhebungen ergaben, dass das Niveau höher lag als angenommen. Das BSI hat sich daraufhin die Ergebnisse näher angeschaut. Zum Beispiel wurde die Frage „Ist Ihre E-Mail-Kommunikation verschlüsselt?“ zu einem hohen Prozentsatz positiv beantwortet. Auf die Nachfrage, wie genau man denn die E-Mails verschlüsseln würde, wurde auf das kleine Schloss in der Adressleiste im Browser hingewiesen. Offensichtlich war den Befragten nicht bekannt, dass das Schloss auf die Kommunikation mit der Webseite über ein sicheres Protokoll https hinweist. Die hier beschriebene Wissenslücke zeigt, dass eine Befragung der Unternehmen nur dann sinnvoll ist, wenn die Fragen den Unternehmen erklärt werden. Das BSI hat erkannt, dass zur Vermeidung von Missverständnissen und zur Verhinderung von falschen statistischen Ergebnissen Mitarbeiter von IT-Dienstleistern in die Unternehmen gehen und sich mit ihnen über die Fragen zu ihrer Informationssicherheit unterhalten müssen.

> IT-Dienstleister sollen Klein- und Kleinstunternehmen Fragen zu Informationssicherheit erklären.

Was ist das typische WLAN-Problem?

von Dr. Joachim Wetzlar

Jeder von Ihnen hat diesbezüglich seine eigene Erfahrung, vermute ich. Mir fällt auf, dass es in den letzten Jahren oft Anfragen zu Problemen mit Web-Konferenzen gab: Zoom, Teams, WebEx, GoTo Meeting und wie sie alle heißen sind inzwischen aus dem Arbeitsleben nicht mehr wegzudenken. Das ist Fluch und Segen zugleich. Die Online-Arbeit lässt uns und unsere Kunden viel effizienter miteinander arbeiten. Dienstreisen sind kaum noch nötig, was ich persönlich bedauere. Aber das ist eine andere Geschichte.

Web-Konferenzen sind also allgegenwärtig. WLAN auch. Viele unserer Kunden verzichten inzwischen völlig auf Ethernet und verlassen sich ganz auf das WLAN. Das ist einerseits eine gute Idee, denn der Wechsel eines Endgeräts vom Ethernet zum WLAN, etwa wenn man es ein- oder ausdockt, hat unerwartete Effekte zur Folge [1]. Andererseits beschweren sich Mitarbeiterinnen und Mitarbeiter seither über Aussetzer bei der Sprache oder eingefrorene Videobilder. „Beliebt“ ist auch die einseitige Sprachverbindung: Ich höre meinen Partner, er mich aber nicht, oder umgekehrt.

Wie kommt es, dass solche Probleme offensichtlich nur die Web-Konferenzen betreffen? Ich behaupte, dass andere Anwendungen wahrscheinlich auch betroffen sind, man es nur nicht merkt. File-Sharing oder Web-Zugriffe sind nicht anfällig gegen kurze Unterbrechungen oder Paketverluste, dem Transmission Control Protocol (TCP) sei Dank. Ich behaupte sogar, eine Anwendung ist erst dann WLAN-tauglich, wenn sie Unterbrechungen von bis zu 10 Sekunden verkraften kann.

Das funktioniert bei Voice und Video leider nicht. Alle Pakete müssen rechtzeitig ankommen, man sagt auch „in Echtzeit“. Zuhörer reagieren empfindlich auf kürzeste Unterbrechungen, und Artefakte in Videos werden als störend empfunden. Wie aber findet man die Ursache für Paketverluste im WLAN?

Nehmen wir der Einfachheit halber an, die Pakete gingen auf der Luftschnittstelle verloren, d.h. auf dem Weg vom Access Point zum Client oder zurück. Als Erstes schaue ich dann auf die Statistiken in den Access Points bzw. im WLAN-Controller.

„Retries“ weisen darauf hin, dass Pakete auf dem Weg zum Empfänger verloren gingen und demzufolge wiederholt werden mussten. Sie sind ein Hinweis auf Kollisionen oder auch Funkstörungen. Die Kanalauslastung sagt, zu welchem Anteil das Medium von irgendeiner Station belegt ist. Hohe Kanalauslastung bei gleichzeitig geringer Sende- und Empfangsrate entsteht z. B. durch starke Überlappung von Funkzellen.

In der Regel liegen diese Werte jedoch im grünen Bereich. Auch die gute WLAN-Ausleuchtung werden Sie schon des Öfteren verifiziert haben. Und die Probleme sind immer noch da. Jetzt hilft vielleicht eine Paketaufzeichnung weiter. Sie haben die Wahl: Entweder zeichnen Sie im Ethernet, auf der Luftschnittstelle oder auf beiden Wegen auf.

Pakete können Sie zwischen Access Points und Ihrer Infrastruktur abgreifen; oft ist das ein WLAN-Controller. In diesem Fall sind die eigentlichen WLAN-Pakete in irgendein Tunnel-Protokoll eingebettet. Die WLAN-Pakete findet man im Tunnel so wie sie auch im Funk zu sehen wären mit einer Ausnahme: Sie werden nicht verschlüsselt sein. Quittungspakete (ACK) wird man nicht finden. Auch viele Management-Pakete sind im Ethernet nicht zu sehen.