

Aspekte und Hinweise zur Einführung von Office 365 und Microsoft Teams

von Cornelius Höchel-Winter

Microsoft mischt mit Azure und Office 365 den Markt für Cloud-Anwendungen derzeit kräftig auf. Microsoft nutzt dabei seine marktbeherrschende Stellung bei den Büroanwendungen und ist auf dem besten Weg diese Position auch bei Cloud-Office-Anwendungen zu behaupten, wenn nicht sogar auszubauen. Denn mit Teams als Nachfolger von Skype for Business wurde sehr erfolgreich eine Komponente integriert, die das Potential hat, die Bereiche Kommunikation und Kollaboration im Unternehmen auf eine komplett neue Ebene zu heben.

Natürlich ist Microsoft Teams nicht das einzige Produkt, das solche neuen, teamorientierten Arbeitsweisen adressiert. Gerade Cisco und Unify haben mit WebEx Teams und Circuit ebenfalls spannen-



de Produkte im Angebot, die jedoch beide auf sehr speziellen Ansätzen beruhen. Bei WebEx Teams steht der Meeting-Bereich klar im Vordergrund, bei Circuit liegt der Schwerpunkt auf der Kommunikation. Microsoft Teams hat daher mit seiner breiten Abdeckung praktisch aller Funktionsfelder aus Kommunikation und Kollaboration derzeit einen deutlichen Vorsprung.

In diesem Artikel werden zunächst die Voraussetzungen und Konsequenzen auf Arbeitsabläufe und Geschäftsprozesse analysiert und einige Aspekte zur Administration von Office 365 mit dem Augenmerk auf Einführung und Migration beleuchtet. Im Anschluss werden Tipps und Erfahrungen bei der Einführung und Konfiguration einer Teams-Umgebung diskutiert.

weiter auf Seite 6

Fog und Edge Computing – Datenverarbeitung im IoT

von Tanja Ulmen

Zwei Begriffe sind seit einigen Jahren in aller Munde: IoT und Cloud. Passen sie zusammen?

Ja und nein.

Das Internet of Things (IoT) erhöht die Anzahl der Endgeräte und das von ihnen generierte Datenvolumen. Man spricht von Big Data. Die Verarbeitung und Speicherung von Big Data kann nur in einer ska-

lierbaren Struktur wie der Cloud erfolgen.

Andererseits ist IoT mit erhöhten Anforderungen an Netzübertragungsleistung, Verfügbarkeit und Echtzeitfähigkeit verbunden. Nicht immer ist die Cloud über eine leistungsfähige Netzverbindung mit kürzester Latenz erreichbar.

Wenn die Endgeräte weit weg von der Cloud sind, muss eben die Cloud zu den

Endgeräten. Wenn sich die Wolke der Erde nähert, wird sie zum Nebel. Dann spricht man von Fog Computing. Und wenn die Endgeräte selbst zur Verarbeitung der Daten beitragen, nennt man das Edge Computing.

Dieser Beitrag befasst sich mit Fog und Edge Computing, Beispielen für ihren Einsatz und den Unterschieden zwischen Fog und Edge Computing. weiter ab Seite 19

Geleit

Wer hat Angst vor Huawei?

auf Seite 2

Standpunkt

**Achtung:
IEEE 802.11ax kommt!**

auf Seite 17

Top Veranstaltungen im Sommer

**Strahlenbelastung
auf Mitarbeiter durch
Funktechniken**

Aktuelles Seminar

**Sommerschule - Neueste
Trends der IT-Infrastruktur**

ab Seite 4

**Sonderveranstaltung:
Künstliche Intelligenz –
Möglichkeiten und Grenzen**

auf Seite 14

Geleit

Wer hat Angst vor Huawei?

Die jüngste indirekte Stellungnahme der Bundesregierung zum Fall Huawei kam von der Bundeskanzlerin bei der Eröffnung der Industriemesse in Hannover:

„Ich bin dagegen, dass wir einfach per Definition jemanden ausschließen. Wichtig sind die Standards, die eingehalten werden müssen.“

Der Präsident des Zentralverbands der Elektrotechnik- und Elektro-Industrie (ZVEI), Michael Ziesemer, äußerte sich ähnlich: „Was wir nicht brauchen, ist die Abriegelung bestimmter Sektoren unter Sicherheitserwägungen.“

Worum geht es?

Das Portfolio des chinesischen Herstellers Huawei umfasst neben Consumer-Produkten wie PCs und Smartphones viele Komponenten für Unternehmen, zum Beispiel Switches, Router, WLAN und Storage. Was aber vor allem in der Öffentlichkeit diskutiert wird, sind die Huawei-Produkte für Carrier. Huawei ist mittlerweile der führende Hersteller für Mobilfunkausrüster.

Die Anteilsmehrheit bei Huawei gehört offiziell der Belegschaft. Einige Regierungen in Ländern, in denen die wichtigsten Mitbewerber von Huawei ihren Hauptsitz haben, werfen dem Hersteller aus China allerlei vor. Dazu gehört der diffuse Vorwurf „Nähe zum chinesischen Staat“. Es wird spekuliert, dass Huawei-Komponenten dem chinesischen Staat die Möglichkeit geben, die Infrastrukturen, in denen diese Komponenten eingesetzt werden, auszuspionieren oder gar zu sabotieren. Belege für diesen Vorwurf gibt es bisher nicht. Der einzige offiziell artikuliert Verdacht gegen die in Kanada auf Amtshilfegesuch der US-Behörden festgehaltene Huawei-Finanzchefin, Meng Wanzhou, ist ein mutmaßlicher Verstoß gegen die Iran-Sanktionen.

Laut einem Bericht des Magazins „Der Spiegel“ hat Arne Schönbohm, der Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI), dem Nachrichtenmagazin mitgeteilt, dem BSI lägen keine Belege für den Spionageverdacht gegen Huawei vor. Vielmehr kam Lob vom BSI aus Anlass der Eröffnung des Huawei Security Lab in Bonn. In dieser Einrichtung können Kunden von Huawei u.a. den Quellcode von Huawei-Produkten prüfen. Das muss natürlich auch für jeden Update gelten. Der BSI-Präsident Schönbohm wünscht sich Ähnliches auch von anderen Herstellern. Nichtsdestotrotz überprüft das BSI Huawei-Produkte, die es auf eige-



nem Eingeweihten erlaubt, ein Gerät auch von Ferne abzuschalten. Das Schreckensszenario: In einem globalen Konflikt schaltet China die Netze in anderen Ländern ab.

Laut dem Präsidenten des BSI konnte ein solcher „Kill-Switch“ in den Huawei-Produkten nicht gefunden werden. Wer Software einigermaßen kennt, weiß um den sehr hohen Aufwand für den Nachweis, dass es eine solche Abschaltvorrichtung nicht gibt. Dieser Nachweis ist bislang weder bei Huawei-Produkten noch bei Produkten der Mitbewerber erbracht.

Also begnügt sich das BSI damit, aus dem Munde seines Präsidenten die Entscheidung über die Zulassung oder Nichtzulassung von Huawei beim 5G-Aufbau als politische Entscheidung zu bezeichnen. Im Klartext: Die Sicherheitsexperten sehen bisher keinen Grund, Huawei zu verbannen. Aber die Politik kann aus anderen

ne Initiative in verschiedenen Ländern besorgt hat. Man sucht zum Beispiel nach einem „Kill-Switch“. Darunter versteht man einen versteckten Mechanismus, der ei-

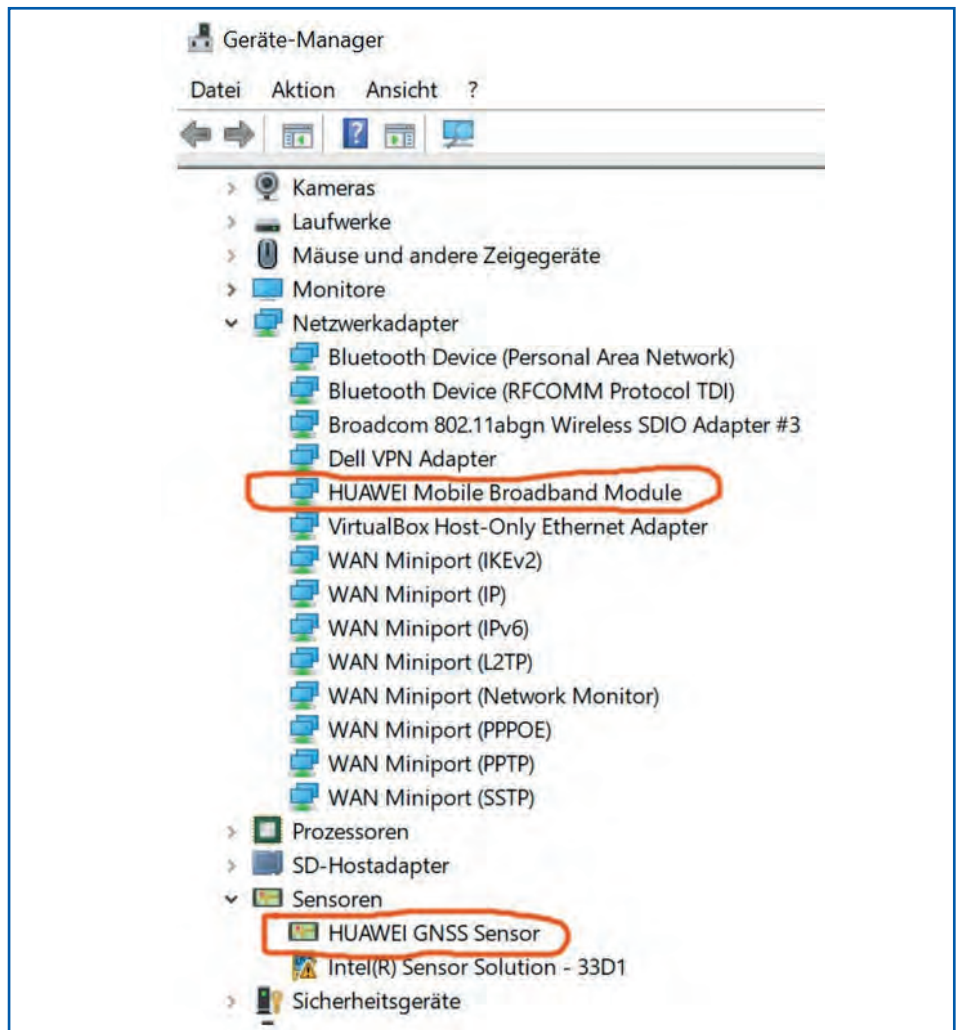


Abbildung 1: Dieser PC ist ein Spion

Aspekte und Hinweise zur Einführung von Office 365 und Microsoft Teams

Aspekte und Hinweise zur Einführung von Office 365 und Microsoft Teams

Fortsetzung von Seite 1



Cornelius Höchel-Winter arbeitet als Senior-Consultant, Autor, Trainer und Referent auf Seminaren und Kongressen seit 2001 für die ComConsult Firmengruppe. Schwerpunkte seiner Tätigkeit sind die Bereiche Data Center, Virtualisierung, Storage, Netzwerke, Cloud Computing und Systemintegration, sowie Evaluierungen neuester Hard- und Softwareprodukte und die Beobachtung aktueller Entwicklungen im IT-Markt. Herr Höchel-Winter besitzt langjährige Erfahrung in der Konzeptionierung, im Aufbau und Betrieb von RZ- und Campusnetzen und von Windows- und Linux-Umgebungen. So hat er als verantwortlicher Projektmanager die Rechenzentren und Netzwerke auf dem Gelände der EXPO2000 in Hannover aufgebaut und während der Weltausstellung betrieben.

So schön wie sich die Office-365-Produkte auch in der Theorie präsentieren, die Einführung von Office 365 ist alles andere als ein Selbstläufer:

- Bei der Verlagerung von Dokumenten in die Cloud sind rechtliche und sicherheitstechnische Aspekte zu beachten und Lösungen zur Klassifizierung, zu DLP (Data Loss Prevention) und Verschlüsselung von Dateien und E-Mails sowie zur Gewährleistung von Aufbewahrungsfristen und Löschpflichten umzusetzen.
- Teams **muss** moderiert, mit technischer und administrativer Unterstützung und flankierenden Mitarbeiterschulungen eingeführt werden. Die Auswirkungen auf die Administration und Verwaltung von Benutzern und Benutzergruppen sind sehr hoch und auch die Anforderungen und notwendigen Veränderungen bei Arbeitsabläufen und Geschäftsprozessen sind zu groß als dass man das einfach so laufen lassen sollte. Detaillierte Vorschläge zur kontrollierten Einführung von Teams werden weiter unten in diesem Artikel diskutiert.
- Selbst vermeintlich wohl bekannte Anwendungen wie Word, Excel oder PowerPoint verhalten sich in der Cloud anders! Auch hier spielen Kollaborationsfunktionen (jetzt auf Dokumentenebene) verstärkt eine Rolle, auch hier gibt es das Potential, dass sich alt hergebrachte Arbeitsabläufe zugunsten einer effektiveren Zusammenarbeit verändern.
- Erfahrungen bei fast allen Projekten und Kundengesprächen haben gezeigt, dass eine Cloud selten allein bleibt. Umgebungen mit mehreren Clouds, die untereinander vernetzt und integriert werden müssen, werden zunehmend zur Regel.

Bereits im Netzwerk Insider vom November 2018 hatten wir grundlegende Fragen und Rahmenbedingungen für den Gang in die Cloud und die Einführung von Cloud-Anwendungen generell diskutiert:

1. Sie benötigen eine Zielbeschreibung/ eine Vision, wo Sie beschreiben, was Sie erreichen wollen.
2. Sie müssen einen geeigneten Cloud-Provider als sogenannten Identity-Provider festlegen, der es Ihnen erlaubt, alle Cloud-Anwendungen und die gesamte Benutzerverwaltung in allen Clouds inklusive Single Sign-On und Multifaktor-Authentifizierung über eine einzige Schnittstelle abzuwickeln.
3. Sie müssen entscheiden, wo welche Daten liegen und wie sie gegebenenfalls geschützt werden sollen. Auch hier ist es sinnvoll, einen einzigen Cloud-Dienst zur Ablage aller Dokumente auszuwählen und es nicht den Vorlieben von Mitarbei-

ten zu überlassen, in welcher Cloud welche Dokumente abgelegt werden.

4. Sie müssen klären, welche Auswirkungen die Einführung der Cloud-Anwendungen auf Ihre Infrastruktur hat. Hier sind natürlich das interne Netzwerk, aber auch WAN-Verbindungen und -Zugänge zu betrachten. Insbesondere Ihr Internet- und Cloud-Zugang muss hinsichtlich Bandbreite, Qualität und Verfügbarkeit kritisch hinterfragt werden.

Sie brauchen eine Vision

Eine weitreichende und tragfähige Vision ist hierbei der wichtigste Aspekt und eine wesentliche Grundlage für die erfolgreiche Umsetzung eines Cloud-Projekts. Sie müssen für Ihr Unternehmen und für Ihre Mitarbeiter beschreiben, was durch den Gang in die Cloud erreicht werden soll und welche Geschäftsprozesse hierdurch optimiert und verbessert werden sollen. (siehe Abbildung 1)

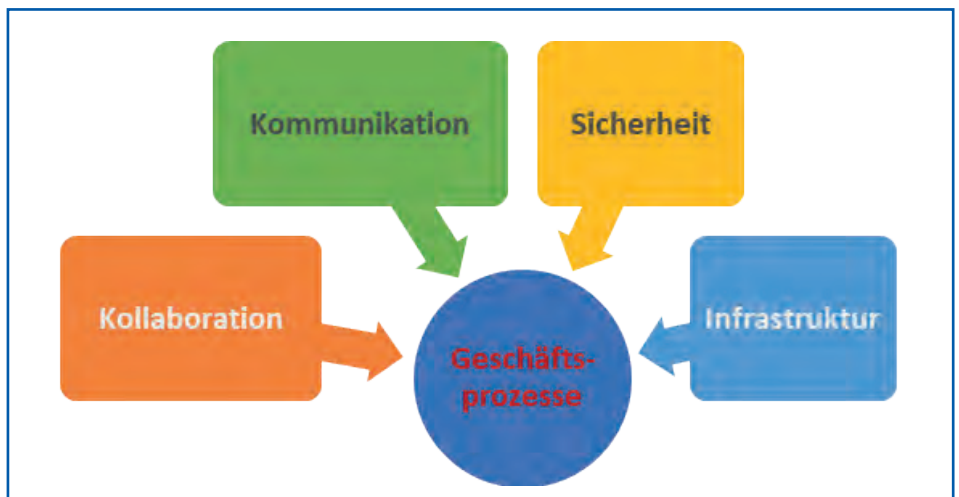


Abbildung 1: Sie brauchen eine Vision

Aspekte und Hinweise zur Einführung von Office 365 und Microsoft Teams

Wenn Sie hierfür keine glaubhaften Argumente finden, werden sie den Übergang in eine moderne Büro- und Arbeitswelt (Stichwort: Digitalisierung 2.0) nicht schaffen!

Bei der Einführung von Office 365 stehen in diesem Zusammenhang die Bereiche Kommunikation und Kollaboration weit im Vordergrund. Fast jedes aktuelle Schlagwort in diesen Bereichen führt Sie früher oder später zu Office 365: Dokumentenkollaboration, mobiles Arbeiten, Integration Externer, Persistent Chat, Huddle Rooms, Integration von künstlicher Intelligenz in Arbeitsabläufe – und immer ist die Basis ein Übergang von benutzerzentrischen, hierarchisch geprägten Arbeitswelten hin zu mehr Teamorientierung. Die Schlagworte aus der Digitalisierung-2.0-Diskussion führen in die gleiche Richtung: kollektive Intelligenz, Selbstorganisation, Selbstregulierung, Sharing Economy etc.

Der Übergang von einer benutzerzentrischen Arbeitsweise zu einer teamzentrischen ist eine der zentralen Grundsatzentscheidungen, die Sie treffen müssen.

Aber aufgepasst: Teams, die nicht mehr in einer Organisationslinie angesiedelt sind, erfordern neue Lösungen und neue Arbeitsweisen für die Mitglieder im Team und neue Führungskonzepte seitens der Führungskräfte im Team. Gerade die modernen Kollaborationstools, die auf teamorientierten, persistent Chats beruhen, stellen die bisherige auf E-Mail basierende Kommunikationsweisen praktisch auf den Kopf – und Microsoft Teams unterscheidet sich hier in nichts vom Wettbewerb (Satya Nadella hat dies auf der Ignite 2017 als „a new culture of work“ bezeichnet).

Drei neue Konzepte kennzeichnen diese neue Arbeitskultur:

1. Im Team sieht jeder alles. Alle haben Zugriff auf dieselben Informationen.
Anmerkung: Ja, das kann bei dem einen oder anderen einen Kulturschock auslösen.
2. Es gibt nicht mehr den einen Ansprechpartner. Aufgaben werden an das Team delegiert und vom Team gelöst.
Anmerkung: Ja, das ist spannend: Es wird Mitarbeiter geben, die sich im Team wegducken, und solche, die sich unerwartet nach vorne stellen.
3. Bereitgestellte Informationen unterliegen im Team einer Holschuld jedes einzelnen Teammitglieds!
Anmerkung: Das ist in vielen Organisationen die größte Herausforderung. Viele Mitarbeiter empfinden eine E-Mail als

persönliche Darreichung einer Information, selbst wenn das drei- oder viermal redundant erfolgt und man persönlich nur in CC steht. Im Team muss man sich selbst darum kümmern, gut informiert zu sein, was zunächst schwerfällt. Nachrichten wie „Wichtige Information bitte weiterhin per E-Mail schicken!“ sind in der Einführungsphase nicht selten.

Hierbei müssen Sie Ihre Mitarbeiter mitnehmen und unterstützen – und zwar durch alle Führungsebenen hindurch. Natürlich geht es vordergründig um mehr Produktivität durch Kreativität und Dynamik im Team. Die Effizienz Ihrer Teams ist ein ernstes Thema.

Effizienz können Sie aber nur erreichen, wenn Ihre Mitarbeiter lernen und verstehen, dass sie im Team und mit diesen Tools besser und effektiver arbeiten können, dass Teamarbeit ein konkreter Vorteil für sie selbst darstellt. Wenn Teamorientierung als Schikane wahrgenommen wird oder von der Führungsebene nicht unterstützt wird, können Sie nicht erwarten, dass sich ein solches Produkt von allein auf breiter Basis in der Belegschaft durchsetzt.

Warum Office 365 wichtig ist

Aber kommen wir jetzt zur technischen Umsetzung einer Office-365-Einführung.

Office 365 ist nicht einfach die nächste Version von Office 2016 oder Office 2019, auch wenn Microsoft diese Assoziation offensichtlich ganz recht ist. Unter dem Namen Office 365 versammeln sich zunächst einmal eine Reihe unterschiedlicher Lizenzpakete, Microsoft nennt sie „Pläne“, auf Mietbasis für Cloud-Dienste, Cloud-Anwendungen, Apps für Desktops und Smartphones und klassische Desktop-Anwendungen. Gemeinsam ist allen Plänen:

- Azure AD als Basis für Administration und Verwaltung,
- die Cloud-Dienste Exchange, SharePoint, OneDrive, Skype for Business bzw. Teams als Basis für E-Mail, Datenerhaltung und Kommunikation (die Pläne ProPlus und Business enthalten nur OneDrive),
- den Zugriff auf klassische Office-Formate wie Word, Excel, PowerPoint und Outlook – in jedem Fall in den browserbasierenden Online-Versionen, in den höherwertigen Plänen auch als lokal installierbare Version für Windows und MacOS.

In jedem Fall umfasst Office 365 durch die Integration der Cloud wesentlich mehr

Funktionen und Anwendungen als nur die vier oder fünf Büroanwendungen der klassischen Office-Suiten. Mit Office 365 sind Sie in der Cloud und müssen damit Ihre oben andiskutierten Basisaufgaben erledigen!

Die große Bedeutung, die Office 365 am Markt hat, liegt jetzt nicht zuletzt darin, dass Microsoft mit Office 365 viele der oben angesprochenen Anforderungen durchaus zufriedenstellend und mit stellenweise umfangreicher Funktionalität adressiert:

- Azure AD stellt das zentrale Benutzer- und Gruppenverzeichnis für alle Office-365-Anwendungen zur Verfügung.
- Mit AD Connect kann ein eigenes Active Directory on-premises mit Azure AD synchronisiert werden.
- Cloud-Anwendungen Dritter können im Azure AD eingebunden werden und via SAML, Single Sign-On (SSO) und Auto-Provisioning kann auch deren Benutzerverwaltung in den meisten Fällen integriert und damit zentral administriert werden.
- Mit Funktionen wie Multi-Faktor Authentifizierung (MFA) und Conditional Access kann darüber hinaus auch der Zugriff auf Cloud-Anwendungen (egal ob es sich um Office-365-Anwendungen oder eingebundene Anwendungen Dritter handelt) detailliert gesteuert werden.
- SharePoint und OneDrive decken den Bereich Dokumentenverwaltung, Dokumentenkollaboration und Freigabe ab.
- Mit Intune stehen Werkzeuge zum Mobile Device Management (MDM) und zum Schutz mobiler Endgeräte zur Verfügung.
- Über das Office 365 Security & Compliance Center haben Sie Zugriff auf eine Reihe von Überwachungsfunktionen und Sicherheitsberichte zum Zustand und Nutzung von Office 365.
- Azure Information Protection (AIP) und Azure Advanced Threat Protection (ATP) runden die verfügbaren Sicherheits- und Datenschutzmechanismen weiter ab.

Microsoft bietet ihren Kunden also einen durchaus komfortablen Weg in die Cloud. Ein Komfort, der jedoch gefährlich sein kann! Insbesondere dann, wenn Sie kein Plan haben, was Sie in der Cloud wollen, wenn Sie keine Vision, keine Zielvorgaben, keine „Cloud Policy“ haben.

Microsoft baut übrigens diesen Komfort, alles aus einer Hand beziehen und betreiben zu können, mit neuen Lizenzsuiten, die nicht mehr „Office 365 ...“, sondern

Ethernet im Takt

Fog und Edge Computing – Datenverarbeitung im IoT

Fortsetzung von Seite 1



Tanja Ulmen ist als Beraterin im Competence Center Smart Technologies der ComConsult Beratung und Planung GmbH tätig. Sie beschäftigt sich mit der Datenverarbeitung in smarten Systemen und im Rahmen ihrer beruflichen Tätigkeit setzt sie sich intensiv mit intelligenten Gebäuden auseinander.

IoT: Die Menge ist der Unterschied

Jeden Tag kommen neue vernetzte Geräte auf den Markt. Sei es eine smarte Kaffeemaschine, ein neuer Sensor oder lediglich ein neues Smartphone. Diese Geräte sind mittlerweile so weit vernetzt, dass es keinen Menschen mehr braucht, um Daten untereinander auszutauschen. Im Internet of Things (IoT) kommunizieren verschiedenste Geräte untereinander mit dem Ziel, Prozesse zu automatisieren und zu verbessern.

Ein Smartphone schickt Daten an eine Kaffeemaschine, ohne dass eine Interaktion des Nutzers notwendig ist. Das Resultat ist der fertig gebrühte Kaffee, nachdem morgens der Smartphone-Wecker klingelt (sofern abends eine Tasse bereitgestellt wurde). Ein Getränkeautomat bestellt automatisch Nachschub wenn Bedarf besteht und das Licht im Flur geht an, wenn der Bewohner nach Hause kommt.

Bei diesen Beispielen sind die entstehenden Datenmengen eher gering. In vielen Fällen sind die Größenordnungen allerdings deutlich kritischer. Ein autonomes Fahrzeug erkennt die rote Ampel und hält an. Das Bauteil einer Industrieanlage bestellt automatisch einen Techniker noch bevor es kaputt geht (Predictive Maintenance). In diesen Fällen sind enorm viele Sensordaten notwendig, um entsprechende Entscheidungen automatisch treffen zu können. Und von diesen Entscheidungen hängen unter Umständen Menschenleben ab.

Ein interessantes Beispiel ist der Airbus A350, in dem insgesamt rund 6000 Sensoren verbaut sind. Jeden Tag werden hier 2,5 TB an Daten generiert. Der Airbus A380 soll 10.000 Sensoren pro Tragfläche enthalten. Es wird geschätzt, dass mindestens dreimal so viele Daten anfallen, die verarbeitet und analysiert werden müssen. [1]

Das Problem ist allgemein nicht die Größe der einzelnen Datenpakete, sondern die Menge. Ähnliche Ausgangssituationen treten bei smarten Gebäuden und vielen weiteren Anwendungsfällen auf.

Wohin also mit den anfallenden Daten? Wo gibt es genug Performance und Speicherplatz, um diese Daten zu verarbeiten?

Datenverarbeitung in der Cloud

Eine Möglichkeit, diese Daten zu verarbeiten ist die Nutzung der Cloud. Bei einem Cloud-Dienstleister kann je nach Bedarf Hardware (Infrastructure as a Service, IaaS), eine Plattform (Platform as a Service, PaaS) oder direkt vorkonfigurierte Software (Software as a Service, SaaS) gemietet werden. Gerade bei schwankendem Speicherbedarf oder wenn die Anschaffung eigener Hardware/Software vermieden werden soll, sind diese Lösungen sehr vorteilhaft.

Cloud Computing bietet also skalierbare Performance, skalierbaren Speicherplatz und zudem eine Erreichbarkeit unabhängig vom Standort und Endgerät. Die Daten können über Funknetze in die Cloud übertragen werden oder über die lokal vorhandene Netzwerkverbindung. Speziell für die Verarbeitung von vielen und großen Daten scheint Cloud Computing also ideal.

Für viele Anwendungsfälle ist die Datenverarbeitung in der Cloud auch tatsächlich ideal. Zum Beispiel für langfristiges Speichern von Daten, um Daten von überall erreichen zu können, für komplexe Datenanalysen oder Ähnliches. Big-Data-Analysen beispielsweise sind ohne die Datenverarbeitung in der Cloud kaum denkbar.

Für andere Anwendungsfälle ergeben sich bei der Nutzung der Cloud allerdings folgende Schwachstellen:

- **Bandbreite:** Zum einen kann die Datenübertragung in die Cloud sowohl über das lokale Netz als auch über Funknetze bereits einige Schwierigkeiten verursachen. Ein smartes Gebäude, ein autonomes Fahrzeug oder der bereits erwähnte Airbus hat schnell eine fünfstellige Anzahl von Sensoren. Diese Sensoren erfassen mehrmals pro Sekunde Daten. Wenn die erfassten Daten direkt über die lokale Netzwerkverbindung in die Cloud geschickt werden, kommt jedes Netz auf Grund der Menge an Daten irgendwann an seine Grenzen. Insbesondere die Bandbreite, die über Mobilfunk zur Verfügung steht, kann gerade in schlecht angebundenen Bereichen für diese Datenmengen zu gering sein. So kann bei einer falschen Konfiguration des Netzes und der Netzwerkkomponenten eine DoS-Attacke (Denial of Service) durch die eigenen Komponenten erzeugt werden.
- **Lange Wege:** Ein weiteres Problem ergibt sich zum Beispiel bei autonomen Fahrzeugen. Um eine angemessene Reaktionszeit des Fahrzeugs gewährleisten zu können, müssen Analysen, basierend auf den erfassten Sensordaten, möglichst in Echtzeit erfolgen. Eine Verzögerung von einigen Millisekunden kann in diesem Fall schon über Menschenleben entscheiden. Somit wäre es in diesem, und auch in anderen Anwendungsfällen, ein erheblicher Nachteil, auf eine hohe Latenz bei der Cloud-Anbindung angewiesen zu sein. Je nachdem wo sich die Server des Cloud-Dienstleisters befinden, die diese Berechnungen durchführen, können die Latenzen mehrere Sekunden betragen.
- **Offline-Analyse:** Darüber hinaus müssen die Daten von autonomen Fahrzeugen nicht nur in Echtzeit verarbeitet werden, sondern auch offline. Sollte das Auto durch ein Funkloch oder ei-

Fog und Edge Computing – Datenverarbeitung im IoT

nen Tunnel fahren, müssen die Funktionen des Autos (die auf der Auswertung der Sensordaten basieren) genauso zur Verfügung stehen, wie mit einer stabilen Netzanbindung. Das gilt natürlich nicht nur für autonome Fahrzeuge, sondern auch für weitere Anwendungsfälle.

Diese Punkte können also ausschlaggebend sein, wenn entschieden wird wo die Daten verarbeitet werden. Eine Alternative ist hier die lokale Vorverarbeitung der Daten. Eine solche Vorverarbeitung bieten sowohl Fog Computing als auch Edge Computing, jeweils mit anderen Schwerpunkten, die im Folgenden erläutert werden.

Fog Computing

Fog Computing ist ein Architekturmodell, um Daten lokal vorzuverarbeiten. Dafür wird eine zusätzliche Hierarchie-Ebene zwischen den Endgeräten, die Daten produzieren und der Cloud aufgebaut. Diese Ebene befindet sich im lokalen Netz, weist Cloud-ähnliche Strukturen auf und wird daher Fog genannt (engl.: fog = Nebel). Es bringt die Cloud also näher zu den Endgeräten (siehe Abbildung 1).

Die Elemente, die zwischen der Cloud und Endgeräten agieren, werden Fog Nodes genannt. Fast jedes Gerät im lokalen Netzwerk kann als Fog Node genutzt werden. Zum Beispiel Router, Kameras, Notebooks, Gateways, Server, etc. Also jedes Gerät, das eine gewisse Performance bereitstellt und sich im lokalen Netzwerk befindet.

Ist diese Struktur aus Fog Nodes erst einmal eingerichtet, bildet sie eine Art lokale Cloud. Die Fog Nodes kennen sich untereinander, interagieren miteinander und „wissen“, wer welche Daten verarbeiten muss und welche Daten wohin weitergeleitet werden müssen.

Da Fog Nodes meistens bereits vorhandene Geräte im Netzwerk sind, die schon für andere Aufgaben zuständig sind, ist es wichtig diese nur für einfache Analyseaufgaben zu verwenden. Komplexere Aufgaben müssen auf Grund der geringen Ressourcen der Fog Nodes weiterhin außerhalb dieses Netzes verarbeitet werden. Hierfür ist weiterhin die Cloud eine geeignete Lösung.

In einigen Fällen ist es möglich diese komplexen Aufgaben aufzuteilen, sodass ein Fog Node den zeitkritischen Teil einer Analyse übernimmt, um eine schnelle Antwort zu gewährleisten. Der fortführende Teil der Analyse, der dann weniger zeitkritisch oder komplexer ist, kann in der Cloud ausgeführt werden.

Ein einfaches Beispiel ist eine Maschine in einer Industriehalle, die mit Hilfe eines Sensors Bewegungen erkennt und daraufhin stoppt. Diese Reaktion muss in Echtzeit erfolgen, da ansonsten Menschen verletzt werden könnten. Hier ist es möglich, die direkte Reaktion (Maschine Stopp) von einem Fog Node zu erhalten. Die weiteren Schritte, die in einem solchen Fall nötig sein können (Bericht erstellen, Benachrichtigungen versenden, Arbeit ggf. wieder aufnehmen) kann ein entfernter Knoten in der Cloud übernehmen.

Fog Computing bietet also verschiedene Vorteile:

- Da diese einfachen Aufgaben nun lokal verarbeitet werden, sind die Latenzen deutlich geringer und Echtzeitanforderungen können eingehalten werden.
- Die Datenmengen, die über das Netzwerk übertragen werden, sind geringer, da bereits vorab Daten analysiert und zusammengefasst werden können. So ist es möglich die verfügbare Bandbreite anders zu nutzen oder diese sogar zu verringern.

- Durch die geringeren Datenmengen entstehen weniger Bottlenecks im Netz, somit ist die Fehleranfälligkeit geringer und der Datenfluss kann optimiert werden.
- Die Daten liegen nicht mehr auf unbekanntenen Servern an unbekanntenen Orten, sondern werden lokal verarbeitet. So kann im eigenen Umfeld sichergestellt werden, dass ein angemessener Datenschutz eingehalten wird. Entweder indem die Daten komplett im Fog verarbeitet werden oder indem sie vor dem Upload in die Cloud anonymisiert oder verschlüsselt werden.
- Die Daten werden dort verarbeitet wo sie entstehen, also bleibt der Kontextbezug erhalten.
- Anstatt einfache Analysen in batteriebetriebenen Endgeräten durchzuführen, können diese auf den nächsten Fog Node ausgelagert werden. So kann im Endgerät Energie gespart werden.
- Zudem ist die Performance im Fog skalierbar. Je mehr Geräte Teil des Fog Netzwerkes sind, desto mehr Daten können verarbeitet werden.

Fog Computing ist also eine gute Variante, um Daten aus dem Internet of Things zu verarbeiten und dabei die oben genannten Schwachstellen des Cloud Computing zu umgehen. Ein weiteres Konzept, um diese Daten außerhalb der Cloud zu verarbeiten ist Edge Computing.

Edge Computing

Edge und Fog Computing werden oft gleichgesetzt, bezeichnen aber unterschiedliche Strategien. Edge Computing findet im Gegensatz zu Fog Computing direkt am oder sogar im Endgerät statt, also am äußersten Rand des Netzwerkes (engl.: edge = Rand).

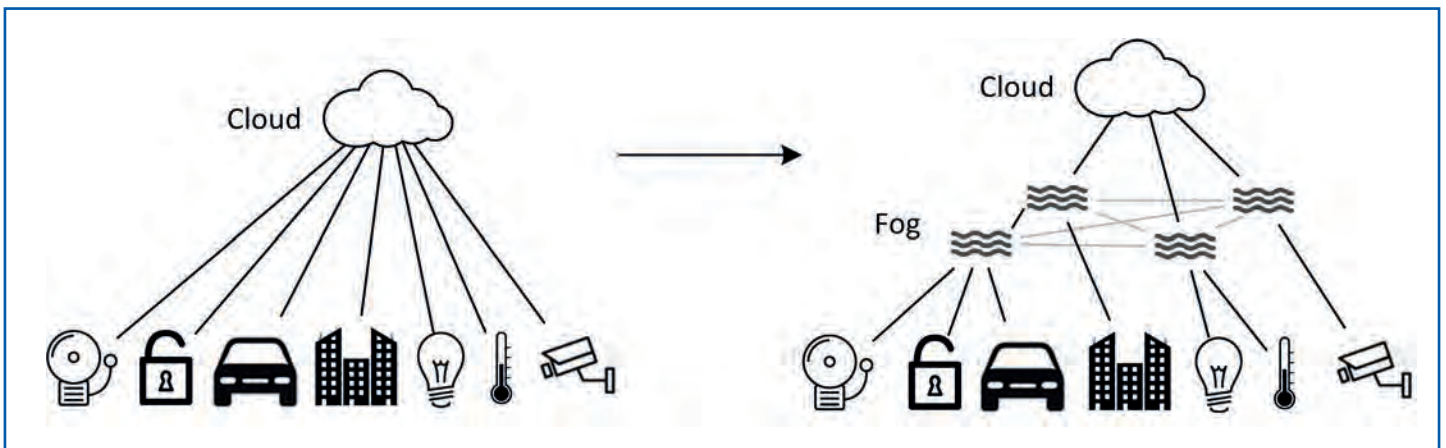


Abbildung 1: Fog Computing ermöglicht eine lokale Datenvorverarbeitung

Anmeldung

ComConsult Informationsservice

Verpassen Sie keine wichtigen Informationen mehr und tragen Sie sich in unserem ComConsult Informationsservice ein.

Unser Informationsservice informiert Sie regelmäßig per E-Mail und per Post über aktuelle Entwicklungen in der IT-Branche und über unsere Veranstaltungen und Neuerscheinungen. Der Service umfasst unser monatliches Magazin „Der Netzwerk Insider“, sowie regelmäßige E-Mails über unser aktuelles Produktangebot. Darüber hinaus senden wir Ihnen im Bedarfsfall unsere Technologie-Standpunkte und Technologie-Warnungen zu aktuellen Entwicklungen zu.

Anrede

Name

Firma

E-Mail-Adresse

oder online unter

<https://www.comconsult-research.de/insider-2/>