BOS-Leitstellen aus der Cloud

Whitepaper zur Betrachtung der Anwendbarkeit von Cloudlösungen bei den Leitstellen der Behörden und Organisationen mit Sicherheitsaufgaben (BOS)

von

Dipl.-Ing. Gerhard Schulz

Projektberatung
BOS-Leitstellen

Mit Unterstützung durch:

accellonet
wir finden eine Lösung

STF Gruppe
ENGINEERING NOW

TÜVIT
TÜV NORD GROUP

1 Einführung

Einsatzleitstellen sind bei Notfällen und Belangen der öffentlichen Sicherheit sowie im Brand- oder Katastrophenfall von hoher und oftmals sogar von existenzieller Bedeutung. Sie sind in der Regel rund um die Uhr erreichbar. Für das Gemeinwohl und zur Aufrechterhaltung von Recht und Sicherheit stellen Leitstellen einen erheblichen Beitrag im täglichen Leben der Bürger dar.

Die Aufgaben und Funktionen von Leitstellen werden durch die polizeilichen und nichtpolizeilichen Behörden mit Sicherheitsaufgaben (BOS) subsidiär wahrgenommen. Aufgrund des technologisch-gesellschaftlichen Wandels kommen zunehmend neue Anforderungen auf diese Behörden und deren Aufgabenwahrnehmung zu. Leistellen aus der Cloud stellen hierfür einen möglichen Weg dar.

Die föderale Struktur der Bundesrepublik Deutschland weist im Jahr 2018

- den Bund, und 16 Bundesländer,
- 294 Landkreise und 107 Kreisfreie Städte sowie
- 11.054 Gemeinden auf.

Während die polizeilichen BOS länder- und bundesorientiert organisiert sind, sind die nichtpolizeilichen BOS kommunal, d.h. kreis- und gemeindebezogen organisiert.

Nach einer Erhebung aus dem Jahre 2017 gibt es

- 122 polizeiliche Leitstellen,
- 233 nichtpolizeiliche Leitstellen sowie
- 130 Leitstellen der Institutionen des Bundes.

Die Anzahl der Leitstellen ist einem ständigen Wandel unterworfen, da durch Gebietsreformen oder durch Zusammenlegung von Leitstellen mehrerer Kreise eine Neuordnung erfolgt, die ihre Ursache maßgeblich in der Wirtschaftlichkeit und Effizienzsteigerung des Betriebes hat.

Die Zusammenlegung von Leitstellen erfolgt in den beiden Ausprägungen:

- Technikkonzentration oder
- Dienstleistungskonzentration.

Unabhängig von der Zusammenlegung von Leitstellen, die eine Dienstleistungskonzentration bedeutet, bleibt die Möglichkeit einer Technikkonzentration, die sowohl für eine dislozierte als auch für eine konzentrierte Leitstellenlandschaft angewandt werden kann. Hier ergibt sich der Vorteil der gleichzeitigen Eigenständigkeit der kommunalen Leitstellen mit einer wirtschaftlichen Einrichtung und dem wirtschaftlichen Betrieb der erforderlichen Technik. Durch immer weiter fortschreitende Digitalisierung und den qualitativen und quantitativen immer besseren Ausbau der Infrastruktur ist der sichere Transport von Daten über größere Entfernungen heute kein Problem mehr.

Es befinden sich bereits gemeinsam genutzte Anwendungen in Gebrauch. So werden z.B. geografische Daten an zentraler Stelle aufbereitet und den Leitstellen zur Verfügung gestellt. Oder in der Sprachkommunikation werden Gateways oder Konzentratoren eingesetzt, um mehrere Leitstellen mit dem BOS-Digitalfunk zu verbinden.

Ein Vergleich mit der „nicht-BOS-Welt“ zeigt, dass die deutsche Industrie und der Handel bereits umfangreich auf zentralisierte Datenhaltung im eigenen Bereich aber auch ausgelagert bei Dienstleistern setzen.

Dabei werden derzeit noch überwiegend Daten in Private Clouds ausgelagert. Laut einer jährlich aktualisierten Studie der KPMG im Auftrag der BITKOM nutzten Ende 2017 66% der Unternehmen in Deutschland Cloud Computing. Näheres bitte ich dem Cloud-Monitor 2018[1]der KPMG/ bitkom zu entnehmen.

Grund für die Auslagerung sind die enormen Aufwände, die jedes Unternehmen für sich leisten müsste, um die Sicherheit und die Verfügbarkeit der sensiblen Datenhaltung zu gewährleisten. Es ist wirtschaftlicher die infrastrukturellen und betrieblichen Voraussetzungen zu schaffen, die von möglichst vielen Leitstellenbetreibern in Anspruch genommen werden.

Die Kontrolle der eigenen Daten verbleibt vollständig beim Leitstellenbetreiber.

2 Cloud - was ist das?

Unter einer Cloud (engl. Wolke) wird gemeinhin ein Ort für die elektronische Datenhaltung und -verarbeitung beschrieben, der irgendwo liegen kann. Die elektronische Datenverarbeitung kann dabei Daten und/oder Software beinhalten. Charakteristisch für eine Cloud ist die dynamisch anpassbare, flexible Rechen- und Datenkapazität.

Die Cloudlösungen werden nach der Nutzung und dem Zugang unterschieden. Sowohl bei der Nutzung als auch beim Zugang gibt es Mischformen der Cloud-Typen.

Entscheidend ist, dass der Ort nicht unbedingt beim Leitstellenbetreiber der Daten liegen muss. Er kann eben irgendwo liegen.

Der sichere Zugriff auf die Cloud und damit auf die Daten oder die Software erfolgt über ein IT-Netzwerk, das über öffentliche oder private Netze geführt wird.

Eine Cloud wird durch einen Cloud-Betreiber bereitgestellt, der seine Investitionen und Betriebskosten an den Leitstellenbetreiber in Form von regelmäßigen Zahlungen weitergibt.

Die Nutzung einer Cloud wird mit Cloud Computing beschrieben. Sie stellt die dynamische Bereitstellung IT-Ressourcen und gegebenenfalls Anwendungen dar.

2.1 Unterscheidung der Cloud-Typen

Nach der Definition des National Institute of Standards an Technology (NIST) aus dem Jahre 2009 wird Cloud Computing in drei unterschiedliche Servicemodelle (nach Nutzung) und vier verschiedene Liefermodelle (nach Zugang) unterscheiden.

2.1.1 Servicemodelle

Die nachstehenden Service-Modelle unterscheiden sich in den Dienstleistungen, die durch den Cloudbetreiber erbracht werden. In der Praxis ergibt sich überwiegend aus einer Mischung der Service-Modelle. Es hat sich ein Begriff „Anything as a Service“ (XaaS) etabliert, der diese Nutzung beschreibt.

[1] KPMG im Auftrag der bitkom (https://www.bitkom.org/Presse/Anhaenge-an-PIs/2018/180607-Bitkom-KPMG-PK-Cloud-Monitor-2.pdf)

Infrastructure-as-a-Service (IaaS)

Der Cloud-Betreiber bietet in diesem Fall lediglich den Nutzungszugang zu Rechnern, Speichern und sonstigen Hardware-Ressourcen.

Der Leitstellenbetreiber ist für die Auswahl, die Einrichtung, den Betrieb und die Funktion der Software selbst verantwortlich.

Platform-as-a-Service (PaaS)

Der Cloud-Betreiber bietet bei der PaaS den Zugang zu Laufzeit- und Programmierumgebungen. Der Leitstellenbetreiber kann seine eigenen Software-Anwendungen entwickeln und ausführen.

Software-as-a-Service

Hier werden vollständig Anwendungen durch den Cloud-Betreiber angeboten. Der Leitstellen-betreiber kann über den bereitgestellten Zugang Anwendungsprogramme und Speicher nutzen. Die Einrichtung und Pflege der Hard- und Software obliegt ausschließlich dem Cloud-Betreiber.

2.1.2 Liefermodelle

Public Cloud

Der Cloud-Betreiber bietet öffentlich IT-Infrastrukturen an, die nach der tatsächlichen Nutzung abgerechnet werden.

Private Cloud

Die Private Cloud bietet lediglich einem fest umrissenen Nutzerkreis den Zugang zur darin befindlichen IT-Infrastruktur. Sie ist individuell auf den Nutzerkreis zugeschnitten und von anderen Clouds getrennt. Die Hardware der Private Cloud wird meist im eigenen Unternehmen oder in landesspezifischen Lokationen eingerichtet.

Hybrid Cloud

Die Verbindung der beiden vorgenannten Liefermodelle bietet die Sicherheit einer Private Cloud für sicherheitsrelevante Anwendungen und Daten und die Möglichkeit öffentliche IT-Services zu nutzen. Die Sicherheit durch Abgrenzung der beiden Modelle gegeneinander hat der Cloud-Betreiber zu gewährleisten.

Community Cloud

Die Community Cloud bietet ihre Dienste einem örtlich verteilten Nutzerkreis an. Eine Community-Cloud ist eine mandantenfähige Infrastruktur, die von einer Gruppe von Organisationen mit den gleichen Anforderungen gemeinsam genutzt wird. Die gemeinsamen Interessen können beispielsweise in der Einhaltung von offiziellen Compliance-Vorgaben liegen.

2.2 Cloud-Betreiber

Je nach Liefermodell sind verschiedene Anbieter vorhanden bzw. möglich. Die Public Cloud wird von verschiedenen Betreibern angeboten (z.B. Microsoft, Dropbox).

Private Clouds und Hybrid Clouds werden meist als firmenweite, auch landesweite oder globale, gemeinsame Daten- und Anwendungsplattform genutzt, die sowohl IaaS, PaaS und SaaS liefern.

Dabei nimmt die Hybrid-Cloud den größeren Anteil ein, weil er den Leitstellenbetreiberanforderungen nach sicherer Umgebung für sensible Daten und Anwendungen bei gleichzeitiger Nutzung öffentlicher IT-Dienste am nächsten kommt.

3 Exemplarische Cloudlösungen

Reine „private Cloud“-Lösungen bieten in sich geschlossene Systeme. Übergänge bzw. Kopplungen mit anderen Systemen müssen sehr genau geplant und bedacht werden, damit der Sinn der „private Cloud“ nicht ad absurdum geführt wird.

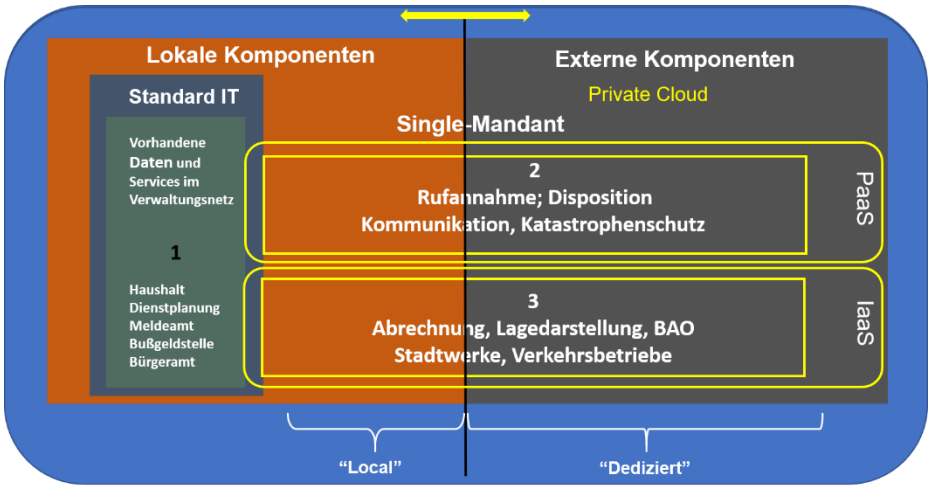

Abbildung 1: Private Cloud

Wird hingegen eine Hybrid Cloud eingesetzt, wird die Private Cloud um eine Public Cloud ergänzt.

Die Anteile der Hybriden Cloud, die durch einen Dienstleister geliefert werden sollen bzw. die Anteile, die im eigenen Bereich verbleiben sollen, können dynamisch verschoben werden. Je nach Vertrauen, das der Leitstellenbetreiber dem Cloud-Betreiber entgegenbringt, werden sich die Anteile der Daten- und Anwendungshaltung unterschiedlich verteilen.

Entscheidend ist aber, dass die Aufteilung der Anteile nur in der Private Cloud vorgenommen werden, da die Public Cloud von verschiedenen Nutzergruppen genutzt wird und somit vollständig in der Verantwortung des Cloud-Betreibers verbleiben muss. Der Cloud-Betreiber hat für die Sicherheit am Übergang zwischen Private und Public Cloud zu sorgen.

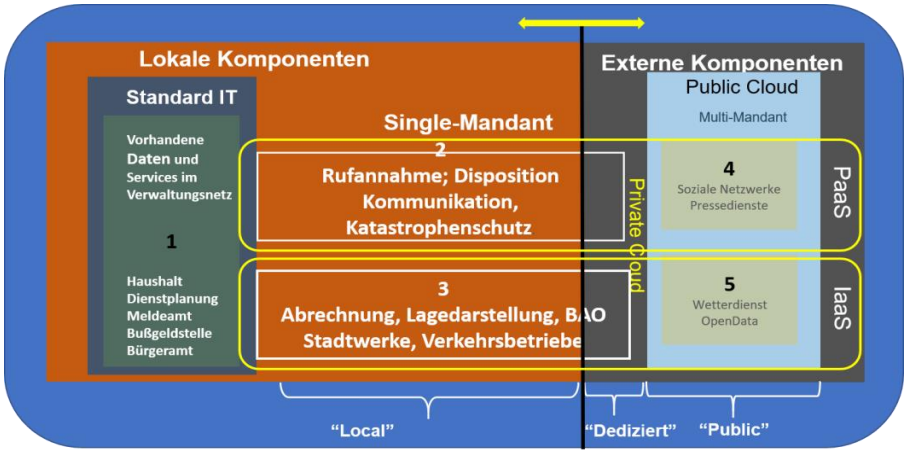

Abbildung 2: Hybrid Cloud mit hohem Nutzeranteil

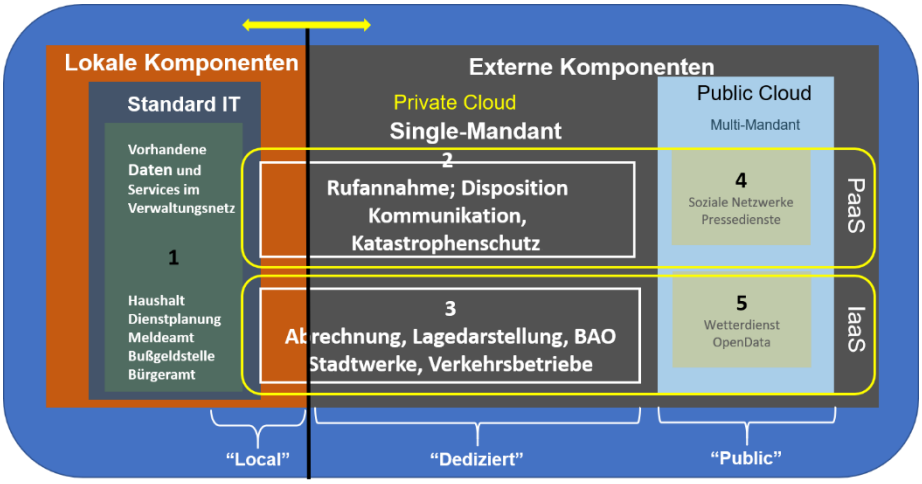

Abbildung 3: Hybrid Cloud mit hohem Betreiberanteil

Bei einer Auslagerung der Softwareanteile in die Private Cloud kann auch der Übergang in die Managed Cloud gewählt werden, bei der der Cloud-Betreiber nicht nur die Infrastruktur und die Plattformen bereitstellt, sondern auch die darauf aufsetzenden Tools und Anwendungen einrichtet und betreut. Im Extremfall errichtet und betreibt der Cloud-Betreiber die gesamte Anwendung und bietet dem Kunden die Nutzung als Dienstleistung an. Damit sind alle Vorhaltungen, auch die Endgeräte, die beim Kunden zur Nutzung der Anwendung benötigt werden Teil der ausgelagerten Leistung.

Bei den BOS sind bereits Cloud-Lösungen vorhanden, die aber nicht so benannt wurden. Beispielsweise die eingesetzten Digitalfunkkonzentratoren, die für mehrere Nutzer Digitalfunkressourcen bereitstellen ist eine Cloudlösung. Ein anderes Beispiel sind zentral bereitgestellte GIS-Daten, die von verschiedenen Nutzern abgerufen und in den eigenen Applikationen eingesetzt werden.

4 Abgrenzung der Cloudlösungen

4.1 Auslagerung der Daten

Nur Datenbanken in der Cloud:

- Die Bereitstellung und Pflege der Datenbankhardware und datenbanknaher Funktionen erfolgt durch den Cloud-Betreiber.
- Die Inhalte der Datenbanken werden durch die Leitstellenbetreiber gepflegt.

Alle anderen Applikations-Server und Endgeräte und die zugehörigen Applikationen und die Zugriffe auf die Datenbankinhalte verbleiben in der Verantwortung des Leitstellenbetreibers.

4.2 Auslagerung der Daten und der Server

Datenbank und Server in der Cloud:

- Datenbank wird ausgelagert
  - Die Bereitstellung und Pflege der Datenbankhardware und datenbanknaher Funktionen erfolgt durch den Cloud-Betreiber.
  - Die Inhalte der Datenbank werden durch den Leitstellenbetreiber gepflegt.

- Server werden ausgelagert
  - Die Bereitstellung und Pflege der Server liegen beim Cloud-Betreiber.
  - Betriebssystem und betriebssystemnahe Software durch Cloud-Betreiber.
  - Anwendungs-Software wird durch den Leitstellenbetreiber installiert und gepflegt.

Alle anderen Applikationen und die Zugriffe auf die Datenbankinhalte verbleiben in der Verantwortung des Leitstellenbetreibers.

4.3 Auslagerung der Daten und der Software

- Datenbank wird ausgelagert
  - Die Bereitstellung und Pflege der Datenbankhardware und datenbanknaher Funktionen erfolgt durch den Cloud-Betreiber.
  - Die Inhalte der Datenbank werden durch den Leitstellenbetreiber gepflegt.
- Server werden ausgelagert
  - Die Bereitstellung und Pflege der Server liegen beim Cloud-Betreiber.
  - Betriebssystem und Betriebssystemnahe Software durch Cloud-Betreiber.
- Software wird ausgelagert
  - Anwendungs-Software wird durch den Cloud-Betreiber installiert und gepflegt.
  - Der Anwender nutzt die vom Cloudbetreiber angebotene Dienstleistung.

5 Vorteile einer Cloudlösung

Nutzer von Cloud Computing können auf bedarfsgerechte Kapazitäten zugreifen. Nach kurzfristiger Ankündigung kann der Kapazitätsbedarf dann fallspezifisch immer wieder den aktuellen Erfordernissen und Gegebenheiten angepasst werden.

Zudem können Anwender von massiven Größenvorteilen der Anbieter nachhaltig profitieren, da die hohen Nutzungsraten zu niedrigeren Preisen führen Die Preisgestaltung erfolgt in der Regel nutzungsabhängig (Pay-per-use-Modell).

Es muss lediglich für EDV-Ressourcen gezahlt werden, die auch tatsächlich in Anspruch genommen werden. Investitionskosten, zum Beispiel für eigene Server und Rechenzentren, fallen beim Outsourcing komplett weg.

Da neue IT-Ressourcen in einer Cloud Computing Umgebung stets zeitnah zur Verfügung stehen, erhöht sich die Agilität einer Organisation enorm. Denn der Aufwand für Entwicklung und experimentelle Nutzung, z.B. für Pilotvorhaben, verringern sich in einem wesentlichen Umfang. Die Bearbeitung von gleichbleibenden Vorgängen wird damit effizienter.

Entsprechende Anwendungen können landesweit schnell in Betrieb genommen werden. So erhöhen Organisationen ihre regionale Reichweite durch einfache zusätzliche Konfiguration und Freischaltung.

In Abhängigkeit vom Nutzungsmodell fallen mehr oder weniger Kosten für den Betrieb von eigenen Servern, der allgemeinen Datenverarbeitung oder etwa für die Wartung von Rechenzentren an.

5.1 Zukunftssicherheit

Eine zentralisierte IT-Infrastruktur ergibt einfachere Möglichkeiten der Aktualisierung der Hard- und Software. Infolge dessen sind auch zukünftige auf die Leitstellenbetreiber zukommenden Aufgaben-stellungen oder Veränderungen der externen Schnittstellen einfacher, weil einmalig, darzustellen. Eine Reaktion auf Veränderung der Umgebung kann schneller und gezielter erfolgen. Das Ergebnis steht dann allen Leitstellenbetreibern der Cloud-Lösung gleichzeitig zu Verfügung.

Somit ist für viele gleichzeitig ein hohes Maß an Zukunftssicherheit gegeben.

Die Verpflichtung zur Dienstleistungserbringung durch den Cloudbetreiber ist vertraglich langfristig zu sichern.

5.2 Standardisierung

Die Zentralisierung von Leitstellenlösungen in einer Cloud wird automatisch eine stärkere Standardisierung fördern, da der Cloud-Betreiber bestehende oder gleiche Lösungen erheblich günstiger anbieten können.

Eine zunehmende Standardisierung wird sich positiv auf die Kostenentwicklung für die Leitstellen-betreiber auswirken, da die Industrie weniger Aufwand in Entwicklung, Prüfprozesse und Wartung stecken muss.

Weitere Vorteile, die sich aus der Standardisierung ergeben sind:

- Synergien, die sich bei Um- und Nachrüstungskonzepten für neue Techniken
- Gemeinsame Konzepte zur Informationssicherheit
- Einheitliche ggf. gemeinsame Ausbildungs- und Schulungsmaßnahmen
- Vereinfachung und Bündelung von Beschaffungsprozessen
- Vereinfachte Investitionsentscheidungen
- Herstellerunabhängigkeit.

5.3 Dienstebereitstellung

Für die Dienstebereitstellung aus einer Cloud sind nachstehende Aspekte zu beachten, die durch den Cloud-Betreiber dargestellt werden müssen und sich positiv auswirken:

- Sichere Übergänge zur Außenwelt (Internetzugänge, andere Datenbanken, Updates, Grafikdaten)
- Gemeinsame Dienste bereitstellen
- Gemeinsame mandantengetrennte oder getrennte Datenbanken in einer großen DB-Lösung
- Anwendungen gemeinsam verfügbar machen
- Diensteübernahme durch andere Leitstelle möglich
- Landeslösungen einfach möglich

Durch die konzentrierte Bereitstellung der Dienste auf der Basis getrennter Datenbanken und Anwendungen ist eine relativ leichte Verschiebung von Verantwortlichkeiten von einer Leitstelle auf eine andere oder von einer Leitstelle auf eine Not-Leitstelle möglich.

Die in einer Cloud gegebene Skalierbarkeit können steigende Anforderungen an die Dienstebereitstellung rasch realisiert werden.

5.4 Infrastruktur

Wenn die einzelnen Komponenten mit einer Priorität versehen werden, die für einen Leitstellenbetrieb wichtig sind, ergibt sich folgende Reihenfolge:

1. Haus oder Raum
2. Stromversorgung (redundante Hauseinführung, redundante USV und Ersatzstrom)
3. Klimatisierung
4. Sicherheit (Zugang, BSI-Grundschutz, Datenschutz)
5. Server/Netzwerk/Applikationen
6. Hochverfügbarkeit und Bandbreite der Anbindung an das Rechenzentrum

Daraus wird deutlich, dass der Infrastruktur eine maßgebende Bedeutung zukommt, die sowohl einen gesicherten technischen Betrieb als auch die Sicherheit der verarbeiteten Daten durch die dort beheimateten IT-Einrichtungen gewährleistet. Alle aufgeführten Komponenten sind in sicherer und gesicherter Form einzurichten.

Die erforderliche bauliche Ausführung der Infrastruktur erfordert erhebliche Investitionen und Betriebskosten. Die EN 50518 beinhaltet Anforderung für Alarmempfangszentralen. Sie kann als Anhaltspunkt für infrastrukturelle Anforderungen an einen Cloudbetreiber dienen.

Gemäß BSI-Grundschutz und EN 50518 sind infrastrukturellen Anforderungen für einen Serverbetrieb in einem Rechenzentrum (Gebäudesicherheit, Zugangssicherheit, Stromversorgung, unterbrechungsfreie- und Ersatzstromversorgung, Klimatisierung) zu erfüllen, die für einen sicheren und gesicherten Betrieb von Leitstellenanwendungen notwendig sind.

Mit der Nutzung einer Cloudlösung wird der notwendige infrastrukturelle Aufwand drastisch reduziert, da der Aufwand nur einmal für mehrere Nutzer getrieben werden muss.

Was für die Technik in der Cloud gilt, ist auch für die in der Leitstelle vorhandene Technik erforderlich. Je größer der eigenbetriebene Anteil der Leitstellentechnik ist, je größer sind die Aufwände für den Leitstellenbetreiber im eigenen Hause. Rechenzentren (also Serverstandorte und Netzwerkkomponenten) haben z.B. erheblich höhere Grundschutz-Anforderungen als Arbeitsplatztechnik.

5.5 Technischer Betrieb

Ein zentralisierter Betrieb der Server (inkl. Betriebssysteme und betriebssystemnaher Software), dem Netzwerkkomponenten sowie die Betreuung der Datenbanken wird durch spezialisiertes und gut ausgebildetes Personal, das die Einrichtungen ständig überwacht und daran arbeitet, erheblich effizienter und sicherer.

Durch Nutzung des Rechenzentrums durch mehrere Organisationen wird der Serverpark z.B. durch einen hohen Grad der Virtualisierung flexibel und skalierbar, sodass die Rechenleistung kurzfristig bedarfsgerecht bereitgestellt werden kann.

Die Virtualisierung von Rechnerkapazitäten bietet ein hohes Maß an Verfügbarkeit und eine optimale Lastverteilung. Durch rasche Verlagerungen von Anwendungen können wartungsbedingte Down-times von Applikationen nahezu ausgeschlossen werden.

In verschiedenen Service-Modellen kann in Abhängigkeit von der Cloud-Variante ein angepasstes Konstrukt mit dem Cloud-Betreiber verhandelt werden.

Ist die Nutzung einer Managed Cloud geplant, werden Updates und erforderliche bzw. gewünschte Anpassungen durch den Cloud-Betreiber vorgenommen. Sollen lediglich Dienstleistungen aus der Cloud genutzt werden, so ist mit dem Cloud-Betreiber vertraglich der Umfang der Dienstleistung festzulegen. Der Cloud-Betreiber ist dann für die Datenhaltung, die Anwendungssoftware, die Server-Hardware und das Netzwerk verantwortlich.

5.6 Reinvestitionen

Die Einrichtungen der Cloud werden kontinuierlich durch den Cloud-Betreiber auf dem aktuellen Stand gehalten. Für die Erneuerung der Hardware fallen somit für den einzelnen Leitstellenbetreiber keine wellenartigen Investitionsbedarfe an, sondern werden auf die Leitstellenbetreiber verteilt und kontinuierlich finanziert.

5.7 Verfügbarkeit

Rechenzentren, die Cloudoptionen anbieten, müssen per se redundant ausgelegt sein, da sie sonst die erforderlichen Service-Level nicht einhalten können. Die Redundanz kann unterschiedlich ausgestaltet sein. Von einer Standortredundanz bis zu einer Redundanz in verschiedenen Brandabschnitten gibt es verschiedene Varianten, die der Cloud-Betreiber anbieten kann. Durch die Virtualisierung der Server ist eine schnelle Ersatzgestellung möglich, sodass Ausfallzeiten auf ein Minimum reduziert werden können.

Die Darstellung der ständig und gleichbleibend hohen erforderlichen Verfügbarkeit ist Aufgabe des Cloud-Betreibers. Der Cloud-Betreiber muss die Redundanzmechanismen und deren Wirkung nachweisen. Zugleich muss er die SLA (Service Level Agreements) offenlegen, die er garantieren kann.

5.8 Datensicherheit

Die Datensicherheit wird beschrieben als die Menge der Maßnahmen zum Schutz des Anwenders in Hinblick auf die Funktionsfähigkeit von DV-Systemen und insbesondere zu Schutz vor Verfälschung und Verlust von Daten und vor unberechtigten Zugriffen auf Daten.

Um diese Anforderungen sicherzustellen sind Maßnahmen zu treffen, die den Schutz gegen beabsichtigte Angriffe und gegen unbeabsichtigte Ereignisse gewährleisten.

Diese umfangreichen Schutzmechanismen sind durch die jeweiligen Betreiber von Rechenzentren, also auch von jedem Leitstellenbetreiber sicherzustellen.

Sehr gute Kenntnisse der Gefahreneinschätzung und der angepassten Maßnahmen sind erforderlich, damit die Datensicherheit gegeben ist.

Durch hohe Kompetenz, die ein Cloud-Betreiber besitzen muss, ist die hohe Datensicherheit und der professionelle Umgang mit der Verantwortung sicherzustellen.

5.9 Datenschutz (DSGVO)

Die Nutzung einer Cloudlösung entbindet den Leitstellenbetreiber nicht von seiner grundsätzlichen Verpflichtung zum Datenschutz gemäß der DSGVO. Für die gespeicherten und verarbeiteten Daten ist auch bei einer Cloudlösung immer der Leitstellenbetreiber, also der Leitstellenbetreiber, verantwortlich.

Vom Cloud-Betreiber sollte sich der Leitstellenbetreiber mit anerkannten Zertifikaten eine Teilbescheinigung für dessen Zuständigkeitsbereich geben lassen.

Am 25. Mai 2018 trat die Europäische Datenschutzgrundverordnung in Kraft mit teils weitreichenden Konsequenzen für Unternehmen. So haben Privatpersonen damit das Recht, von Unternehmen, denen sie im Zuge einer Geschäftsbeziehung ihre Daten anvertraut haben, auf Anfrage umfassende Auskunft über die Verarbeitung ihrer persönlichen Daten zu erhalten. Die Unternehmen wiederum unterliegen dann der Kontrolle staatlicher Prüfinstanzen, weshalb sie gefordert sind, nicht nur für Sicherheit, sondern auch für Transparenz in ihren Datenverarbeitungsprozessen zu sorgen.

Zu den Garantien sagt die DSGVO: „Die Einhaltung genehmigter Verhaltensregeln (Artikel 40) oder eines genehmigten Zertifizierungsverfahrens (Artikel 42) durch einen Auftragsverarbeiter kann als Faktor herangezogen werden, um hinreichende Garantien nachzuweisen."

Der Cloud-Betreiber muss zwingend die Vorgaben der neuen EU-DSGVO einhalten. Um dies nachzuweisen sollte er geprüft und auditiert sein. Der Nachweis kann mittels eines von der Forschungsgruppe AUDITOR entwickelten Standards, dem Trusted Cloud Datenschutz-Profil für Cloud-Dienste (TCDP), für eine Datenschutzzertifizierung nach der DSGVO erfolgen. Dabei wird eine Anerkennung durch den Europäischen Datenschutz-Ausschuss nach Art. 42 Abs. 5 DSGVO angestrebt. Eine eigene Prüfung nach § 11 Abs. 2 BDSG durch den Auftraggeber, also die Leitstelle selbst, ist damit nicht mehr erforderlich.

Trusted Cloud Datenschutz-Profil für Cloud-Dienste

Unabhängig vom genutzten Modell einer Cloud, selbst ohne Einsatz einer Cloud, sind die Vorschriften der DSGVO einzuhalten. Werden Cloud-Dienste genutzt, unterliegen die Endgeräte ebenfalls den Vorschriften der DSGVO. Die polizeilichen und nichtpolizeilichen Leitstellenbetreiber müssen für sich prüfen, ob sie die personelle und fachliche Kompetenz besitzen diese Anforderungen umzusetzen und kontinuierlich fortzuschreiben.

5.10 Wirtschaftlichkeit

Gemeinsam betriebene oder genutzte Cloud-Lösungen sind überaus wirtschaftlich für die Leitstellenbetreiber.

Durch die Bereitstellung von Infrastruktur, Hardware und Software, gepaart mit der zugehörigen Wartung, Instandhaltung und Reinvestition für sehr viele Leitstellenbetreiber steigert sich die Wirtschaftlichkeit sowohl für den Leitstellenbetreiber, der nur die von ihm genutzten Ressourcen bezahlen muss, als auch für den Cloud-Betreiber, der Ressourcen für mehrere Leitstellenbetreiber gemeinsam bereitstellen kann.

Durch den konzentrierten Betrieb mit kompetentem Personal sind durch Leitstellen geforderte SLA wirtschaftlich einzuhalten.

5.11 Haushalt

Da nur die vom Leitstellenbetreiber tatsächlich genutzten Ressourcen abgerechnet werden, ist die Einstellung von Haushaltsmitteln seitens der Leitstellenbetreiber berechenbar und in die lang- und mittelfristige Haushaltsplanung zu verankern.

Der Cloud-Betreiber kann aufgrund der langfristigen Verträge mit den Leitstellenbetreibern eine strategisch langfristige Planung der technischen Einrichtungen durchführen und sukzessive weitere Dienstleistungen anbieten, die den Anteil der nutzereigenen Datenverarbeitung reduzieren.

5.12 Vergabe von Cloud-Dienstleistungen

Bei der Vergabe von Cloud-Dienstleistungen sind neue, bisher noch nicht bei Leitstellenausschreibungen beschriebene Leistungen und Bedingungen zu fordern (wie z.B. die Virtualisierung der Ressourcen und Dienste, die verbrauchsabhängige Abrechnung der Leistungen, die dynamische Anpassung der Kapazitäten gemäß den Anforderungen der Leitstellenbetreiber, der Schutz und die Isolation verschiedener Mandanten), die im Detail erarbeitet werden müssen.

Im Zuge der Planung einer Cloudlösung sind bei der Vergabe der Leistungen die vergaberechtlichen Bedingungen zu prüfen, da die Auslagerung der Dienstleistung eine langfristige Entscheidung darstellt.

6 Risiken einer Cloudlösung

Die Nutzung einer Cloudlösung birgt natürlich auch verschiedene Risiken in sich. Nachstehend sind einige Risiken aufgeführt, die bei einer Nutzung der Cloud-Dienste weitgehend ausgeschlossen werden müssen. Wie bei jeder Risikobetrachtung sind auch hier den Risiken entsprechende Maßnahmen entgegen zu setzen, die das Risiko auf ein verantwortbares Maß reduzieren.

6.1 Risiken der Cloud

Der Einsatz einer Cloudlösung ist bei den BOS noch nicht so verbreitet, dass umfangreiche und komplexe Integration in eine Cloud als Standardprodukt vorhanden sind. Daher ist eine der Beginn mit einer zu umfangreichen Umsetzung ein grundsätzliches Risiko, das vermieden werden muss. Wie bereits unter Pkt. 3 dargestellt kann eine Cloudlösung mit einem geringen Teil ausgelagerter Daten oder Applikationen beginnen und mit wachsender Erfahrung sukzessive gesteigert werden.

- Missbrauch und schädliche Nutzung von Cloud Computing:
  Begünstigt durch grundlegende Eigenschaften von Cloud-Infrastrukturen - etwa die schnelle und einfache Verfügbarkeit neuer Ressourcen mit sehr guter Netzanbindung - ist die Nutzung von Cloud-Ressourcen für Angreifer sehr interessant, um beispielsweise Denial-of-Service-Attacken (DoS) zu starten oder Schadsoftware zu hosten.
- Unsichere Schnittstellen und APIs:
  Cloud-Services und die von den Anbietern zur Verfügung gestellten Managementschnittstellen sind bei Cloud-Angeboten über das Internet/Intranet erreichbar und lassen sich daher leicht angreifen. Darüber hinaus existieren Programmierschnittstellen, die von den Anwendern zur Steuerung und Konfiguration der Cloud-Services verwendet werden können. Schwachstellen an diesen Interfaces öffnen möglicherweise Einfallstore, die von Unbefugten genutzt werden, um beispielsweise unrechtmäßigen Zugriff auf Kundendaten zu erhalten.
- Böswillige Insider:
  Sicherheitsmaßnahmen der Software sind oft wirkungslos, wenn der Angreifer auf die Infrastruktur des Cloud-Anbieters legal zugreifen kann. Das ist beson-

ders bei böswilligen Insidern der Fall - also Mitarbeitern des Cloud-Anbieters, die sich Zugriff auf Kundendaten verschaffen.

- Risiken durch geteilte Technologien:
  Eine weitere Eigenschaft von Cloud Computing ist das sogenannte Pooling von Ressourcen. Das bedeutet, dass die physischen Ressourcen von allen Anwendern der Cloud-Services gemeinsam verwendet werden. Dabei können sich Probleme bei der zuverlässigen Trennung der Nutzerdaten ergeben.
- Datenverlust und -kompromittierung:
  Weil die Daten in der Cloud gespeichert sind und viele Anwender gleichzeitig dieselbe Infrastruktur verwenden, ergeben sich besondere Anforderungen an die Datensicherheit. Probleme bei Cloud-Betreibern in der Vergangenheit zeigen, dass es auch durch technische Schwierigkeiten zu Datenverlusten kommen kann.
- Diebstahl von Benutzerkonten oder Cloud-Diensten:
  Damit Anwender ihre Dienste schnell und einfach benutzen können, setzen viele Cloud-Anbieter auf einen simplen Anmeldeprozess. Gelingt es einem Angreifer, die Zugangsdaten eines Kundenkontos in Erfahrung zu bringen, kann er unter falschem Namen auf fremde Daten zugreifen, Ressourcen missbrauchen und Schaden anrichten.
- Unbekannte (neue) Risiken:
  Um die Risiken von Cloud-Services abzuschätzen, müssen Anwender die Sicherheitsvorkehrungen der Anbieter analysieren und in die eigene Betrachtung mit einbeziehen. Findet diese Risikoanalyse nicht oder nur unzureichend statt, etwa weil der Cloud-Betreiber nicht alle benötigten Informationen bereitstellt, bleibt ein nicht einschätzbares Risiko bestehen.

Neben diesen faktisch vorhandenen Risiken, denen man durch entsprechende Maßnahmen begegnen muss, bleiben weitere Risiken durch soziale und emotionale Widerstände, die oft auch durch gute Argumente nur schwer widerlegbar sind und wohl nur durch Vertrauen und Erfahrung überwunden werden können.

- Nicht mehr unmittelbaren Zugriff auf Daten und Technik
  Je nach Grad der Auslagerung können Server, Daten und Anwendungen durch den Cloudbetreiber zur Verfügung gestellt werden. Damit ist die bisher in Eigenregie betriebene Leitstellentechnik in Händen des Cloudbetreibers.
- Trennung der taktischen Nutzung des Systems von der betrieblich-technischen Umsetzung in verschiedene Organisationseinheiten, d.h. diese Schnittstelle muss ausreichend definiert sein.
- Abhängigkeit vom Cloudbetreiber
  Durch die Auslagerung wird Knowhow im eigenen Betrieb abgebaut. Die Abhängigkeit vom Cloudbetreiber wird sehr groß. Eine Umkehrung des Auslagerungsprozesses ist schwierig.
- Kontrollverlust
  Da der unmittelbare Zugriff auf die Cloud-Dienste nicht gegeben ist, ist eine unmittelbare Kontrolle der Cloud nicht möglich. Der Leitstellenbetreiber ist darauf angewiesen, dass seine Anforderungen durch den Cloud-Betreiber wirklich umgesetzt werden. Es können jedoch regelmäßige Berichte des Cloudbetreibers über Speicherorte von Daten oder SLA-Kennzahlen gefordert werden, die ein Controlling der Cloud erlauben.

- Misstrauen gegenüber dem Cloud-Betreiber
  Da Leitstellenbetreiber bisher keine Erfahrungen mit Cloud-Diensten haben, besteht wahrscheinlich ein grundlegendes Misstrauen gegen den Cloud-Betreiber, das nur durch strikte Vereinbarungen, Controllingmaßnahmen und Erfahrungen abgebaut werden kann.
- Verlust von Arbeitsbereichen
  Durch die Auslagerungen von Technik und Dienstleistungen sind beim Leitstellenbetreiber für den Betrieb verantwortliche Arbeitsbereiche nicht mehr in dem zuvor erforderlichen Maße vorzuhalten.

6.2 Risiken der Übertragungswege

Für die Nutzung der Cloudlösung ist immer ein Übertragungsweg notwendig. Dabei ist die Integrität, die Sicherheit und die Verfügbarkeit der Daten in jedem Falle sicherzustellen.

Ohne eine funktionierende Verbindung zur Cloud sind sowohl Daten als auch Funktionen nicht verfügbar. Dieser Übertragungsweg ist natürlich gegen Angriffe (man in the middle attack) und Ausfall zu sichern.

Angriffe werden mit entsprechend sicherer Verschlüsselung abgewehrt. Die benötigte Verfügbarkeit ist mit einer Mehrwege- und Mehrmedienführung zu erreichen.

6.3 Risiken der Energieversorgung

Risiken, die durch den möglichen Ausfall der Energieversorgung entstehen, sind für alle beteiligte Systeme zu betrachten. Hier gilt wieder der die Weisheit, dass die Kette nur so stark ist, wie das schwächste Glied.

Der Fall eines flächendeckenden Stromausfalls muss bei der Auswahl der Übertragungswege und -verfahren berücksichtigt werden. Während die Leitstellen selbst mit autarker Energieversorgung für einen begrenzten Zeitraum gegen Stromausfall gesichert werden, ist die Energieversorgung für die Übertragungswege, die häufig angemietet werden, vom Anbieter der Übertragungswege für den gleichen Zeitraum sicherzustellen. Der Cloudbetreiber muss bei Stromausfall ebenfalls für diesen Zeitraum die Dienstebereitstellung bieten.

Die Problematik der Energieversorgung kann auch nicht isoliert von den übrigen Systemen (z.B. Notruf, öffentliches und privates Telefon, Digitalfunk) betrachtet werden.

7 Schritte zur Cloudlösung

Vor der Nutzung einer Cloudlösung stehen verschiedene Schritte, die der Cloud-Nutzer in spe gehen muss, um für seine Ansprüche die richtige Lösung und den richtigen Partner für den Start zu finden.

Die wichtigsten Schritte, die bei der Errichtung einer Cloudlösung zu gehen sind, sind nachstehend aufgeführt:

- Festlegung der Sicherheitseinstufung und Compliance-Anforderungen
- Definition des Service- und Liefermodells
- Definition der Anforderungen an die Cloud, die Cloud-Infrastruktur und den Cloud-Betreiber
- Definition der Vergabebedingungen
- Fertigung der Vergabeunterlagen

- Nachweisliche Prüfung der Erfüllung der Anforderungen
- Migrationskonzept zur Verlagerung der Daten und Anwendung

Diese Schritte sind schwierig durch den Leitstellenbetreiber selbst durchzuführen. Externe Hilfe ist hier angeraten.

7.1 Anforderungen an die Cloud

Der Leitstellenbetreiber muss für die Auswahl der Cloudlösung das für seine Ansprüche angemessene Service-Modell und das passende Liefermodell wählen. Darüber hinaus ist der Grad der Verlagerung von Aufgabenstellungen in die Cloud oder an den Cloudbetreiber festzulegen. Dabei ist zu beachten, dass eine anfangs vielleicht geringe Auslagerungskapazität im Laufe der Vertragslaufzeit mit wachsendem Vertrauen in die Lösung sukzessive gesteigert werden kann.

Bei Cloud-Diensten für Leitstellen kann man fest von einer Private- oder Hybrid-Cloud ausgehen. Lediglich die Services werden unterschiedlich sein.

Der zu spannende Bogen der Dienste geht von einer reinen Datenhaltung beim Cloudbetreiber bis hin zur Lieferung der Endgeräte beim Leitstellenbetreiber.

Darüber hinaus ist auch die Verknüpfung verschiedener Cloud-Betreiber zu bedenken, die klare Kompetenz-, Verantwortungs- und Dienstleistungsabgrenzung erfordert. Die Definition dieser Abgrenzungen erfordert ein hohes Maß an gesamtsystemischen Kenntnissen.

Die Anforderungen an Dienstleistung, Sicherheit und Datenschutz der Cloud-Dienste und -Infrastruktur des Cloud-Betreibers sind klar zu definieren. Hierzu ist allerdings umfangreiches Wissen über die komplexen Risiken, Möglichkeiten und Chancen der Cloud-Dienste erforderlich.

7.2 Anforderungen an den Cloud-Betreiber

Ein Cloud-Betreiber muss seine Dienste auf der Basis der zertifizierten Sicherheit gemäß DSGVO liefern. Auch bei landeseigenen Betreibern muss dieser Grundsatz gelten.

Der Cloud-Betreiber muss eine solide Sicherheitsarchitektur und eine Mandatentrennung vorweisen. Die Mandatentrennung sollte auf allen Infrastrukturebenen (Virtualisierung, Plattform, Anwendung und Daten) sichergestellt sein.

Der Technische Betrieb sollte seine Prozesse an ITIL ausrichten. Er muss ein zertifiziertes Notfallmanagement vorweisen.

In Abhängigkeit von den vom Cloud-Betreiber abgeforderten Diensten sind die Anforderungen an den Cloud-Betreiber unterschiedlich.

Grundsätzlich gilt: Die Server der Cloud müssen in Europa, bevorzugt in Deutschland stehen. Ein Standort im nichteuropäischen Ausland bedarf einer besonderen Prüfung der jeweiligen Landesdatenschutzgesetze. Ein Standort in den USA ist auszuschließen, da alle dort gespeicherten Daten gemäß dem dort geltenden „Patriot Act“ der US-amerikanischen Regierung vorgelegt werden müssen, was mit dem in Europa geltenden Datenschutz nicht vereinbart werden kann.

Die Ausgestaltung der Infrastruktur eines Cloud-Betreibers sollte aufgrund der hohen Sicherheitsanforderungen den Anforderungen der EN 50518, die zwar für Alarmempfangszentralen gilt, entsprechen.

7.3 Vergabe von Cloud-Dienstleistungen

Die Vergabe von Cloud-Dienstleistungen ist derzeit noch Neuland im Bereich der BOS. Daher sind die Rahmenbedingungen, die Inhalte der unmittelbar zu beziehenden Leistungen, die SLA und die Wartungsverträge an die neuen Bedingungen anzupassen und ggf. neu zu definieren.

Damit dies umfassend und möglichst vollständig im Sinne der Sicherheit des Leitstellenbetreibers erfolgt, ist meist externe Expertise notwendig.

7.4 Migrationsplan zur Verlagerung der Anwendungen und Daten

Sind die Entscheidungen zum Aufbau und Nutzung einer Cloudlösung getroffen, ist ein dezidierter Migrationsplan zur Verlagerung der Dienste und Daten erforderlich.

Entscheidend ist dabei, dass die Datenbasis während der Migration ihre Aktualität beibehält und bei der Verlagerung keine Verluste entstehen.

Dies ist eine große Herausforderung, da die Leitstellen stets ein großes Volumen an Bestands- und Einsatzdaten vorhalten, die in das Datenmodell der Cloud eingepasst werden müssen.

8 Fazit

Der Einsatz einer Cloud für polizeiliche und nichtpolizeiliche BOS ist eine Option, über die im Zuge der Suche nach wirtschaftlichen Lösungen des Leitstellenbetriebs nachgedacht werden muss. Sie steht neben den Optionen der Zusammenlegung von Leitstellen oder der Bildung von Leitstellenverbünden. Dabei kann der Leitstellenverbund ebenfalls durch eine Cloud dargestellt werden.

Die Cloud hat den Vorteil der gemeinsamen Vorhaltung von IT-Ressourcen, Anwendungssoftware und technischem Personal, was eine Cloudlösung überaus wirtschaftlich gestalten kann. Dabei werden verschiedene Leitstellenformen für polizeiliche und nichtpolizeiliche Leitstellenbetreiber

- einzelne Leitstellen
- Leitstellenverbund
- Leitstellen als Landeslösung

unterstützt.

Selbst bei einzelnen Leitstellen kann die Verlagerung in eine Cloud bei einem IT-Dienstleister sinnvoll sein, da durch die professionelle Betreuung der Hardware, der Anwendungssoftware und der Datenbank(en) die Betriebssicherheit der Leitstelle erheblich gesteigert werden kann. Präventive und korrektive Wartung wird kontinuierlich durch Fachpersonal durchgeführt, dessen Hauptaufgabe in der Betreuung von IT-Systemen liegt.

Der Druck der Zusammenlegung von Leitstellen wird durch die Cloudlösung gemindert, da bei Nutzung gemeinsamer IT-Ressourcen lediglich die Personal-Ressource örtlich vorgehalten werden muss.

Unter dem wirtschaftlichen Druck der öffentlichen Haushalte sollte die öffentliche Hand den seitens der Unternehmen und der Industrie bereits beschrittenen Weg der Nutzung von Cloud-Diensten auch für sich nutzen, um die Potentiale dieses Ansatzes auch für die eigenen Aufgabe zu erschließen.

Eine Umkehrung des Prozesses ist später möglich aber schwer, da organisatorische, personelle und infrastrukturelle Voraussetzungen durch den Leitstellenbetreiber vor Vollzug dieses (Rück)-Schrittes dargestellt werden müssen.

Für alle Schritte, die in Richtung der Nutzung einer Cloudlösung gehen, wird die externe Unterstützung von fachlich beschlagenen Dienstleistungsunternehmen angeraten, da dieser Schritt langfristig angelegt ist und die komplexen Abhängigkeiten in allen Verästelungen möglichst bis zum Ende durchdacht werden muss. Dafür stehen die an diesem White Paper beteiligten Firmen gerne zur Verfügung.

Ansprechpartner:

Dipl.-Ing. Bernd Appel, +49 7222 83812, Bernd.Appel@accellonet.com

Quellen:

Dokumente von Cloud Computing Insider (Vogel Business Media)

https://www.cloudcomputing-insider.de/

Dokumente von Security Insider (Vogel Business Media)

https://www.security-insider.de/

Cloud Monitor 2018 (KPMG, bitkom)

https://www.bitkom.org/Presse/Anhaenge-an-PIs/2018/180607-Bitkom-KPMG-PK-Cloud-Monitor-2.pdf