

Aus der Cloud

Vorteile und Chancen durch die Auslagerung von BOS-Leitstellen

Gerhard Schulz

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. 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. Leitstellen aus der Cloud stellen hierfür einen möglichen Weg dar.

Zur Vertiefung des Themas haben die Firmen GS-Projektberatung, Accellonet, STF-Group und TÜV Nord IT ein ausführliches Whitepaper erstellt, das eine Befassung mit dem Thema unterstützen soll. Es kann bei bernd.appel@accellonet.com abgerufen werden.

Gerhard Schulz ist als freiberuflicher Senior Consultant tätig und wurde bei der Erstellung des Whitepaper durch die Firmen Accellonet, STF und TÜV Nord-IT unterstützt

Die föderale Struktur der Bundesrepublik Deutschland weist 16 Bundesländer, 294 Landkreise, 107 kreisfreie Städte und 11.054 Gemeinden auf. Die polizeilichen BOS sind länder- und bundesorientiert, die nichtpolizeilichen BOS kommunal, d.h. kreis- und gemeindebezogen organisiert.

Nach einer Erhebung des Autors aus dem Jahr 2017 gibt es 122 polizeiliche, 233 nichtpolizeiliche und 130 Leitstellen der Institutionen des Bundes, wobei die Zahl der Leitstellen sich ständig ändert, z.B. durch Gebietsreformen oder das Zusammenlegen von Leitstellen mehrerer Kreise. Letzteres kann zum einen durch eine Technik-, zum anderen durch eine Dienstleistungskonzentration erfolgen.

Unabhängig von der Zusammenlegung von Leitstellen bleibt eine mögliche Technikkonzentration, die sowohl für eine dislozierte als auch für eine konzentrierte Leitstellenlandschaft angewandt werden kann. Durch immer weiter fortschreitende Digitalisierung und den qualitativ und quantitativ immer besseren Ausbau der Infrastruktur ist der sichere Transport von Daten über größere Entfernungen heute kein Problem mehr.

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 hybriden Clouds ausgelagert. Grund für die Auslagerung sind die enormen Aufwände, die jedes Unternehmen für sich aufbringen müsste, um die Sicherheit und die Verfügbarkeit der sensiblen Datenhaltung zu gewährleisten.

Cloud – was ist das?

Mit Cloud wird gemeinhin ein Ort für die elektronische Datenhaltung und

-verarbeitung bezeichnet, der irgendwo liegen kann. Charakteristisch für eine Cloud ist die dynamisch anpassbare, flexible Rechen- und Datenkapazität. Cloud-Lösungen werden nach der Nutzung (Servicemodell) und dem Zugang (Liefermodell) unterschieden. Die Servicemodelle funktionieren i.d.R. nach dem As-a-Service-Prinzip. Bei Infrastructure as a Service (IaaS) bietet der Cloud-Betreiber lediglich den Nutzungszugang zu Rechnern, Speichern und sonstigen Hardwareressourcen. Im Plattform-as-a-Service-Modell (PaaS) erhält der Kunde Zugang zu Laufzeit- und Programmierumgebungen. Der Leitstellenbetreiber kann seine eigenen Softwareanwendungen entwickeln und ausführen. Bei Software as a Service (SaaS) werden vollständige Anwendungen durch den Cloud-Betreiber angeboten.

Bei den Liefermodellen unterscheidet man die Public, die Private, die Hybrid und die Community Cloud. In einer Public Cloud bietet der Cloud-Betreiber öffentliche IT-Infrastrukturen an, die nach der tatsächlichen Nutzung abgerechnet werden. In der Private Cloud hat lediglich ein fest umrissener Nutzerkreis Zugang zur darin befindlichen IT-Infrastruktur. Die Hybrid Cloud kombiniert beide vorgenannten Liefermodelle und bietet so die Sicherheit einer privaten Cloud für sicherheitsrelevante Anwendungen und Daten und die Möglichkeit, öffentliche IT-Services zu nutzen. Eine Community Cloud bietet ihre Dienste einem örtlich verteilten Nutzerkreis an.

Je nach Liefermodell sind verschiedene Anbieter vorhanden bzw. möglich. Die Public Cloud wird von diversen Betreibern angeboten (z.B. Microsoft, Dropbox usw.). Private und Hybrid Clouds werden meist als firmenweite, auch landesweite oder globale, gemeinsame Daten- und Anwendungsplattformen genutzt, die sowohl IaaS, PaaS und SaaS bieten.

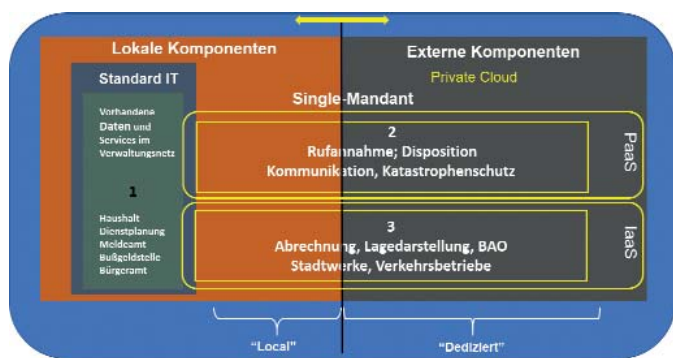


Bild 1: Private-Cloud-Lösungen

Exemplarische Cloud-Lösungen

Reine private Cloud-Lösungen bieten in sich geschlossene Systeme (Bild 1). Übergänge bzw. Kopplungen mit anderen Systemen müssen sehr genau geplant und bedacht werden.

Wird hingegen eine hybride 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 (Bilder 2 und 3). Je nach Vertrauen, das der Leitstellenbetreiber dem Cloud-Betreiber entgegenbringt, werden sich die Anteile der Daten- und Anwendungshaltung unterschiedlich verteilen.

Der Cloud-Betreiber hat für die Sicherheit am Übergang zwischen Private und Public Cloud zu sorgen. 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.

Vorteile einer Cloud-Lösung

Für die *Dienstbereitstellung* aus einer Cloud sind folgende Aspekte zu be-

achten, die durch den Cloud-Betreiber dargestellt werden müssen:

- sichere Übergänge zur Außenwelt (Internetzugänge, andere Datenbanken, Updates, Grafikdaten);
- Bereitstellung gemeinsamer Dienste;
- gemeinsame mandantentrennte oder getrennte Datenbanken in einer großen Datenbanklösung;

gemeinsame Verfügbarkeit der Anwendungen;

- mögliche Diensteübernahme durch andere Leitstelle;
- Landeslösungen einfach möglich.

Die *Infrastruktur* ist bei der Einrichtung eines Rechenzentrums von herausragender Bedeutung, da sie sowohl einen gesicherten technischen Betrieb als auch die Sicherheit der verarbeiteten Daten durch die dort beheimateten IT-Einrichtungen gewährleistet. Alle Komponenten sind in sicherer und gesicherter Form gemäß BSI-Grundschutz einzurichten.

Die erforderliche Ausführung bedingt erhebliche Investitionen und Betriebskosten. Die EN 50518 stellt erhebliche Anforderungen an die Infrastruktur für Alarmempfangszentralen, an die sich auch Leitstellen anlehnen können.

Ein zentralisierter *Betrieb* der Server, der Netzkomponenten sowie die Betreuung der Datenbanken wird durch spezialisiertes, gut ausgebildetes Personal, das die Einrichtungen ständig überwacht und an ihr arbeitet, erheblich effizienter und sicherer.

Die Einrichtungen der Cloud werden kontinuierlich durch den Cloud-Betreiber auf dem aktuellen Stand gehalten. Für die Erneuerung der Hardware sind somit für den einzelnen Leitstellenbetreiber keine wellenartigen *Reinvestitionen* nötig, sondern die Bedarfe werden auf die Leitstellenbetreiber verteilt und kontinuierlich finanziert.

Für eine hohe *Verfügbarkeit* müssen Rechenzentren, die Cloud-Optionen anbieten, per se redundant ausgelegt

sein, da sie sonst ihre Service Level nicht einhalten können. Die Redundanz kann unterschiedlich ausgestaltet sein – von einer Standortredundanz bis zu einer Redundanz in verschiedenen Brandabschnitten. Durch die Virtualisierung der Server ist eine schnelle Ersatzgestellung möglich, so dass Ausfallzeiten auf ein Minimum reduziert werden können.

Die *Datensicherheit* wird beschrieben als die Menge der Maßnahmen zum Schutz des Anwenders in Hinblick auf die Funktionsfähigkeit von DV-Systemen und insbesondere zum Schutz vor Verfälschung und Verlust von Daten und vor unberechtigten Zugriffen auf Daten. Durch die hohe Kompetenz, die ein Cloud-Betreiber besitzen muss, ist die hohe Datensicherheit und der professionelle Umgang mit der Verantwortung sicherzustellen.

Die Nutzung einer Cloud-Lösung entbindet den Leitstellenbetreiber nicht von seiner grundsätzlichen Verpflichtung zum *Datenschutz* gemäß der DSGVO. Für die gespeicherten und verarbeiteten Daten ist auch bei einer Cloud-Lösung immer der Leitstellenbetreiber verantwortlich. Vom Cloud-Betreiber sollte sich der Leitstellenbetreiber mit anerkannten Zertifikaten eine Teilbescheinigung für dessen Zuständigkeitsbereich geben lassen.

Durch die Bereitstellung von Infrastruktur, Hard- und Software, gepaart mit zugehöriger 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 Service Level Agreements (SLAs) wirtschaftlich einzuhalten.

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

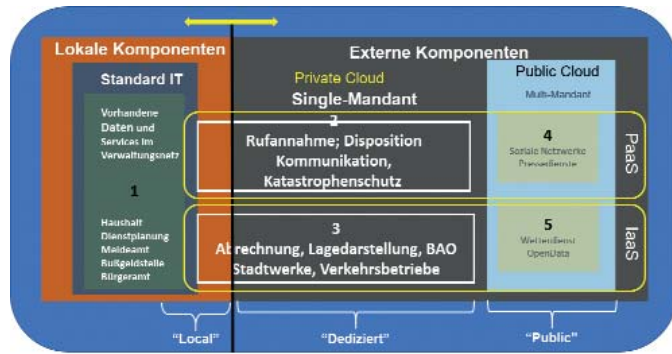


Bild 2: Hybrid Cloud mit hohem Nutzeranteil

Bei der Vergabe von Cloud-Dienstleistungen sind neue, bisher noch nicht bei Leitstellenausschreibungen beschriebene Leistungen und Bedingungen zu fordern, die im Detail erarbeitet werden müssen.

Risiken einer Cloud-Lösung

Die Nutzung einer Cloud-Lösung birgt natürlich auch Risiken, die bei einer Nutzung der Cloud-Dienste weitgehend ausgeschlossen werden müssen. Wie bei jeder Risikobetrachtung sind auch hier entsprechende Maßnahmen vorzuhalten, die das Risiko auf ein verantwortbares Maß reduzieren.

Zu den Risiken der Cloud zählen:

- Missbrauch und schädliche Nutzung von Cloud Computing;
- unsichere Schnittstellen und APIs;
- böswillige Insider;
- Risiken durch geteilte Techniken;
- Datenverlust und -kompromittierung;
- unbekannte (neue) Risiken.

Daneben bleiben weitere Risiken durch soziale und emotionale Widerstände, die oft auch durch gute Argumente nur schwer widerlegbar sind und häufig nur durch Vertrauen und Erfahrung überwunden werden können:

- kein unmittelbarer Zugriff auf Daten und Technik;
- Abhängigkeit vom Cloud-Betreiber;
- Kontrollverlust;
- Misstrauen gegenüber dem Cloud-Betreiber;
- Verlust von Arbeitsbereichen.

Für die Nutzung der Cloud-Lösung ist immer ein Übertragungsweg notwendig. Dabei sind die Integrität, die Sicherheit und die Verfügbarkeit der Daten in jedem Falle sicherzustellen. Risiken, die durch den möglichen Ausfall der Energieversorgung entstehen,

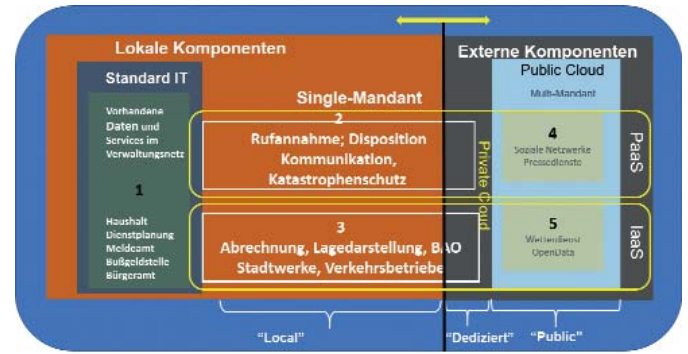


Bild 3: Hybrid Cloud mit hohem Betreiberanteil

sind für alle beteiligte Systeme zu betrachten. Hier gilt die Weisheit, dass die Kette nur so stark ist wie das schwächste Glied. Die Problematik der Energieversorgung darf auch nicht isoliert von den übrigen Systemen (Notruf, öffentliches und privates Telefon, Digitalfunk ...) betrachtet werden.

Chancen durch Cloud-Nutzung

Eine zentralisierte IT-Infrastruktur ergibt einfachere Möglichkeiten der Aktualisierung der Hard- und Software und damit für eine Zukunftssicherheit. Infolge dessen sind auch zukünftige, auf die Leitstellenbetreiber zukommende Aufgabenstellungen oder Veränderungen der externen Schnittstellen einfacher, weil einmalig, darzustellen.

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

Durch die Nutzung der Cloud-Dienste erhöht sich die Sicherheit, da die zentrale Überwachung durch kompetente, speziell für die Datensicherheit und den Datenschutz geschulte Mitarbeiter wahrgenommen wird. Gleichzeitig entstehen durch die Nutzung der Cloud-Infrastruktur durch verschiedene Nutzer/Organisationen/Leitstellen zusätzliche Aufwendungen. Auch die infrastrukturellen und prozessualen Sicherheitsvorkehrungen sind an zentraler Stelle leichter zu treffen und zu überwachen.

Die zentrale Vorhaltung von Leitstellentechnik kann die absolute Verfügbarkeit erheblich steigern. Mit der Vorhaltung von IT-Ressourcen entweder in Redundanzsystemen oder frei

verfügbaren Ressourcen können neben den ungeplanten Nichtverfügbarkeiten, die normalerweise nur in die Verfügbarkeitsberechnung eingehen, auch die geplanten Nichtverfügbarkeiten erheblich reduziert werden.

Ein zentraler technischer Betrieb steigert seine Effizienz mit wachsender Zahl der zu betreuenden Ressourcen. Die Möglichkeit einer steigenden Spezialisierung des Wartungspersonals erhöht die Kompetenz und damit die Dienstleistung des technischen Betreibers.

Der zentrale Betrieb ist durch die von möglichst vielen Leitstellenbetreibern in Anspruch genommenen Ressourcen und Betriebspersonal sehr wirtschaftlich. Die Steigerung von Nutzerzahlen wirkt sich positiv, also senkend, auf die Kosten je Leitstellenbetreiber und damit auf die Wirtschaftlichkeit aus.

Schritte zur Cloud-Lösung

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

- 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.

Für die Durchführung dieser Schritte wird dem Leitstellenbetreiber emp-

Fortsetzung auf Seite 19

Fortsetzung von Seite 16

fohlen, externe Hilfe in Anspruch zu nehmen.

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 Leitstellenverbänden.

Unter dem wirtschaftlichen Druck der 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 Potenziale dieses Ansatzes auch für die eigenen Aufgaben zu erschließen.

Die Cloud hat den Vorteil der gemeinsamen Vorhaltung von IT-Ressourcen, Anwendungssoftware und technischem Personal, was eine Cloud-Lösung überaus wirtschaftlich gestalten kann. 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. Durch die in der Cloud dargestellte Mandantentrennung, ggf. durch nebeneinander

aufgesetzte getrennte Systeme oder Datenbanken, sind die genannten Betriebsformen nebeneinander oder in Kombination darstellbar.

Für alle Schritte, die in Richtung der Nutzung einer Cloud-Lösung gehen, wird die externe Unterstützung von fachlich beschlagenen Beratungsunternehmen angeraten, da dieser Prozess langfristig angelegt ist und die komplexen Abhängigkeiten in allen Verästelungen möglichst bis zum Ende durchdacht werden müssen. Eine Umkehrung des Prozesses ist möglich, aber schwer, da organisatorische, personelle und infrastrukturelle Voraussetzungen durch den Leitstellenbetreiber vor Vollzug dieses (Rück-)Schrittes dargestellt werden müssen. (bk)