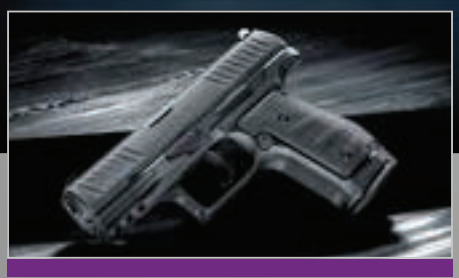
Im Einsatz – im Thema.

Schutzgebühr: 7,50 €

POLIZEI PRAXIS

2020/1

BOS-Leitstellen aus der Cloud?



Walther Q4

Steelframe – aus dem Vollen gefräßt

Tactilon Agnet

Für eine bedienerfreundliche Kommunikation

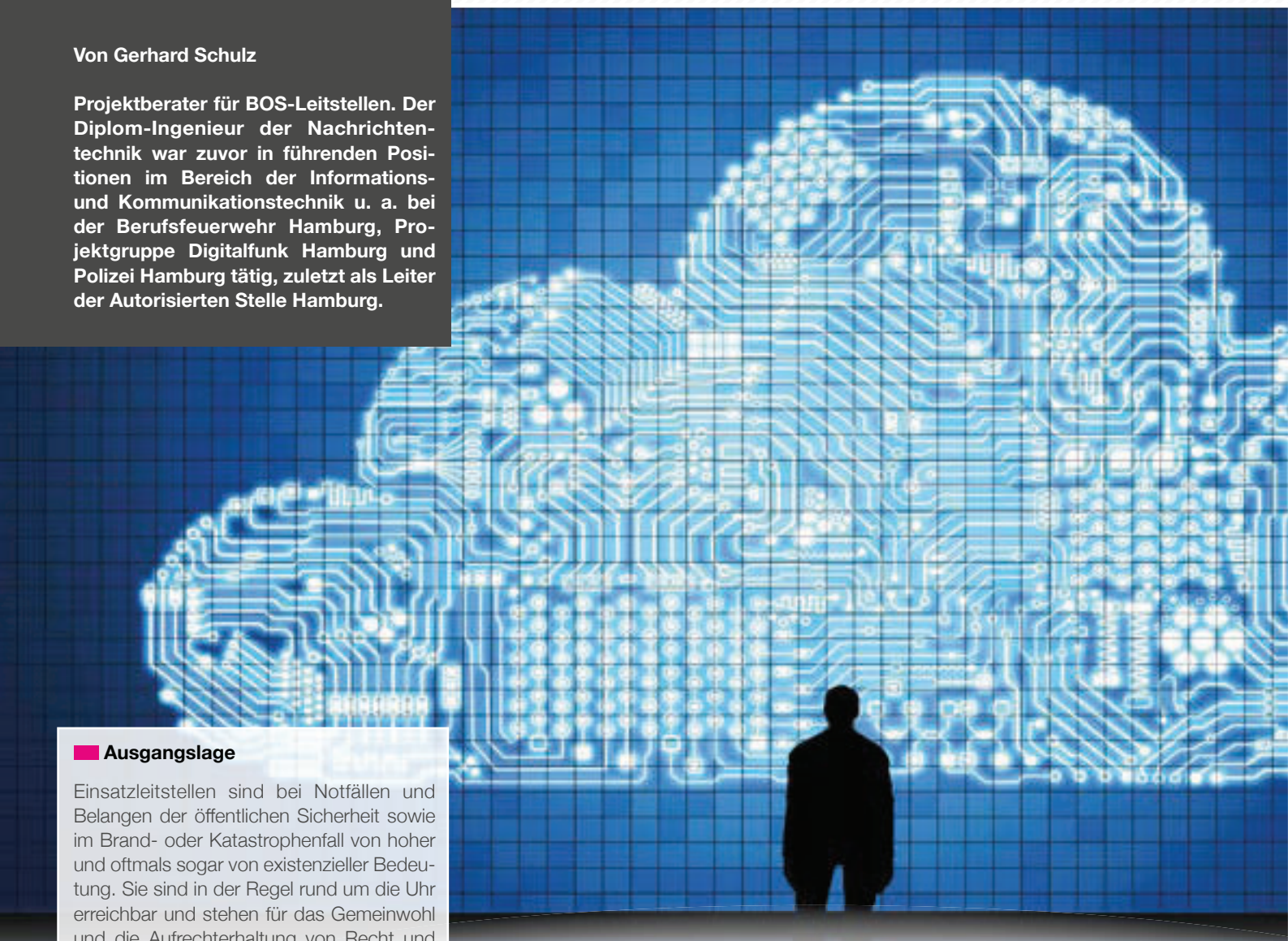
Gewerkschaft der Polizei

BOS-Leitstellen Model

KOMMUNIKATION

Von Gerhard Schulz

Projektberater für BOS-Leitstellen. Der Diplom-Ingenieur der Nachrichtentechnik war zuvor in führenden Positionen im Bereich der Informations- und Kommunikationstechnik u. a. bei der Berufsfeuerwehr Hamburg, Projektgruppe Digitalfunk Hamburg und Polizei Hamburg tätig, zuletzt als Leiter der Autorisierten Stelle Hamburg.



Ausgangslage

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 und stehen für das Gemeinwohl und die Aufrechterhaltung von Recht und Sicherheit.

Nach einer Erhebung des Autors aus dem Jahre 2017 gibt es in Deutschland

- 122 polizeiliche Leitstellen
- 233 nichtpolizeiliche Leitstellen
- 130 Leitstellen der Institutionen des Bundes

Gebietsreformen oder Zusammenlegungen von Leitstellen mehrerer Kreise führen aber aus Gründen der Wirtschaftlichkeit des Betriebes zu einer Reduktion der Anzahl der Leitstellen.

Problemstellung

Die Aufgaben und Funktionen von Leitstellen werden durch die polizeilichen und nichtpolizeilichen Behörden mit Sicherheitsaufgaben (BOS) wahrgenommen. Aufgrund des technologisch-gesellschaftlichen Wandels sowie Veränderungen der Leitstellenumgebung, der Aufgabenstellungen und Abläufe kommen neue Anforderungen auf diese Behörden zu. Die BOS stehen dabei vor der schwierigen Aufgabe, die hohen Ansprüche der Bürger an die Hilfeleistung zu erfüllen. Dazu sind räumliche, technische und personelle Ressourcen erforderlich. Ständig wandelnde Anforderungen müssen unter einem ständig wachsenden wirtschaftlichen Druck bewältigt werden.

Die heutige Vielzahl der Leitstellen kann in Zukunft nicht mehr wirtschaftlich betrieben werden. Auch die Anforderungen an das technische Personal steigen infolge der ständig wachsenden Komplexität der technischen Ausstattung immens an. Sie können in der erforderlichen Quantität und Qualität nicht mehr erfüllt werden. Weiterhin stellt die Ausweitung der Datenschutzgesetzgebung eine hohe personelle und intellektuelle Herausforderung dar. Gleichzeitig erwarten die Bürger aber zu Recht sicher funktionierende Behörden und Organisationen mit Sicherheitsaufgaben. Dieser Anspruch kann durch intelligent sparende organisatorische und technische Lösungen in den Leitstellen erfüllt werden.

aus der Cloud:
der Zukunft oder Risiko?

Bild: phonlamaiphoto, Adobe Stock

Organisatorische Maßnahmen

Eine organisatorische Maßnahme ist die Zusammenlegung der Leitstellen von zwei oder mehreren Landkreisen (Leitstellengebiete) zu einer Leitstelle Diese Maßnahme erfordert vertragliche Regelungen der beteiligten Landkreise zu den rechtlichen, personellen und finanziellen Aspekten der Zusammenlegung. Auch BOS-übergreifende Leitstellen („bunte“ Leitstellen) bieten wirtschaftliche Vorteile: Die Leitstellen werden nur einmal eingerichtet, die technischen Einrichtungen sind nur einmal vorhanden, das operative Personal ist optimiert.

Technische Maßnahmen

Die Sicherstellung der Aufgabenwahrnehmung der Leitstellen kann aber auch durch technische Maßnahmen erheblich unterstützt werden. So ist durch ein Zusammenschalten mehrerer Leitstellen die Übernahme von Diensten einer einzelnen Leitstelle im Überlast- oder Havariefall möglich Die technische Ausstattung der einzelnen Leitstellen des Verbundes gleicht der von diskret aufgebauten Leitstellen, die ausschließlich für den eigenen Bereich arbeiten. Somit ist neben der technischen Ausstattung auch der Anspruch an die Wartung in jeder Leitstelle des Verbundes mit der einer diskreten Leitstelle vergleichbar. Die Komplexität steigert sich gegenüber den diskreten Leitstellen erst durch die Zusammenschaltung des Verbundes.

Unabhängig von der Zusammenlegung von Leitstellen bleibt die Möglichkeit einer Technikkonzentration, die sowohl für eine dislozierte als auch für eine konzentrierte Leitstellenlandschaft in Betracht kommt. Infolge der weiter fortschreitenden Digitalisierung und dem qualitativen und quantitativen Ausbau der Netzinfrastruktur ist der sichere Transport von Daten über größere Entfernungen heute kein Problem mehr. Eine Konzentration der Daten bietet sich somit an. In der „Nicht-BOS-Welt“ hat sie sich durchgesetzt: Die deutsche Wirtschaft setzt bereits heute sehr stark auf zentralisierte Datenhaltung im eigenen Bereich – aber auch ausgelagert bei Dienstleistern. Der von der Wirtschaftsberatungsgesellschaft KPMG erstellte Cloud-Monitor 2018 stellt fest, dass 2018 bereits 66 Prozent der Unternehmen in Deutschland auf Cloud-Computing setzen. Der Grund für die Auslagerung liegt im enormen Aufwand, den jedes Unternehmen für sich leisten müsste, um die Sicherheit und die Verfügbarkeit der sensiblen Daten zu gewährleisten.

Lösungsansatz Cloud

Als 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. Die Cloudlösungen werden nach der Nutzung (Service-Modell) und dem Zugang (Liefer-Modell) unterschieden.

Servicemodelle

Infrastructure-as-a-Service (IaaS)
Der Cloud-Betreiber bietet lediglich den Nutzungszugang zu Rechnern, Speichern und sonstigen Hardware-Ressourcen.

Platform-as-a-Service (PaaS)
Der Cloud-Betreiber bietet den Zugang zu Laufzeit- und Programmierumgebungen. Der Leitstellenbetreiber kann seine eigenen Software-Anwendungen entwickeln und ausführen.

Software-as-a-Service (SaaS)
Der Cloud-Betreiber bietet vollständig Anwendungen an.

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.

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.

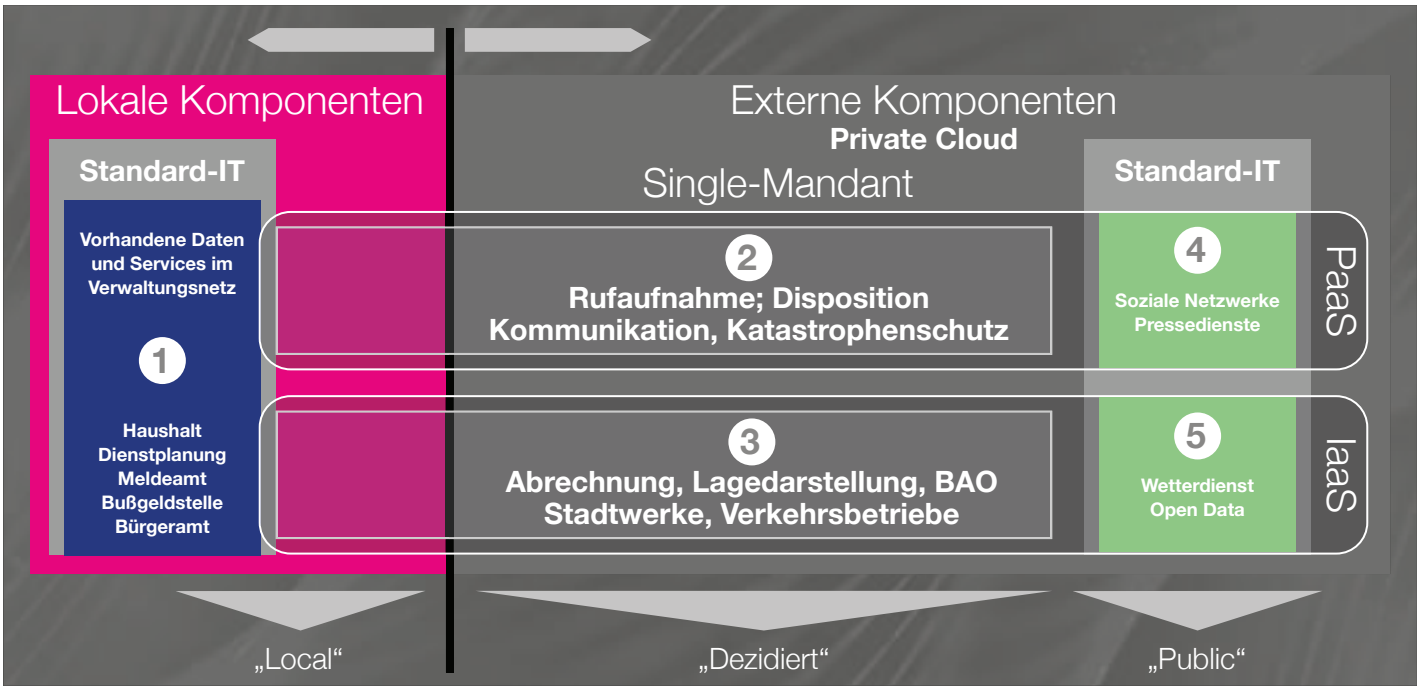
Community Cloud
Die Community Cloud bietet ihre Dienste einem örtlich verteilten Nutzerkreis an.

Cloud-Betreiber

Je nach Liefermodell sind verschiedene Anbieter vorhanden bzw. möglich. Die Public Cloud wird von verschiedenen Betreibern angeboten (z.B. Microsoft, Dropbox uva.) Private Clouds und Hybrid Clouds werden meist als firmenweite, auch landesweite oder globale gemeinsame Daten- und Anwendungsplattformen genutzt, die sowohl IaaS, PaaS und SaaS liefern. Der Cloud-Betreiber übernimmt ein sehr hohes Maß an Verantwortung für das bereitgestellte Service-Modell. Der Nutzer muss ein hohes Vertrauen in den Cloud-Betreiber haben, da dieser seine sensiblen Daten hält und die Verfügbarkeit darstellen muss.

Cloudlösungen für Leitstellen

Für BOS-Leitstellen kommen aufgrund der Sensibilität der verarbeiteten Daten als Liefermodelle nur eine Private oder eine Hybrid Cloud in Frage. Die Service-Modelle sind in diesen Liefermodellen realisierbar.



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

Die Anteile der Private- oder der Hybrid-Cloud, die von einem 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, verteilen sich die Anteile der Daten- und Anwendungshaltung unterschiedlich. 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. In diesem Fall stellt der Cloud-Betreiber nicht nur die Infrastruktur und die Plattformen bereit, sondern er richtet auch die darauf aufsetzenden Tools und Anwendungen ein und betreut diese. 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. Der Leitstellenbetreiber bezieht die Leitstellenfunktionalitäten „nur“ noch als eine Dienstleistung.

Vor- und Nachteile der Lösungsansätze

Bei der Betrachtung der Vor- und Nachteile der verschiedenen Lösungsansätze werden nur die diskreten Leitstellen (inklusive Verbund-Leitstellen) und eine auf IaaS basierende Cloud-Lösung gegenübergestellt, da dies zum gegebenen Zeitpunkt den realistischen ersten Schritt in eine Cloud-Umgebung darstellt.

Kriterium	Zentrale Architektur Cloud-Leitstelle		Dezentrale Architektur Diskrete, Verbund-Leitstellen	
	+ 0 -	Begründung	+ 0 -	Begründung
Technische Leistungsfähigkeit	+	• Zentrale Strukturen bieten durch die Ressourcenverfügbarkeit an zentraler Stelle eine sehr hohe Leistungsfähigkeit.	-	• Dezentrale Strukturen bieten keine Ausgleichsmöglichkeiten an Ressourcen. • Leistungsfähigkeit ist auf den jeweiligen Ausbaugrad begrenzt.
Marktverfügbarkeit	-	• Nicht alle Systeme unterstützen Zentralarchitekturen.	+	• Vielzahl kleinere Systeme für dezentrale Architektur auf dem Markt verfügbar.
Raumbedarf	+	• Optimale Verdichtung der Ressourcen an zentraler Stelle. • In den dezentralen Räumlichkeiten vorhandene Infrastruktur weiter benutzen.	-	• Zusätzlicher Flächenbedarf für Technikaufbau erforderlich. • Ggf. zusätzliche Infrastruktur erforderlich.
Verfügbarkeit des Systems	+	• Durch zentral Ersatzteilbevorratung geringe „Time to Repair“. • Updates ohne Betriebsbeeinträchtigung möglich. • Durch zwei RBZ keine Ausfallszenarien mit hoher Auswirkung.	0	• Dezentrale Ersatzteilbevorratung wirtschaftlich nicht gangbar. • dezentrale Logistik notwendig. • Updates ohne vollständiges Redundanzsystem nur mit erheblichen Betriebsbeeinträchtigungen. • Ausfall ist maximal auf einen Standort beschränkt.
Redundanz	+	• Redundanzsysteme sind zentral beim Cloud-Betreiber vorzuhalten. • Gemeinsame Havarie-Leitstelle möglich.	-	• Redundanzsysteme müssen je dezentralem System gesondert vorgehalten werden. • Zusätzliche Raumbedarfe und Infrastrukturen an anderem Standort. • Gemeinsame Havarie-Leitstelle nicht möglich.
Sicherheit	+	• Hochsicherheitslösungen an einem Standort einfacher einzurichten und vorzuhalten.	-	• Hochsicherheitslösungen bedürfen an jedem Standort erhebliche technische und organisatorische Aufwendungen.
Betreibbarkeit	+	• 24/7-Betrieb ist realistisch. • Einheitliche Applikationen und Versionsstände vereinfachen den Betrieb und die Wartung. • Fachlich versiertes Betriebspersonal.	-	• 24/7-Betrieb ist nicht realistisch. • Voneinander abweichende, da auf den Standort angepasste, Applikationen.
Skalierbarkeit	+	• Systeme durch übergeordnete Ressourcenverwaltung jederzeit skalierbar. • Ressourcenreserven werden gemeinsam vorgehalten.	-	• Systeme nur mit erheblichem Aufwand (Erweiterungen) skalierbar.
Kosten für Investition/ Aufbau des Systems	+	• Gemeinsam genutzte Infrastruktur bedeutet günstigere Lösung. • Vereinfachte Planung und Realisierung.	-	• Infrastruktur muss an jedem Standort diskret aufgebaut werden. • Stark erhöhter Planungs- und Realisierungsaufwand.
Kosten für den Betrieb/ Erhalt des Systems	+	• Zentraler 24/7-Betrieb ist kostengünstig bereitzustellen. • Wartungsverträge gestalten sich einfacher und günstiger.	-	• Dezentraler 24/7-Betrieb unrealistisch; Eingriffszeiten zu lang. • Wartungsverträge für verschiedene Standorte aufwändig und teuer.

Risiken einer Cloudlösung

Die Nutzung einer Cloud-Lösung birgt natürlich auch verschiedene Risiken in sich. Nachstehend sind einige 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.

Risiken der Datensicherheit:
- Missbrauch und schädliche Nutzung von Cloud Computing
- Unsichere Schnittstellen und APIs
- Böswillige Insider
- Risiken durch geteilte Technologien
- Datenverlust und -kompromittierung
- Unbekannte (neue) Risiken

Risiken des emotionalen Widerstandes:
Auch weiche Faktoren spielen bei der Risikobetrachtung eine Rolle. So wird durch die abgesetzte Technik und Datenhaltung ein emotionaler Widerstand erzeugt, der nur durch positive Erfahrung abgebaut werden kann. Zu diesen Faktoren zählen:
- Nicht mehr unmittelbarer Zugriff auf Daten und Technik
- Abhängigkeit vom Cloud-Betreiber
- Gefühlter Kontrollverlust
- Misstrauen gegenüber dem Cloud-Betreiber
- Verlust von Arbeitsbereichen
- Angst um Arbeitsplatz

Risiken der Übertragungswege

Für die Nutzung der Cloud-Lösung ist ein hochverfügbarer Übertragungsweg existenziell notwendig. Dabei sind Integrität, Sicherheit und Verfügbarkeit der Daten in jedem Fall sicherzustellen. Ohne sichere und hochverfügbare Übertragungswege sollte der zentralisierte Ansatz nicht verfolgt werden.

Risiken der Energieversorgung

Risiken, die durch den möglichen Ausfall der Energieversorgung entstehen, sind für alle beteiligten Systeme (also auch die Übertragungswege) zu betrachten. Hier gilt wieder die Weisheit, dass die Kette nur so stark ist wie das schwächste Glied. Das Leitstellensystem mit all seinen Komponenten sollte nicht isoliert betrachtet werden. So sind bei einem flächendeckenden Energieausfall auch alle korrespondierenden Techniken (Notruf, öffentliches und privates Telefon, Digitalfunk etc.) betroffen.

Chancen durch Cloudnutzung

Technische Betrachtung

Der zentralisierte Ansatz vereinfacht die Vorhaltung von technischen Ressourcen sehr stark. Nutzen mehrere Leitstellen gemeinsam eine Cloud, so wird der wirtschaftliche Nutzen der technischen Einrichtungen der Cloud immer günstiger. Die schnelle Nutzung von Leistungs-Reserven ist einfach und wirtschaftlich möglich, da diese Reserven für alle Nutzer vorgehalten werden. Die kontinuierliche Erneuerung der technischen Einrichtungen liegt in der Verantwortung des Cloud-Betreibers. Er hat sie ohne Betriebsbeeinträchtigungen bereitzustellen.

Betriebliche Betrachtung

Ein zentraler Betrieb hält ein fachlich sehr gut ausgebildetes und „in ständigem Training“ befindliches Wartungspersonal vor. Durch die mehrfach vorhandene gleichartige Technik (z.B. Server, Virtualisierung, Datenbanken, Netzwerktechnik, Firewalls) ist die Vorhaltung von Spezialisten möglich, die durch präventive und korrektive Wartung die gefordert hohe Verfügbarkeit gewährleisten. Es sind ausgebildete Fachleute am Werk.

Betrachtung der Standardisierung

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

Betrachtung der Sicherheit

Die zentrale Überwachung und Anwendung der Maßnahmen zum Schutz der Daten und der Datensicherheit wird durch kompetente, speziell im Datenschutz geschulte Mitarbeiter wahrgenommen. Gleichzeitig entstehen durch die Nutzung der Cloud-Infrastruktur durch verschiedene Anwender/Organisationen/Leitstellen keine zusätzlichen Aufwendungen. Auch die infrastrukturellen und prozessualen Sicherheitsvorkehrungen sind an zentraler Stelle leichter zu treffen und zu überwachen.

Betrachtung der Verfügbarkeit

Die zentrale Vorhaltung von frei verfügbaren Ressourcen steigert die absolute Verfügbarkeit erheblich. Mit der Vorhaltung von IT-Ressourcen in Redundanzsystemen können neben den ungeplanten Nichtverfügbarkeiten, die normalerweise nur in die Verfügbarkeitsberechnung eingehen, auch die geplanten Nichtverfügbarkeiten (z.B. Wartungsarbeiten, Updates) erheblich reduziert werden.

Betrachtung der Wirtschaftlichkeit

Der zentrale Betrieb ist durch die von möglichst vielen Leitstellenbetreibern in Anspruch genommenen Ressourcen und Betriebspersonal sehr wirtschaftlich. Wartungsverträge sind bei konzentriert gehaltener Hardware erheblich günstiger. Aber auch die Softwarewartung wird erheblich günstiger, da der Wartungsgeber nur noch einen Standort betreuen muss.

Schritte zur Cloudlösung

Vor der Nutzung einer Cloud-Lösung stehen verschiedene Schritte, die der künftige Cloud-Nutzer 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 Cloud-Lösung zu gehen sind:
- Definition des Service- und Liefermodells
- Definition der Anforderungen an die Cloud, die Cloud-Infrastruktur und den Cloud-Betreiber
- Prüfung der infrastrukturellen Gegebenheiten (WAN-Verfügbarkeit)
- Definition der Vergabebedingungen
- Fertigung der Vergabeunterlagen
- Nachweisliche Prüfung der Erfüllung der Anforderungen
- Migrationskonzept zur Verlagerung der Daten und Anwendung

Da bisher nur wenige bis keine Erfahrungen zur Auslagerung einer Leitstelle in eine Cloud vorliegen, kann ein Leitstellenbetreiber diese wichtigen Schritte wahrscheinlich nur schwierig allein bestreiten. Externe Beratung wäre hier angeraten.

Fazit

Die Auslagerung von Leitstellentechnik bis hin zu -diensten wird aufgrund einer sich ständig verändernden Umgebung und der damit einhergehenden wachsenden Komplexität der technischen Lösungen notwendigerweise zunehmen. Insbesondere die wachsenden fachlichen und wirtschaftlichen Ansprüche werden die Treiber in diese Richtung sein. Aber auch die Leitstellenbetreiber haben ein originäres Interesse, ein überaus verlässlicher Dienstleister des Bürgers zu sein und drängen somit auf eine reaktionsschnelle, dem erforderlichen Leistungsniveau angepasste und leistungsfähige Systemlandschaft zur Verfügung zu haben.

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.

Für alle Schritte in Richtung Nutzung einer Cloud-Lösung ist eine externe Unterstützung von fachlich versierten Beratungsunternehmen angeraten. Denn die Nutzung einer Cloud-Lösung ist ein langfristig angelegtes Projekt. Und die komplexen Abhängigkeiten in allen Verästelungen müssen bis zum Ende durchdacht werden. Eine Umkehrung des Prozesses ist zwar möglich, aber schwer, da organisatorische, personelle und infrastrukturelle Voraussetzungen durch den Leitstellenbetreiber vor Vollzug dieses (Rück)-Schrittes dargestellt werden müssen.

White-Paper

Zur Vertiefung des Themas haben die Firmen GS-Projektunterstützung, accellonet, STF-Gruppe und TÜV Nord IT ein White Paper erstellt. Das White Paper ist über die beteiligten Firmen

- GS-Projektunterstützung (gerhard-schulz@kabelmail.de) und
- Accellonet (bernd.appel@accellonet.com) erhältlich.

Quellen:
KPMG Cloud-Monitor 2018
Dokumente von CloudComputing Insider (Vogel Business Media)
Dokumente von Security Insider (Vogel Business Media)

Bild: Pixaline, Pixabay