13. GDI-FORUM NORDRHEIN-WESTFALEN 2022 - „SOUVERÄN IN DIE CLOUD“ **BERLINER (LIEGENSCHAFTS-) KATASTER IN DER CLOUD**

Anette Blaser
Senatsverwaltung für Stadtentwicklung, Bauen und Wohnen
Abt. III - Geoinformation

BERLIN

Was ist eine Cloud?

- Amazon, Google, One drive, Freenet und viele mehr bieten (ungefragt) den Internetnutzenden die Möglichkeit an, Daten in den jeweiligen Clouds abzulegen.
  → Eine Cloud ist also für viele ein riesengroßer Datenspeicher.
- Wikipedia: Cloud Computing (deutsch Rechnerwolke oder Datenwolke) beschreibt ein Modell, das bei Bedarf – meist über das Internet und geräteunabhängig – zeitnah und mit wenig Aufwand geteilte Computerressourcen als Dienstleistung, etwa in Form von Servern, Datenspeicher oder Applikationen, bereitstellt und nach Nutzung abrechnet. *)

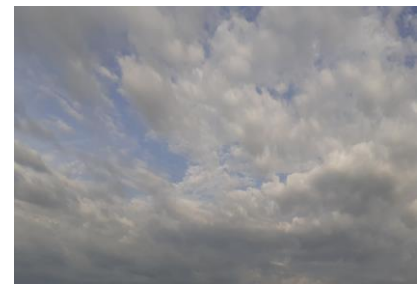
*) Seite „Cloud Computing In: Wikipedia – Die freie Enzyklopädie. Bearbeitungsstand: 23. August 2022, 08:47 UTC. URL: https://de.wikipedia.org/w/index.php?title=Cloud_Computing&oldid=225563547 (Abgerufen: 26. August 2022, 10:37 UTC)

- Auch Verwaltungsrechenzentren wie Dataport oder das Berlin ITDZ bieten Private Clouds an (Virtualisierung).

→Es ist keine eigene IT-Infrastruktur erforderlich (bis auf PC als Frontend).

→Cloud-Anbieter ist für Betrieb und die Sicherheit seine Infrastruktur (aber nicht der eigenen Anwendung) verantwortlich.

Berliner Situation

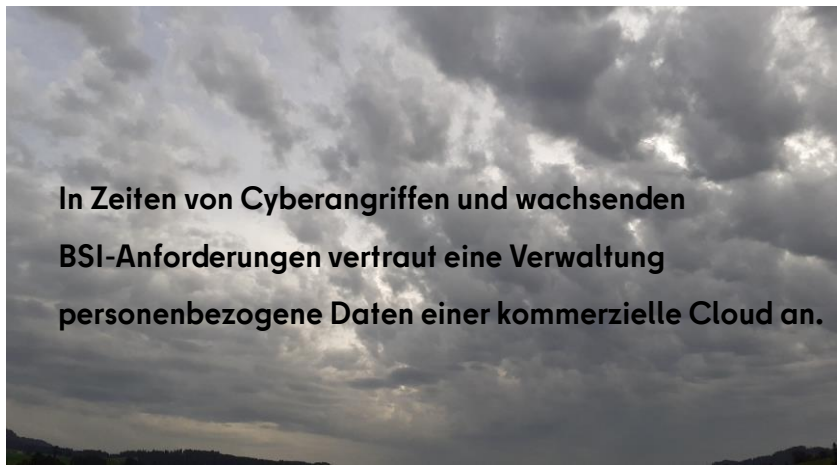


- SenSBW Berlin trägt die Verfahrensverantwortung für das AAA-Verfahren
  - Amtliches Festpunktinformationssystem
  - Amtliches Liegenschaftskatasterinformationssystem
  - Amtliches Topographisch-Kartographisches Informationssystem
  - Geobasisdaten online (AAA-Auskunfts- und Präsentationskomponente)
- Bis 08/2021 – Betrieb des AAA-Fachverfahrens in der Private Cloud des ITDZ Berlin
- Seit 08/2021 – Betrieb des AAA-Verfahrens in der Open Telekom Cloud von T-Systems im Managed Service von VertiGIS

Motivation - Den Aufbruch wagen in mehr Eigenständigkeit!

- Komplette Dienstleistung aus einer Hand
- Weniger Beteiligte, weniger Abstimmungsaufwand
- Betrieb des Verfahrens durch den Software-Anbieter („rund-um-sorglos Dienstleistung“)
- Beschleunigung der Prozesse der Releasewechsel
- Zeitnahe Umsetzbarkeit von außerfachlichen Forderungen an IT-Verfahren, z.B. hinsichtlich IKT-Vorgaben, Barrierefreiheit, Gebrauchstauglichkeit
- Mehr Einfluss auf die Gestaltung des Verfahrens
- Stärkere Fokussierung der Mitarbeitenden auf die fachliche Arbeit möglich
- Kostenneutral

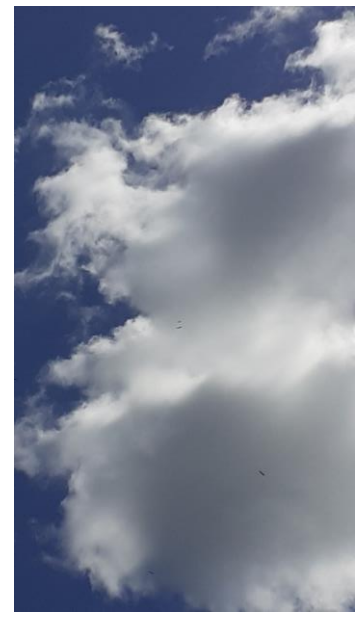
Ein bisschen verrückt?



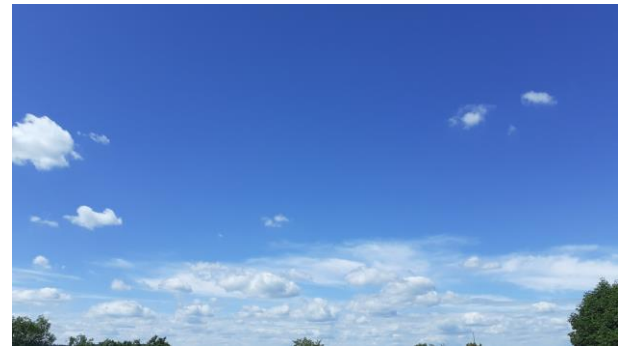
....nein, es muss nur einiges beachtet werden.

Anforderungen an die Dienstleister

- Vertrauenswürdige Cloud-Anbieter
- Vertrauensvolle Zusammenarbeit mit Managed Service-Anbieter
- DSGVO - konforme Anbieter
  - Hosting nur in Rechenzentren der EU oder sogar nur in Deutschland
- Zertifizierung der Dienstleister bspw.:
  - Cloud - BSI-C5 - Zertifizierung
  - Managed Service Anbieter - DIN EN ISO 27001-Zertifizierung (internationale Norm für Informationssicherheits-Management-systeme oder BSI-Zertifizierung)
- Abschluss von Vereinbarung zu Verarbeitung personenbezogener Daten
- Konzepte sind Vertragsbestandteil
- Sicherheitsüberprüfung 2 nach Sicherheitsüberprüfungsgesetz - SÜG
- Mitarbeitenden der Administration



Agiles Projekt - AAA-Betrieb in der OTC



Phase I

- Aufbau von Testumgebungen, um die grundsätzliche Machbarkeit zu verifizieren
- Vertrag für die Entwicklungsphase in 2020 mit kurzen Kündigungsfristen

Phase II

- Aufbau aller Umgebungen
- Tests der Software
- Erstellung der Konzepte
- Migration der Daten (Einspielung personenbezogener Daten erst nach Umsetzung der IT-Sicherheitsvorgaben, nach erfolgreichen Penetrationstest und Sicherheitsscan)
- Entwicklung des EVB-IT-System-Vertrages inkl. SLA, Serviceleistungen, AVV

Rahmenbedingungen Infrastruktur

- Isolierte Kundenumgebung („Tenant“) in der OTC für das AAA-Verfahren
- Berücksichtigung des nach BSI Grundschutz eingestuften Schutzbedarfs (normal)
- Definierte Verfügbarkeit für die jeweiligen Betriebsumgebungen
- Bereitstellung der Zugriffsverfahren für die unterschiedlichen Nutzerkreise (AAA 150, APK über 7.000 in- und extern)
- Sichere Anbindung OTC-Landesnetz
- Absicherung des Rollen- und Rechtekonzeptes
- Performance gleichbleibend oder besser

Konzepte I

- Basiskonzept
- Fachkonzepte jeweils für AFIS, ALKIS, ATKIS und die APK (Geobasisdaten online)
- Schulungskonzepte ALKIS und APK
- Einführungskonzept (EK)
- Migrationskonzept (MigK) inkl. Projektplan

Konzepte II

- Verfahrensspezifisches Sicherheitskonzept (V-SIKO) inkl. Datenschutz- und Löschkonzept, Technische und Organisatorische Maßnahmen, BSI-Bausteine OPS 2.1, 2.2 und 3.1
- AAA-Infrastrukturkonzept (ISK)
- AAA-Betriebskonzept (BK)
- AAA-Datensicherungskonzept (DSK)
- AAA-Testkonzepte (fachlich und infrastrukturell)
- AAA-Notfallkonzept

V-SIKO - Grundlagen

- BSI Grundschutzkompendium
- BSI-Standard 200-2 Version 1.0
- Datenschutz-Grundverordnung (DSGVO)
- Gesetz zum Schutz personenbezogener Daten in der Berliner Verwaltung (Berliner Datenschutzgesetz)
- Vorgehensmodell der SenStadtWohn zur Erstellung von V-SiKos
- Standard-Datenschutzmodell (Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele)" der 99. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 17.04.2020, Version 2.0b (SDM)
- Kurzpapier Nr. 18 der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK): „Risiko für die Rechte und Freiheiten natürlicher Personen“
- DIN ISO 31000:2018-10 Risikomanagement - Leitlinien

BSI-Baustein OPS 2.1 - Outsourcing für Kunden

- 1 Basisanforderungen
- 1.1 OPS.2.1.A1 Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben
- 2 Standard-Anforderungen
- 2.1 OPS.2.1.A2 Rechtzeitige Beteiligung der Personalvertretung
- 2.2 OPS.2.1.A3 Auswahl eines geeigneten Outsourcing-Dienstleisters
- 2.3 OPS.2.1.A4 Vertragsgestaltung mit dem Outsourcing-Dienstleister
- 2.4 OPS.2.1.A5 Festlegung einer Strategie zum Outsourcing
- 2.5 OPS.2.1.A6 Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben
- 2.6 OPS.2.1.A7 Festlegung der möglichen Kommunikationspartner
- 2.7 OPS.2.1.A8 Regelungen für den Einsatz des Personals des Outsourcing-Dienstleisters
- 2.8 OPS.2.1.A9 Vereinbarung über die Anbindung an Netze der Outsourcing-Partner
- 2.9 OPS.2.1.A10 Vereinbarung über Datenaustausch zwischen den Outsourcing-Partnern
- 2.10 OPS.2.1.A11 Planung und Aufrechterhaltung der Informationssicherheit im laufenden Outsourcing-Betrieb
- 2.11 OPS.2.1.A12 Änderungsmanagement
- 2.12 OPS.2.1.A13 Sichere Migration bei Outsourcing-Vorhaben
- 2.13 OPS.2.1.A14 Notfallvorsorge beim Outsourcing
- 2.14 OPS.2.1.A15 Geordnete Beendigung eines Outsourcing-Verhältnisses
- 3 Anforderungen bei erhöhtem Schutzbedarf
- 3.1 OPS.2.1.A16 Sicherheitsüberprüfung von Mitarbeitenden

BSI-Baustein OPS 2.2 - Cloud-Nutzung

- 1 Basisanforderungen
- 1.1 OPS.2.2.A1 Erstellung einer Cloud-Nutzungs-Strategie
- 1.2 OPS.2.2.A2 Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung
- 1.3 OPS.2.2.A3 Service-Definition für Cloud-Dienste durch den Cloud-Kunden
- 1.4 OPS.2.2.A4 Festlegung von Verantwortungsbereichen und Schnittstellen
- 2 Standard-Anforderungen
- 2.1 OPS.2.2.A5 Planung der sicheren Migration zu einem Cloud-Dienst
- 2.2 OPS.2.2.A6 Planung der sicheren Einbindung von Cloud-Diensten
- 2.3 OPS.2.2.A7 Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung
- 2.4 OPS.2.2.A8 Sorgfältige Auswahl eines Cloud-Diensteanbieters
- 2.5 OPS.2.2.A9 Vertragsgestaltung mit dem Cloud-Diensteanbieter
- 2.6 OPS.2.2.A10 Sichere Migration zu einem Cloud-Dienst
- 2.7 OPS.2.2.A11 Erstellung eines Notfallkonzeptes für einen Cloud-Dienst
- 2.8 OPS.2.2.A12 Aufrechterhaltung der Informationssicherheit im laufenden Cloud-Nutzungs-Betrieb
- 2.9 OPS.2.2.A13 Nachweis einer ausreichenden Informationssicherheit bei der Cloud-Nutzung
- 2.10 OPS.2.2.A14 Geordnete Beendigung eines Cloud-Nutzungs-Verhältnisses
- 3 Anforderungen bei erhöhtem Schutzbedarf
- 3.1 OPS.2.2.A15 Sicherstellung der Portabilität von Cloud-Diensten
- 3.2 OPS.2.2.A16 Durchführung eigener Datensicherungen
- 3.3 OPS.2.2.A17 Einsatz von Verschlüsselung bei Cloud-Nutzung
- 3.4 OPS.2.2.A18 Einsatz von Verbunddiensten
- 3.5 OPS.2.2.A19 Sicherheitsüberprüfung von Mitarbeitern

BSI-Baustein - OPS 3.1 - Outsourcing für Dienstleister

- 1 Basisanforderungen
- 1.1 OPS.3.1.A1 Erstellung eines Grobkonzeptes für die Outsourcing-Dienstleistung
- 2 Standard-Anforderungen
- 2.1 OPS.3.1.A2 Vertragsgestaltung mit den Outsourcing-Kunden
- 2.2 OPS.3.1.A3 Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben
- 2.3 OPS.3.1.A4 Festlegung der möglichen Kommunikationspartner
- 2.4 OPS.3.1.A5 Regelungen für den Einsatz des Personals des Outsourcing-Dienstleisters
- 2.5 OPS.3.1.A6 Regelungen für den Einsatz von Fremdpersonal
- 2.6 OPS.3.1.A7 Erstellung eines Mandantentrennungskonzeptes durch den Outsourcing-Dienstleister
- 2.7 OPS.3.1.A8 Vereinbarung über die Anbindung an Netze der Outsourcing-Partner
- 2.8 OPS.3.1.A9 Vereinbarung über Datenaustausch zwischen den Outsourcing-Partnern
- 2.9 OPS.3.1.A10 Planung und Aufrechterhaltung der Informationssicherheit im laufenden Outsourcing-Betrieb
- 2.10 OPS.3.1.A11 Zutritts-, Zugangs- und Zugriffskontrolle
- 2.11 OPS.3.1.A12 Änderungsmanagement
- 2.12 OPS.3.1.A13 Sichere Migration bei Outsourcing-Vorhaben
- 2.13 OPS.3.1.A14 Notfallvorsorge beim Outsourcing
- 2.14 OPS.3.1.A15 Geordnete Beendigung eines Outsourcing-Verhältnisses
- 3 Anforderungen bei erhöhtem Schutzbedarf
- 3.1 OPS.3.1.A16 Sicherheitsüberprüfung von Mitarbeitern

Projekterfolg und Erfahrungen nach einem Jahr vollständigen Betrieb

- Vollständiger Produktionsbeginn aller vier AAA-Teilfachverfahren innerhalb von 22 Monaten ab der Projektidee
- Zuverlässige Releasewechsel nach kurzfristig abgestimmten, standardisierten Zeitplänen
- Unkomplizierter und zügige Bereitstellung weiterer Umgebungen (zusätzliche Server für großen Release, Migrationsumgebung)
- Knowhow-Aufbau bei SenSBW durch die Nähe zum Verfahrensbetreiber
- Umsetzung aller BSI-Anforderungen
- Eingespielte Betriebsabläufe gut dokumentiert im Betriebskonzept
- Datenaustauschlösung Nextcloud unbefriedigend

Ein Lösung für alle?

- Folgende Fragen sollten Sie sich stellen:
- Haben Sie einen SW-Anbieter, mit dem Sie schon länger vertrauensvoll zusammenarbeiten oder der Erfahrung mit dem Managed Service in einer Cloud hat?
- Haben Sie die Zustimmung der Stellen Ihres Landes, die für die IT-Infrastruktur und die IT-Sicherheit zuständig sind?
- Sind Sie bereit, sich mit dem BSI-Grundschutzkompendium gemeinsam mit externer Begleitung auseinander zu setzen?
- Welche Basisdienste Ihres Landes können Sie nutzen? (Verfahren zur 2-Faktor-Authentifizierung, Kommunikationsverbindung (VPN, NdB, Datenaustausch)

→ Viermal Ja? Dann nichts wie ran!


Vielen Dank für Ihre Aufmerksamkeit!
BERLIN
Kontakt: Anette Blaser I anette.blaser@senstadt.berlin.de I 030-91390-5310
Weitnauer Tal / Leutfritz