

Cloud-Computing und Datensicherheit

*Vortrag im Seminar „Gesellschaftliche
Strukturen im Digitalen Wandel“*

von Alexander Girke



*Aus „Introduction to Azure Stack“ von Bert Johnson, erstellt 23.02.2016,
<https://static.allcloud.com/assets/images/blog/there-is-no-cloud.png>, abgerufen 13.01.2019.*

Gliederung

- Grundlagen
- Datensicherheit im Detail
- Cloud-Lösungen
- Staatliche Maßnahmen
- Vergleich zu Alternativen
- Zwischenfazit
- Diskussion

Grundlagen

Cloud-Computing

„Der Begriff Cloud Computing beschreibt ein Konzept, welches die Bereitstellung von elektronischen Diensten (wie z.B. Rechenleistung oder Speicherkapazität) bei Bedarf, [...] ermöglicht.“

[Urbach 2018]

Grundlagen

Cloud-Computing

„Unter Ausnutzung virtualisierter Rechen- und Speicherressourcen und moderner Web-Technologien stellt Cloud Computing skalierbare, netzwerkzentrierte, abstrahierte IT-Infrastrukturen, Plattformen und Anwendungen als on-demand Dienste zur Verfügung. Die Abrechnung dieser Dienste erfolgt nutzungsabhängig.“

[Baun, Kunze, Nimis, Tai 2011, S. 4]

Grundlagen

Datensicherheit

(auch Informationssicherheit, IT-Sicherheit)

„Datensicherheit als wesentlicher Bestandteil des Datenschutzes [...], der technische und organisatorische Maßnahmen beschreibt.“

Datenschutz

„Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten“

[Lenhard 2017, S. 3f]
angelehnt an Richtlinie 95/46/EG des Europäischen Parlaments
und des Rates vom 24. Oktober 1995

Grundlagen

Datensicherheit

(auch Informationssicherheit, IT-Sicherheit)

„Unter IT-Sicherheit verstehen wir den Schutz von Informationen und Informationssystemen gegen unbefugte Zugriffe und Manipulationen sowie die Sicherstellung der Verfügbarkeit [...] für legitime Benutzer, einschließlich aller Maßnahmen zur Verhinderung, Entdeckung oder Protokollierung von Bedrohungen [...], insbesondere während der Speicherung, der Verarbeitung und der Übertragung.“

[Kappes 2013, S. 2]

Grundlagen

Rechtliche Grundlagen

- „BSI-Errichtungsgesetz“ (1991)
- „BSI-Gesetz“ (2009)
- „IT-Sicherheitsgesetz“ (2015)

BSI = **B**undesamt für **S**icherheit in der **I**nformationstechnik

Datensicherheit im Detail

- BSI-Glossar „Grundwerte der Informationssicherheit“
 - Vertraulichkeit, Verfügbarkeit und Integrität
 - zusätzlich: Authentizität, Verbindlichkeit, Zuverlässigkeit, Nichtabstreitbarkeit

[BSI-Glossar 2013]

- in [Kappes 2013]: Verbindlichkeit = Nichtabstreitbarkeit
- manchmal Unterscheidung: Authentisierung & Authentifizierung

Datensicherheit im Detail

- Definitionen in [Kappes 2013, S. 2f]:
 - *Vertraulichkeit*: Schutz von Information gegenüber unbefugten Zugriffen Dritter.
 - *Integrität*: Schutz von Information gegenüber Veränderung durch Unbefugte.
 - *Verfügbarkeit*: Ressourcen und Dienste stehen legitimen Benutzern tatsächlich zur Verfügung.

Datensicherheit im Detail

- Definitionen in [Kappes 2013, S. 2f]:
 - *Authentizität*: Eindeutige Identifikation des Absenders von Information bei der Informationsübertragung.
 - *Verbindlichkeit*: Möglichkeit, den Inhalt und den Absender von Information gegenüber einem [...] Dritten zu beweisen.
 - *Autorisation*: Beschränkung des Zugriffs auf eine Ressource auf bestimmte (authentifizierte) Benutzer.

Datensicherheit im Detail

- Beispiele für Gefahren:
 - Gehaltsabrechnungsdatei geöffnet, Bildschirm nicht gesperrt (Vertraulichkeit)
 - Feuer zerstört Festplatte (Integrität)
 - DDoS-Attacke auf Server (Verfügbarkeit)
 - Abfangen und Verwendung eines Identitäts-Tokens durch einen Dritten (Authentizität)
 - Datei-Signatur nicht verwendet (Verbindlichkeit)
 - standardmäßige Verwendung des Admin-Nutzers am Rechner (Autorisierung)
- keine 100-prozentige Sicherheit

Cloud-Lösungen

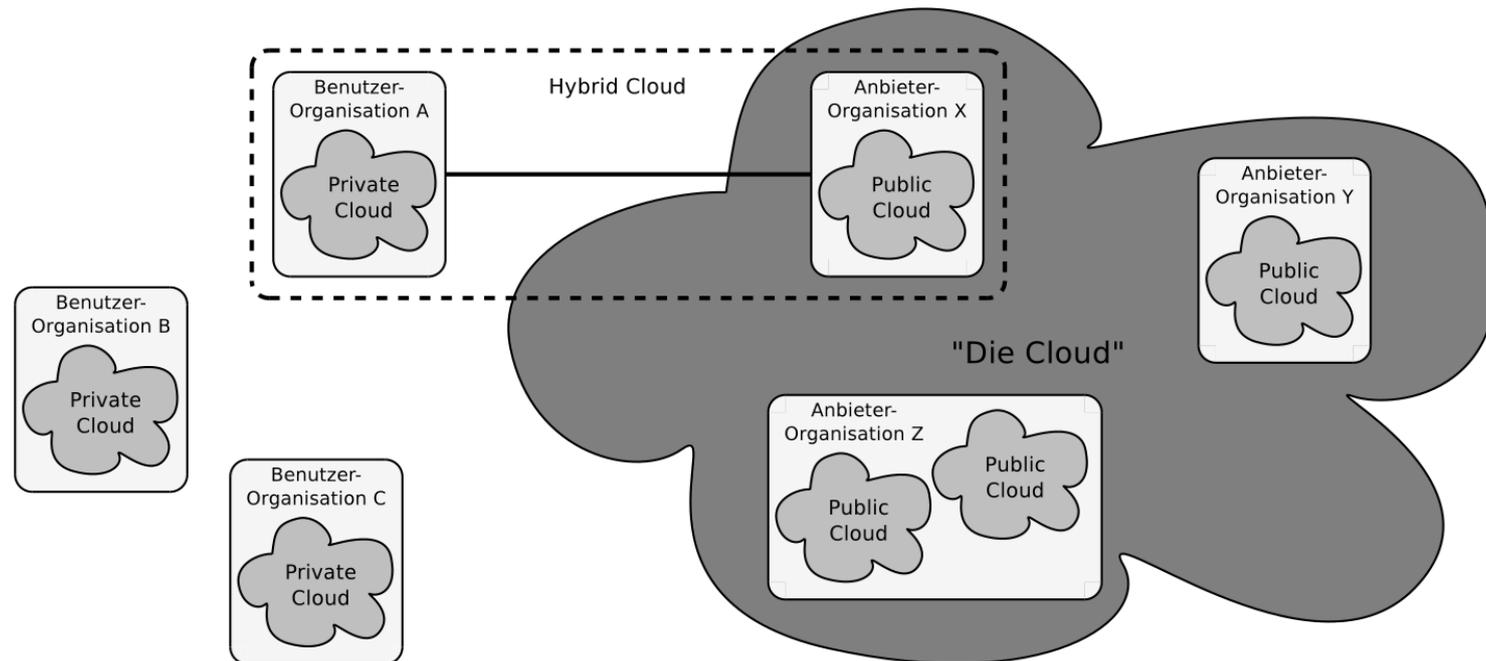
Formen

- *public*: Anbieter und Benutzer nicht in derselben organisatorischen Einheit
- *private*: Cloud innerhalb einer Organisation
- *hybrid*: Regelbetrieb=privat; Spezielles=public

(vgl. [Baun, Kunze, Nimis, Tai 2011])

- weitere: community, personal, **VirtualPrivateCloud**

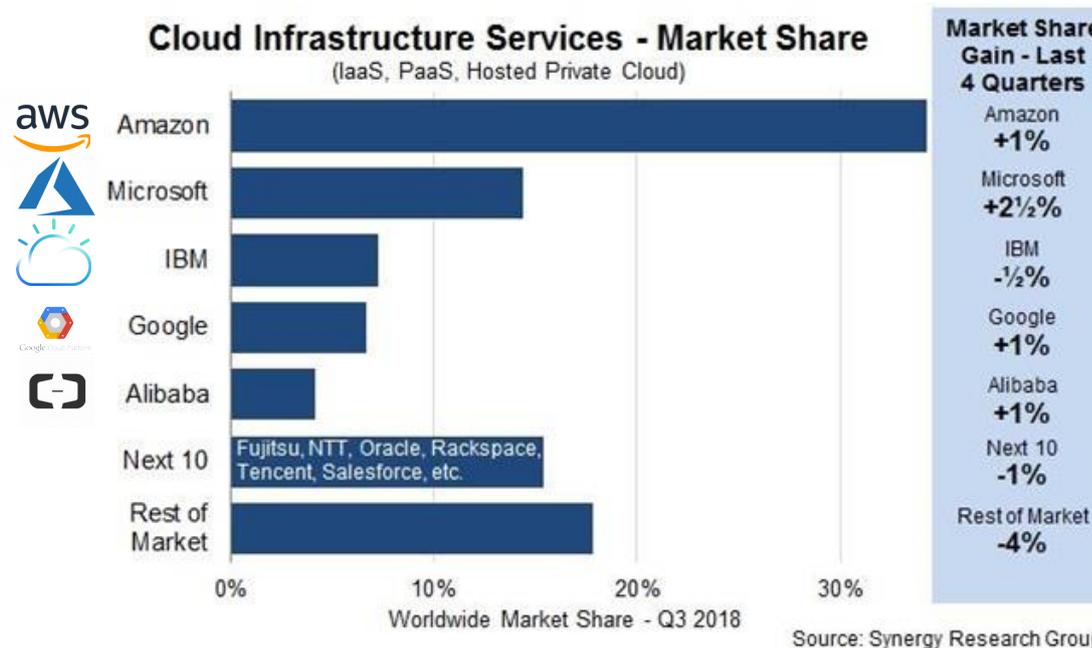
Cloud-Lösungen



Aus [Baun, Kunze, Nimis, Tai 2011, S. 28, Abbildung 3.1]

Cloud-Lösungen

Anbieter



Aus „The Leading Cloud Providers Increase Their Market Share Again in the Third Quarter“ von Synergy Research Group, erstellt 26.10.2018, in: <https://globenewswire.com/news-release/2018/10/26/1627680/0/en/The-Leading-Cloud-Providers-Increase-Their-Market-Share-Again-in-the-Third-Quarter.html>, abgerufen 13.01.2019.

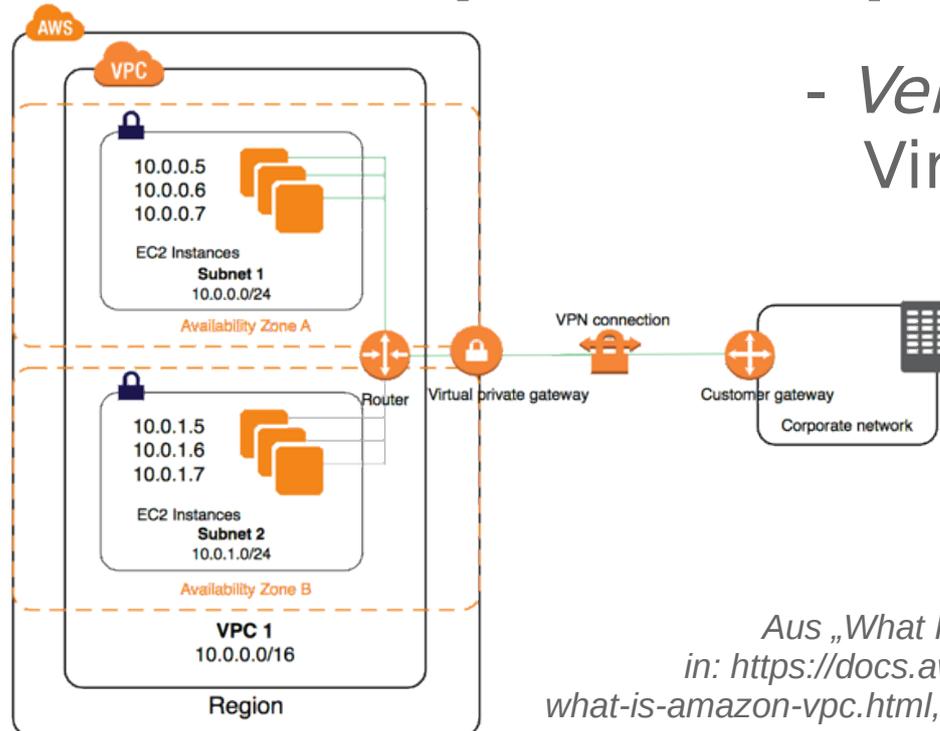
Cloud-Lösungen

Produktarten

- *Infrastructure as a Service (IaaS):*
Speicher, Rechner, Netzwerk, ...
- *Platform as a Service (PaaS):*
Applikationsumgebungen (z.B. Java)
- *Software as a Service (SaaS):*
Endnutzeranwendungen (z.B. Dropbox)

Cloud-Lösungen

Datensicherheitsaspekte (Beispiel AWS)



- *Vertraulichkeit: AWS Virtual Private Cloud*

Aus „What Is Amazon VPC?“ von Amazon AWS, in: <https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html>, abgewandelt, abgerufen 13.01.2019.

Cloud-Lösungen

Datensicherheitsaspekte (Beispiel AWS)

- *Integrität*: AWS Datenzentren
<https://aws.amazon.com/de/compliance/data-center/data-centers/>
- physisch schwer zugänglich
- Replikation über Availability-Zones (AZ)
- mehrere Regionen weltweit

Cloud-Lösungen

Datensicherheitsaspekte (Beispiel AWS)

AWS Global Infrastructure



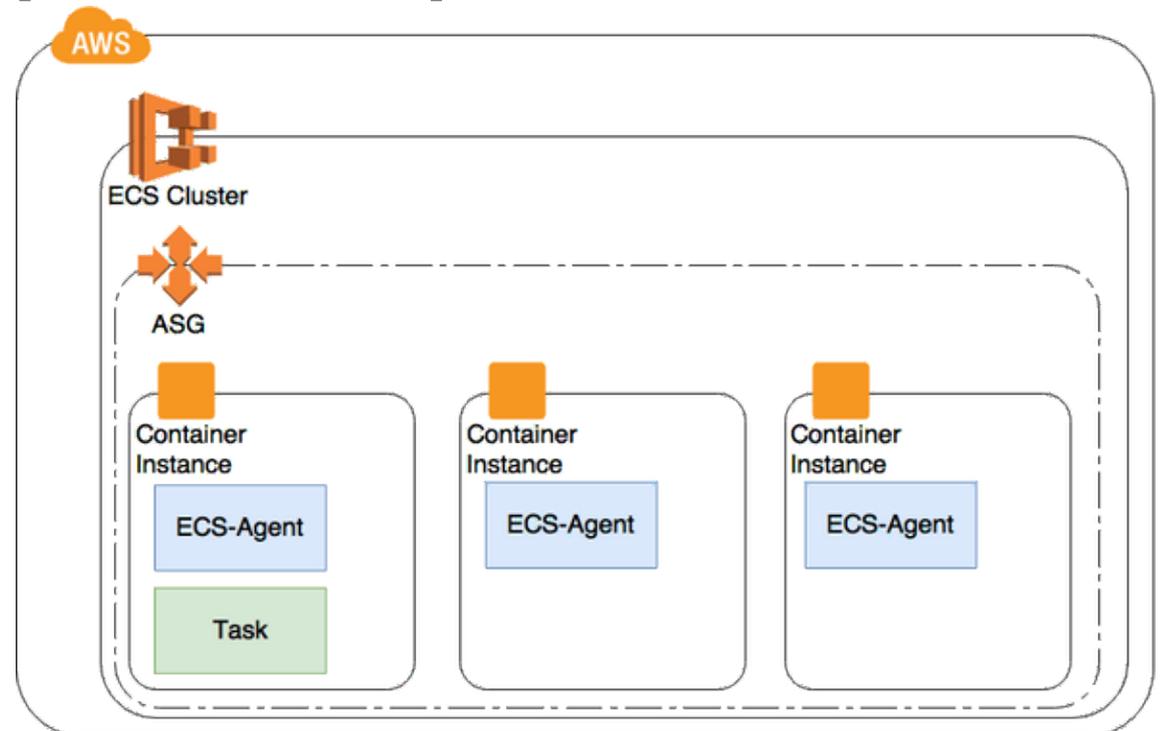
Aus „Should I Build a Multi-Region Architecture in AWS?“ von Onica, erstellt 25.04.2016, in: <https://www.onica.com/blog/should-i-build-a-multi-region-architecture-in-aws/>, abgerufen 13.01.2019.

Cloud-Lösungen

Datensicherheitsaspekte (Beispiel AWS)

- *Verfügbarkeit:*
AWS Elastic
Container
Service

Aus „*Docker, Containers, VMs and ECS - an overview*“ von CRM Trilogix, erstellt 07.05.201, in:
<http://crmtrilogix.com/Cloud-Blog/AWS/Docker-Containers-VMs-and-ECS---an-overview/219>, abgerufen 13.01.2019.

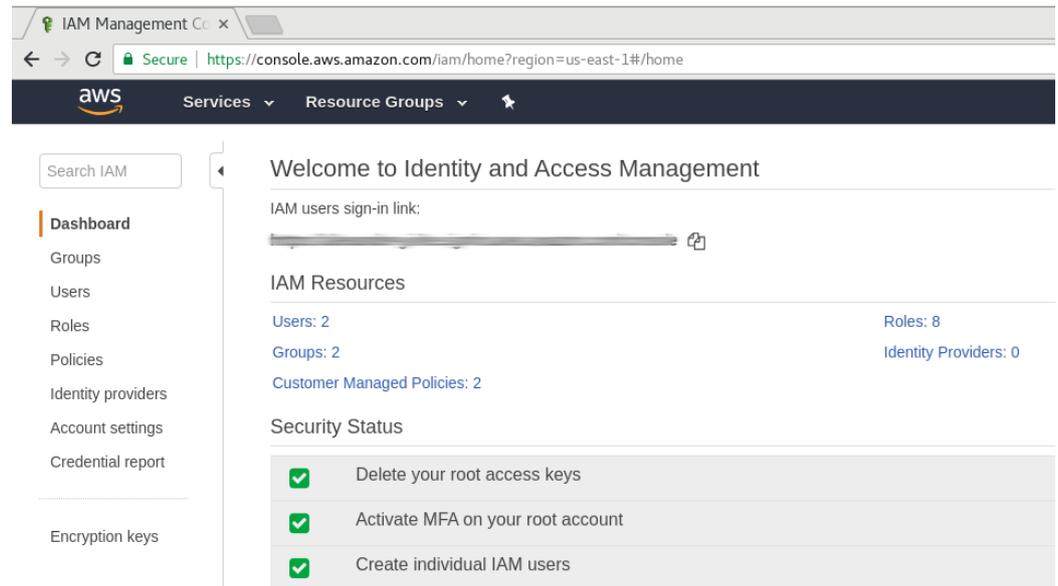


Cloud-Lösungen

Datensicherheitsaspekte (Beispiel AWS)

- *Authentizität & Autorisation:*

AWS Identity
and
Access
Management



The screenshot shows the AWS IAM console dashboard. The main content area displays the following information:

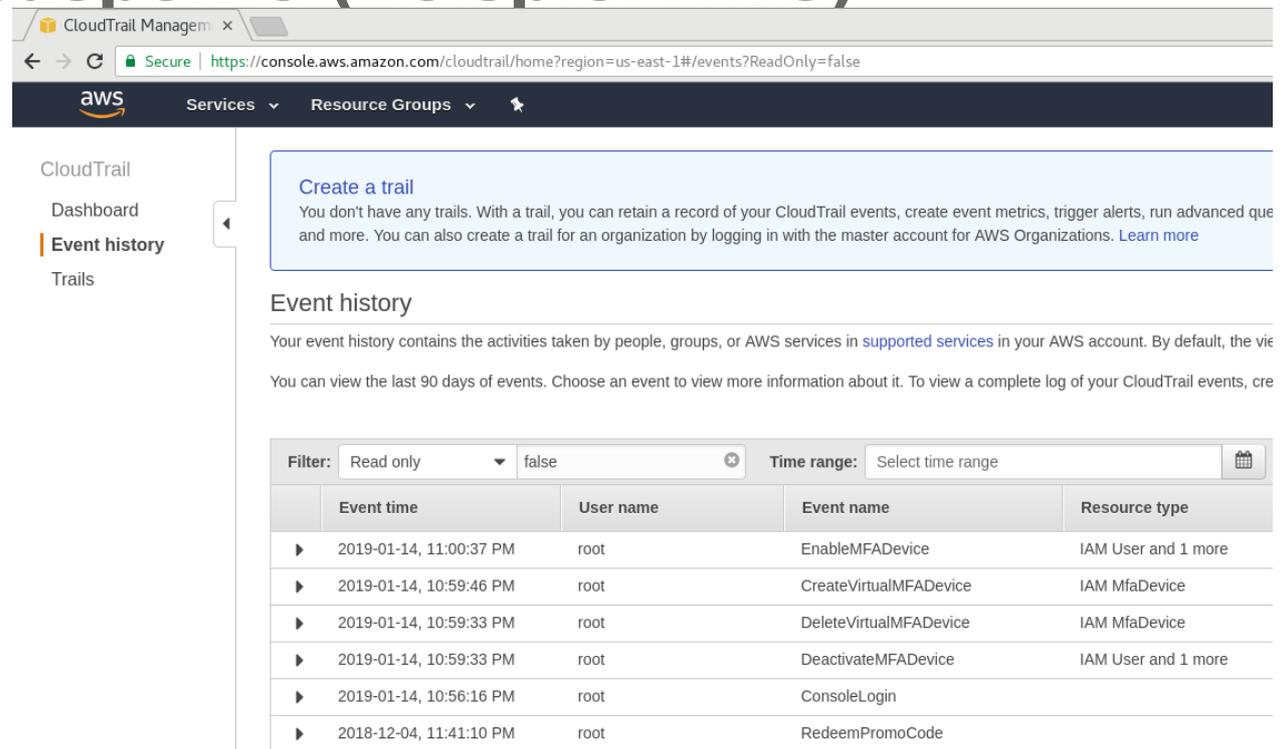
- Welcome to Identity and Access Management**
- IAM users sign-in link:** [Link]
- IAM Resources:**
 - Users: 2
 - Groups: 2
 - Customer Managed Policies: 2
 - Roles: 8
 - Identity Providers: 0
- Security Status:**
 - Delete your root access keys
 - Activate MFA on your root account
 - Create individual IAM users

Screenshot „AWS Console IAM“, erstellt
12.01.2019.

Cloud-Lösungen

Datensicherheitsaspekte (Beispiel AWS)

- Verbindlichkeit:
AWS
CloudTrail
(Auditing)



The screenshot shows the AWS CloudTrail console interface. The top navigation bar includes the AWS logo, 'Services', and 'Resource Groups'. The left sidebar contains a navigation menu with 'CloudTrail', 'Dashboard', 'Event history', and 'Trails'. The main content area features a 'Create a trail' button and a 'Event history' section. The event history table is filtered for 'Read only' and shows a list of events from 2018-12-04 to 2019-01-14.

Event time	User name	Event name	Resource type
2019-01-14, 11:00:37 PM	root	EnableMFADevice	IAM User and 1 more
2019-01-14, 10:59:46 PM	root	CreateVirtualMFADevice	IAM MfaDevice
2019-01-14, 10:59:33 PM	root	DeleteVirtualMFADevice	IAM MfaDevice
2019-01-14, 10:59:33 PM	root	DeactivateMFADevice	IAM User and 1 more
2019-01-14, 10:56:16 PM	root	ConsoleLogin	
2018-12-04, 11:41:10 PM	root	RedeemPromoCode	

Screenshot „AWS Console CloudTrail“,
erstellt 12.01.2019.

Staatliche Maßnahmen

- Staat hat Interesse an digitaler Sicherheit der Bevölkerung und Unternehmen

- Auszug aus [Koalitionsvertrag 2018, S. 43]:

„bessere Unterstützung insbesondere des Mittelstandes bei IT-Sicherheit. [...] (BSI) als Beratungsstelle für kleine und mittlere Unternehmen auszubauen“

- Auszug aus [Koalitionsvertrag 2018, S. 45]:

„Einhaltung dieser [...] IT-Sicherheitsstandards werden wir Verbraucherinnen und Verbrauchern mit einem Gütesiegel für IT-Sicherheit transparent machen.“

- Staatlich Behörden/Ämter:

- BSI: zentrale Meldestelle, Beratung, KRITIS, ...

- ZITiS: „Zentrale Stelle für Informationstechnik im Sicherheitsbereich“;
Terrorismus-/Cybercrimeabwehr, Unterstützung der Sicherheitsbehörden

[ZITiS 2018]

Staatliche Maßnahmen

- Auszüge aus BSI-Magazin 2018/01:
 - *[Mehrfeld 2018]*: Appell zur Zusammenarbeit und offenen Kommunikation der Beteiligten
 - *[Erdrich, Kluge 2018]*: Darstellung der Angriffshistorie; Ausblick
- IT-Sicherheit wird nicht durch Staat erzwungen, nur unterstützt

Vergleich zu Alternativen

Private Nutzung

- Fotospeicherung

	USB-Stick	Cloud-basierter Dienst
Vertraulichkeit	↑ physischer Zugang einfach beschränkbar	↓ Daten auf fremden Servern
Integrität	↓ hohe Ausfallwahrscheinlichkeit ohne Kopie	↑ Redundanz
Verfügbarkeit	↓ Stick muss vor Ort sein	↑ von überall erreichbar
Autorisation	↑ Dateien nur nach Stick-Weitergabe zugänglich	↑ Dateien einzeln freischaltbar (Link/Passwort)

Vergleich zu Alternativen

Kommerzielle Nutzung

- mittelständisches E-Commerce-Unternehmen

	firmeneigenes Rechenzentrum	Cloud-basierte Infrastruktur
Vertraulichkeit	↑ nur im Firmennetz zugänglich	↑ VPC für Netzwerksicherheit
Integrität	↓ Erdbeben, Feuer, ...	↑ Redundanz
Verfügbarkeit	↓ Automatisierung Ausfall	↑ bei Bedarf Skalierung
Autorisation	↓ Rechtekonzept nötig	↑ Rechtekonzept inklusive

Zwischenfazit

- Datensicherheitsaspekte bei Cloud-Diensten berücksichtigt
 - meist besser als „Eigenbau“
 - „Cloud“ (Datenzentren) hoch automatisiert, meist höhere Sicherheitsstandards als bei firmeneigenen Rechenzentren
 - jeweils passende Produkte zur Netzwerksicherheit, Zugriffsbeschränkung und Nachvollziehbarkeit

Diskussion

- Hackerattacke auf Politiker & Prominente
 - neue Gesetze?
 - Umgang mit Datensicherheit schulen?
 - ...
- eigene Erfahrungen?
- ...

Quellen

- [Baun, Kunze, Nimis, Tai 2011]
Baun, Christian; Kunze, Marcel; Nimis, Jens; Tai, Stefan (2011): Cloud Computing - Web-basierte dynamische IT-Services. 2. Auflage, Berlin/Heidelberg: Springer-Verlag, 2011.
- [BSI-Glossar 2013]
BMI (2013): Glossar, in: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/glossar/04.html, erstellt 2013, abgerufen 13.01.2019.
- [Erdrich, Kluge 2018]
Erdrich, Andreas; Kluge, Jens (2018): Cyber-Gefahren für Industrieanlagen, in: Mit Sicherheit - BSI-Magazin 2018/01, S. 28f.
- [Kappes 2013]
Kappes, Martin (2013): Netzwerk- und Datensicherheit - Eine praktische Einführung. 2. Auflage, Wiesbaden: Springer Vieweg, 2013.
- [Koalitionsvertrag 2018]
Bundesregierung (2018): Koalitionsvertrag zwischen CDU, CSU und SPD, in: https://www.cdu.de/system/tdf/media/dokumente/koalitionsvertrag_2018.pdf?file=1, erstellt 7. Februar 2018, abgerufen 13.01.2019.
- [Lenhard 2017]
Lenhard, Thomas H. (2017): Datensicherheit - Technische und organisatorische Schutzmaßnahmen gegen Datenverlust und Computerkriminalität. Wiesbaden: Springer Vieweg, 2017.
- [Mehrfeld 2018]
Mehrfeld, Jens (2018): Gemeinsame Verantwortung, in: Mit Sicherheit - BSI-Magazin 2018/01, S. 26f.
- [Urbach 2018]
Urbach, Nils (2018): Cloud Computing, in: <http://www.enzyklopaedie-der-wirtschaftsinformatik.de/lexikon/uebergreifendes/Kontext-und-Grundlagen/Markt/Softwaremarkt/Geschäftsmodell-%28fur-Software-und-Services%29/Cloud-Computing/index.html>, erstellt 07.03.2018, abgerufen 12.01.2019.
- [ZITIS 2018]
BMI (2018): ZITIS, in: <https://www.bmi.bund.de/SharedDocs/behoerden/DE/zitis.html>, abgerufen 13.01.2019.