Servicebewertung AWS Amazon S3

Amazon Simple Storage Service (Amazon S3) ist ein verwalteter Objektspeicherservice für die Speicherung von beliebigen Datenmengen. Mit Verwaltungsfunktionen kann der Zugriff auf die Daten eingeschränkt werden.

https://aws.amazon.com/de/s3/resources/

Location

Beschreibt, in welchem geografischen Bereich der Service erbracht wird.

Globaler Service, der sich nicht einschränken lässt	
Service, der sich regional einschränken lässt	x

Datentypen, die eingebracht werden dürfen

Die hier selektierten Datentypen dürfen in den Service eingebracht werden. Es wird hier gemäß der Zweckmäßigkeit für den entsprechenden Service bewertet.

Nutzdaten / Daten des Endkunden	x
Personenbezogene Daten	x
Sonstige Daten	x

Telemetriedaten

Werden Daten über Nutzungsverhalten des Services und/oder der Nutzer vom Anbieter erhoben?

Ja	x
Ja, aber deaktivierbar	
Nein	

Verschlüsselung at-rest

Verschlüsselung der Daten bei Speicherung auf einem Speichersystem. Metadaten und Tags werden hier nicht berücksichtigt.

AWS KMS - CMK mit externem Material (BYOK)	x
AWS KMS - Customer-managed Key (CMK)	x
AWS KMS - AWS-managed key	x
Von AWS verschlüsselt ohne Einflussmöglichkeiten	x
Keine Information	

Verschlüsselung in-transit

Verschlüsselung der Daten bei Übertragung. Betrachtet wird hier die Verschlüsselung von und zu AWS verwalteten Services (z.B. DB). Die Verschlüsselung zu der AWS API selbst wird hier nicht betrachtet, da immer

SSL/TLS Verbindung für den Zugriff auf den Service und zwischen allen Komponenten des Services	
Verschlüsselung ist optional nutzbar	
Verschlüsselung kann optional selbst implementiert werden	
Es wird keine Netzwerkverbindung zu Service bereitgestellt (außer AWS API selbst)	x

verschlüsselte Variante verfügbar.

ISO 27001		
Unterliegt der Service der ISO 27001 Zertifizierung des Anbieters?	Ja	x
	Nein	

Zugangssteuerung		
Steuerung des Zugangs zum AWS Service. Der Zugang zu selbst bereitgestellten Anwendungen wird hier nicht betrachtet.	AWS IAM: Individuelle User und Rollen möglich	x
	RBAC: Berechtigung an AWS Ressource selbst	x
	AWS Service-Linked-Role: AWS eigene Rolle zur Serviceerbringung	partial
	Muss selbst implementiert/konfiguriert werden	

Audit Logs		
Art und Weise der Protokollierung. Relevant sind hier Audit Logs: Was wurde wann von wem getan. Applikationslogs werden hier nicht betrachtet.	AWS CloudTrail: Evtl. nicht jeder Eventtyp	x
	AWS Service schreibt eigene Audit Logs	
	Keine Protokollierung	

Netzwerkanbindung		
Wo wird der Service aus Netzwerksicht betrieben? Kann ohne AWS public API netzwerkseitig auf Resourcen des Services zugegriffen werden?	Zugriff nur über AWS API möglich	x
	Eigenes VPC	
	AWS hosted SaaS	x

Backup und Recovery		
Welche Möglichkeiten für Backup- und Recovery gibt es für den Service? Betrachtet werden hier nur von uns selbst im Service abgelegte Daten.	Keine Datensicherung notwendig	
	AWS bietet eine managed Lösung an	x
	Es existiert eine API, um Backup selbst zu implementieren	x
	Datensicherung ist nicht verfügbar	

Internet Inbound		
Über welche Wege kann von außerhalb des eigenen Netzwerks auf selbst im Service gespeicherte Daten zugegriffen werden?	AWS API bietet Möglichkeit Daten abzurufen	x
	Abruf von Daten über VPC möglich	

Internet Outbound		
Ist ein Zugriff auf das Internet über diesen Service möglich oder können	Service ermöglicht Internetzugriff	
	Daten können mit dem Service in das Internet publiziert werden	x

damit im Service gespeicherte Daten in das Internet publiziert werden?

Datum der Analyse	**23.05.22**

Nutzungskonzept

- Buckets dürfen nicht public zur Verfügung gestellt werden
- Mindestens AES256 Verschlüsselung nutzen, wenn für Datenklasse gefordert AWS-CMK oder BYOK
- Zugriff auf Bucket nur per HTTPS: Enforcement ist per Policy implementiert
- Es dürfen keine IAM Ressourcen freigegeben werden, die nicht zur eigenen Organisazion gehören

Bei Fragen oder Problem kontaktieren Sie kontakt@be-bold.today