TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

"T.I.S.P. Community Meeting 2020"

Berlin, 03.-04.11.2020

Cloud Security –
Sicherheitsprinzipien und -maßnahmen für die Cloud

Heidrun Müller, eGovCD GmbH

KURZVORSTELLUNG

Heidrun Müller

Senior Researcher and Consultant, eGovCD GmbH

Mehr als 15 Jahre Erfahrung in den Bereichen:

- Digitalisierungskonzeption von der Idee bis zur Umsetzung
- Informations- und Prozessmanagement
- IT-Sicherheitsmanagement und Datenschutz
- Cloud-Technologien

Zertifikate

- "Lead Auditor Training CSA CoC for GDPR Compliance" (01/2019)
- "Cloud Security Knowledge" der Cloud Security Alliance (12/2016)

- Spin Off von Fraunhofer FOKUS
- Kernthemen:
  - Digitalisierung im Public Sector
  - Datenschutz- und Datensicherheit
  - Cloud-Technologien

- Mitglied im Privacy Center of Excellence der CSA EMEA

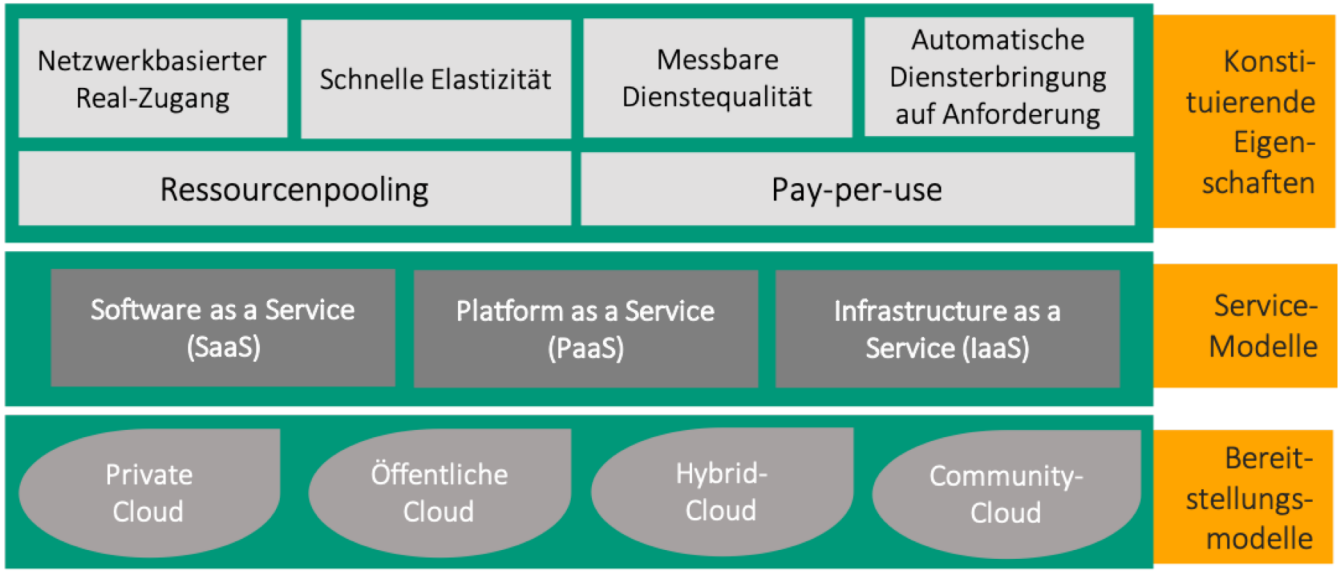
AGENDA

I. Einordnung: Cloud – Besonderheiten und Herausforderungen

II. Basis-Set: Sicherheitsprinzipien und -maßnahmen für die Cloud

III. Ausgewählte Normen und Standards für Cloud Security

CLOUD – AUF DEN ERSTEN BLICK VIELE VORTEILE…



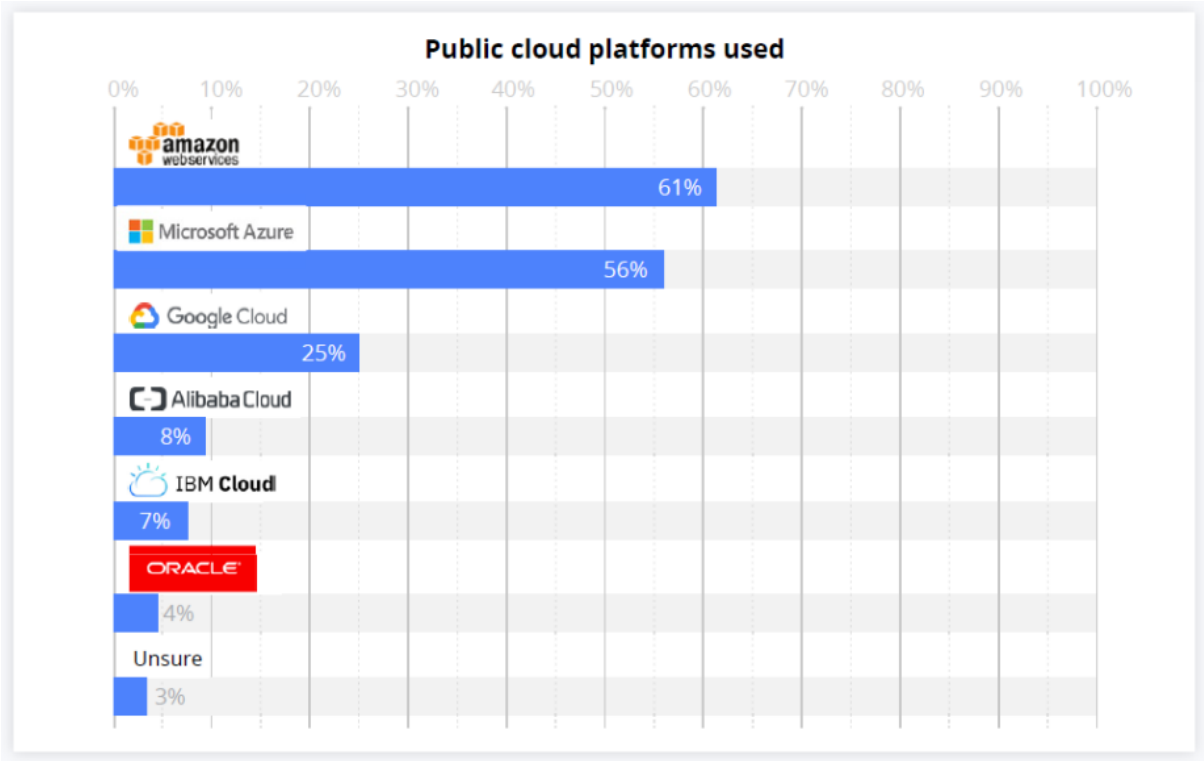
(Wahrgenommene?) Vorteile

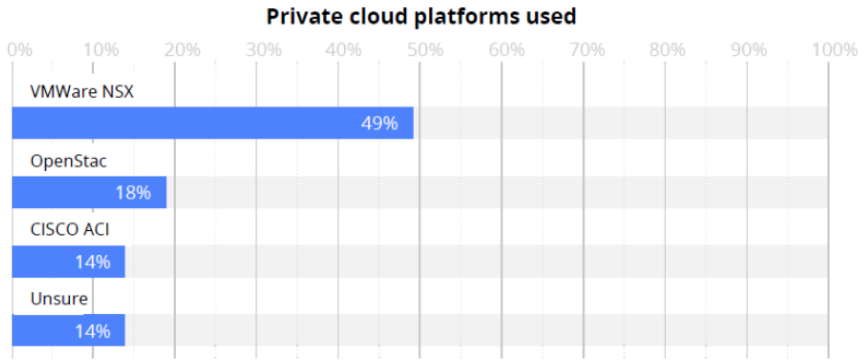
- Vermeidung Vendor Lock-In
- Kostenreduktion und -transparenz
- Skalierbarkeit
- Einfacher Zugang zu Services auch für „Nicht-Experten“

- Jede Kombination ist möglich und wird auch genutzt!!

Aber: Neue Steuerungsmodi für Security erforderlich!

CLOUD-NUTZUNG WELTWEIT

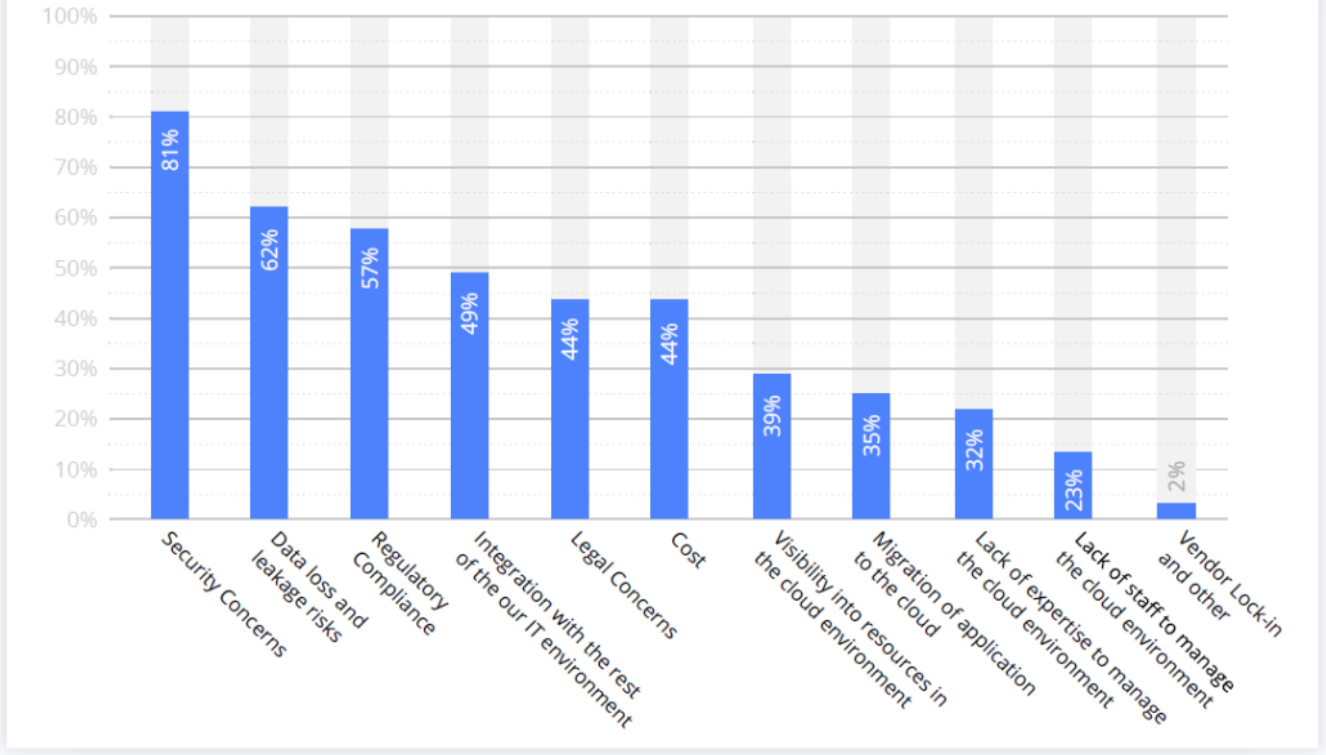




- Trend zur Nutzung von Public Clouds hält an (Ausnahme: Finanzsektor und Gesundheitssektor)…

N=700 IT Professionals, 2019.

WAHRGENOMMENE RISIKEN BEI NUTZUNG VON PUBLIC CLOUDS

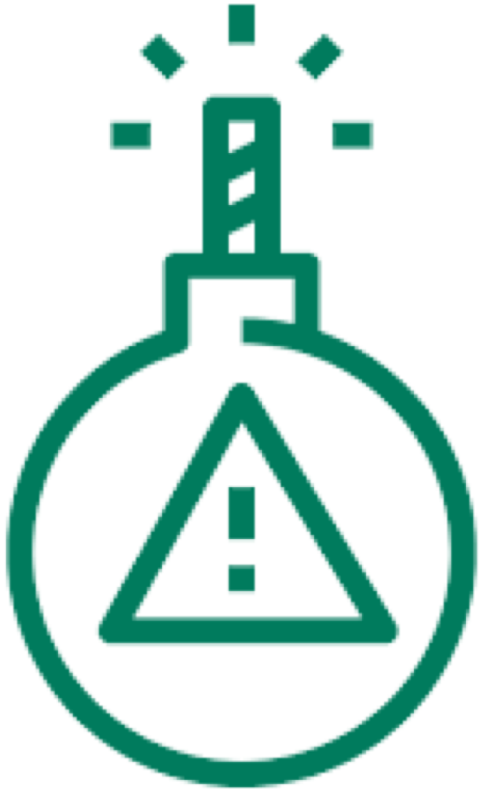


- Cloud-Anwender ggf. kein Zugriff auf Protokollierung und Dokumentation
- Unübersichtlichkeit durch Datenablage an diversen Standorten, weltweit verteilt und fragmentiert
- Keine Individualisierung von Sicherheitsanforderungen möglich
- Transparenz der Datenhaltung gefährdet
- Trennbarkeit?

N=700 IT Professionals, Mehrfachnennungen möglich, 2019.

RELEVANTE BEDROHUNGEN BEI DER CLOUD-NUTZUNG (1/2)

1. Datenlecks
2. Miskonfiguration und keine angemessenen Change Prozesse
3. Fehlende Cloud Security Architektur und Cloud- Strategie
4. Unzureichendes Identitäts-, Passwort-, Schlüssel- und Zugangsmanagement
5. Account Hijacking
6. Bedrohung durch Insider



RELEVANTE BEDROHUNGEN BEI DER CLOUD-NUTZUNG (2/2)

7. Unsichere Interfaces und APIs
8. Ungenügende Kontroll- und Monitoringsysteme
9. Unangemessene Metastructure und Applistructure
10. Begrenzte Sichtbarkeit und Transparenz bei der Cloud-Nutzung
11. Missbräuchliche Nutzung der Cloud Services

…UND TROTZDEM: CLOUD IST SICHERER ALS JEDES RECHENZENTRUM?!

Denn:

- (Große) Cloudanbieter haben die sicherste Infrastruktur – weltweite Absorption von Cloud-Spezialisten
- Lecks entstehen durch Fehlkonfiguration, nicht durch die Cloud an sich → Menschen und Kompetenzen erforderlich

Aber:

- Herkömmliche Sicherheitsmethoden und -werkzeuge sind für die Cloud nicht geeignet
- Alles ist softwarebasiert! („security as code“) → neues Verständnis für Betrieb erforderlich
- So viel wie möglich automatisieren → „Manuell“ wird immer zu langsam sein
- Auch andere Anbieter haben „schöne Services“ → sorgfältiges Sourcing erforderlich

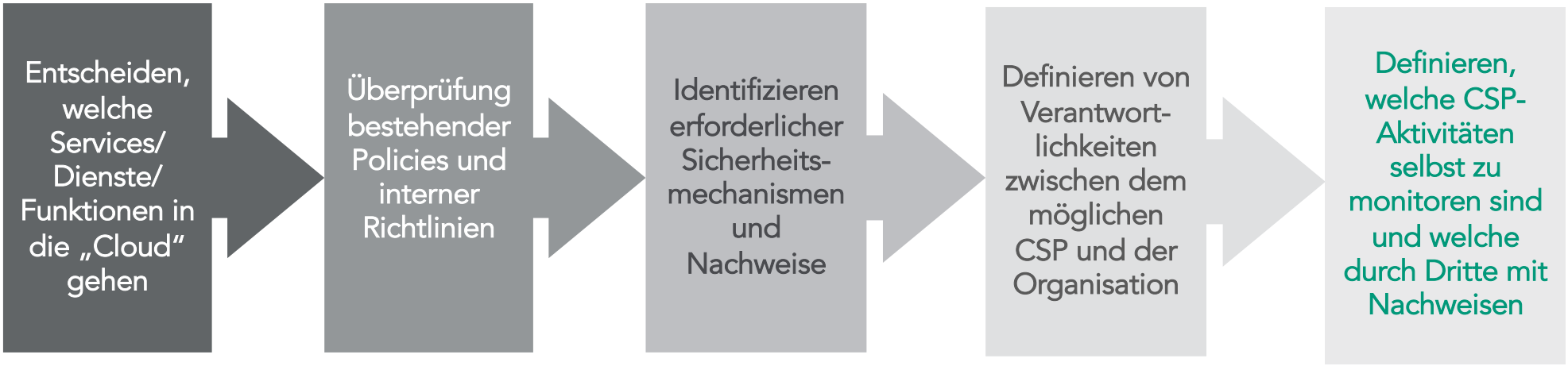
WAS TUN? EINFACH TOM – TECHNISCH-ORGANISATORISCHE MASSNAHMEN AUF CLOUD ANPASSEN?

Zur Illustration

- **Vertraulichkeit:** Einschränkung von Leserechten, Protokollierung lesender Zugriffe, (Ende-zu-Ende-)Verschlüsselung der Daten, Verschwiegenheitsvereinbarungen
- **Integrität:** Einschränkung von Schreib- und Änderungsrechten, Protokollierung von schreibenden/ändernden Zugriffen und geänderten Daten, Nachberichtigung, technische Integritätskontrollen, Audits, Schutz vor Schadsoftware, Benutzerkonzepte
- **Verfügbarkeit:** Einschränkung von Lösch-/Veränderungsrechten, Schutz vor Schadsoftware, Backup von Daten, Software und Konfigurationen, Hardwareredundanz, Vertretungsregeln, Notfallszenarien
- **Verfahren zur Gestaltung, Kontrolle und Evaluation:** ISMS, Incident-Response-Management

Normale Sicherheitskonzepte für Cloud-Services nicht ausreichend…

VORGEHEN: EIGENE CLOUD-EIGNUNG PRÜFEN



Wichtig:
Management, Gesamt-IT-Operations und Compliance einbinden…

VORGEHEN: EIGNUNG DES ANBIETERS PRÜFEN

Anforderungen definieren und beschreiben

Evaluieren und entscheiden, ob der angebotene Service den Anforderungen entspricht

Überprüfen, ob der CSP die erforderlichen Nachweise hat

Verstehen, ob und wie Sicherheits-mechanismen des CSP sichtbar sind und wie sie zu monitoren sind

STANDARDS UND „SCHEMATA“ ALS ORIENTIERUNGSHILFEN

Standard	Akteur	Nachweisart	„Prüfstelle“	Laufzeit/Gültigkeit
IT-Sicherheitsbezogene Schemata				
ISO 27001	Internationale Normungsorganisationen	Zertifikat	Zertifizierte Prüfstelle	3 Jahre, jedoch jährliches Überwachungsaudit
C5	BSI	Testat	Wirtschaftsprüfer	2 Jahre
Trusted Cloud	Kompetenznetzwerk Trusted Cloud e.V.	Label und öffentliche Anbieterliste	Trusted-Cloud-Beirat	
CCM	Cloud Security Alliance	Selbsteinschätzung mit öffentlicher Listung Testat Zertifikat	selbst Wirtschaftsprüfer Zertifizierte Prüfstelle	s.o., bzw. entsprechend der Prüfsysteme
EuroCloud	EuroCloud	Zertifikat	Von EuroCloud akkreditierte Partner	2 Jahre
Datenschutzbezogene Schemata				
TCDP/Auditor	Bundesstiftung Datenschutz	Zertifikat	Zertifizierungsstelle	n.a.
CSA DSGVO Verhaltenskodex	Cloud Security Alliance	Selbsteinschätzung Zertifikat	selbst Zertifizierungsstelle	n.a.

DEEP DIVE: CLOUD CONTROLS MATRIX DER CSA – ORIENTIERUNG FÜR DIE EIGENE SICHERHEIT UND DES PROVIDERS

- Personalmanagement
- Identitäts- und Zugangsmanagement
- Sicherheit von Infrastruktur und Virtualisierung
- Interoperabilität und Portabilität
- Mobile Sicherheit
- Sicherheitsvorfallmanagement, E-Discovery und Cloud-Forensik
- Lieferkettenmanagement, Transparenz und Rechenschaftspflicht
- Bedrohungs- und Schwachstellenmanagement

DEEP DIVE: CLOUD CONTROLS MATRIX DER CSA – ORIENTIERUNG FÜR DIE EIGENE SICHERHEIT UND DES PROVIDERS

- Anwendungs- und Schnittstellensicherheit
- Gewährleistung und Befolgung von Auditauflagen
- Geschäftskontinuitätsmanagement und betriebliche Belastbarkeit
- Änderungskontroll- und Konfigurationsmanagement
- Datensicherheits- und Informationslebenszyklus-Management
- Sicherheit von Rechenzentren
- Verschlüsselung und Schlüsselmanagement
- Governance und Risikomanagement

THERE IS NO HALFWAY HOUSE? – LET YOUR APPS AND DATA OUT OF THE CAGE?

1. **Ganz oder gar nicht:** Cloud first!-Strategie braucht Commitment und entsprechende Ressourcen
2. **Spitz rechnen:** Kostenvergleiche unter Berücksichtigung aller Kosten für den „IT-Betrieb“
3. **Komplexer als vorher:** Cloud-Fähigkeit von Applikationen prüfen, und ob Daten so integriert sind, dass sie nur schwer „trennbar“ sind
4. **Kein Mut zur Lücke:** Einschätzung der Sicherheit und Governance des „Cloud-Betriebs“
5. **Cloud ist schnell:** bisherige Reaktionszeiten und „Change“-Abläufe cloud-gerecht verändern

KONTAKT

Heidrun Müller

Senior Researcher and Consultant

heidrun.mueller(at)egovcd.de

+49 (0)172 59 44 067

www.egovcd.de

UNSERE WHITEPAPER-REIHE – KOMPAKTES WISSEN

Einfach QR-Code scannen und Einzelpaper oder Bundle entdecken.
http://bit.ly/main-sales-eGovCD