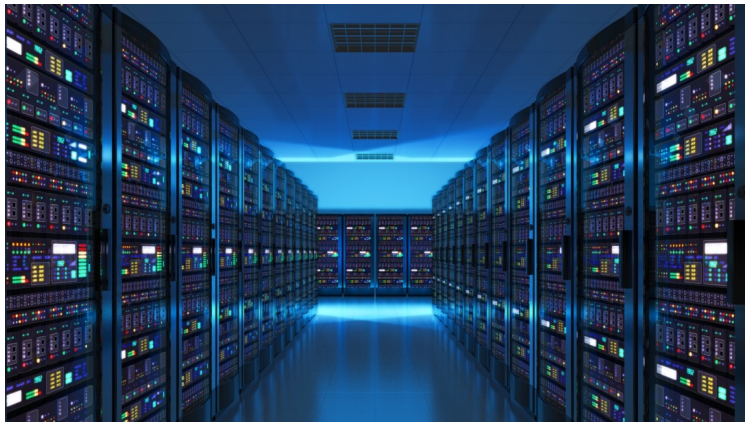
CLOUD MIGRATION



Strategie

Organisation

Regulatorik

Technik

Referenten:

Jens Borchers, cat out

Marina Doehling, cat out

Webinar am 9. November 2022

cat out

CAT OUT – IT UNTERNEHMENSBERATUNG

- ganzheitlich unter technischen, organisatorischen und rechtlichen Aspekten
- heterogene Systemlandschaften von Mainframe bis Cloud
- Branchenübergreifend
  - Handel, Logistik, Banking und Finance, Industrie, Telekommunikation
- Themenauszug: Digitalisierung, Transformation, Migration, Qualitätssicherung, User Management, Daten Management, Integration, Software Development

CAT OUT - WAS WIR MACHEN

- Wir beraten Sie individuell, ganzheitlich oder in Teilgebieten zu den Themen
- Wir identifizieren mit Ihnen die notwendigen Maßnahmen und Prioritäten
- Wir übernehmen die Projektleitung und Dienstleistersteuerung
- Wir realisieren gemeinsam mit Ihnen die Umsetzung der Projekte
- Wir unterstützen Sie beim Aufbau und Ergänzung passender Projekt-Teams
- Wir arbeiten mit Experten und Dienstleistern aus unserem Partner-Netzwerk mit Spezial-Knowhow

AGENDA

1|Welches Ziel will ich erreichen, welche Optionen habe ich, wie gehe ich vor?

2|Welche Cloud-Optionen habe ich und was muss ich beachten?

3|Welche regulatorischen Rahmenbedingungen sind zu berücksichtigen

4|Welche Migrations-Optionen habe ich?

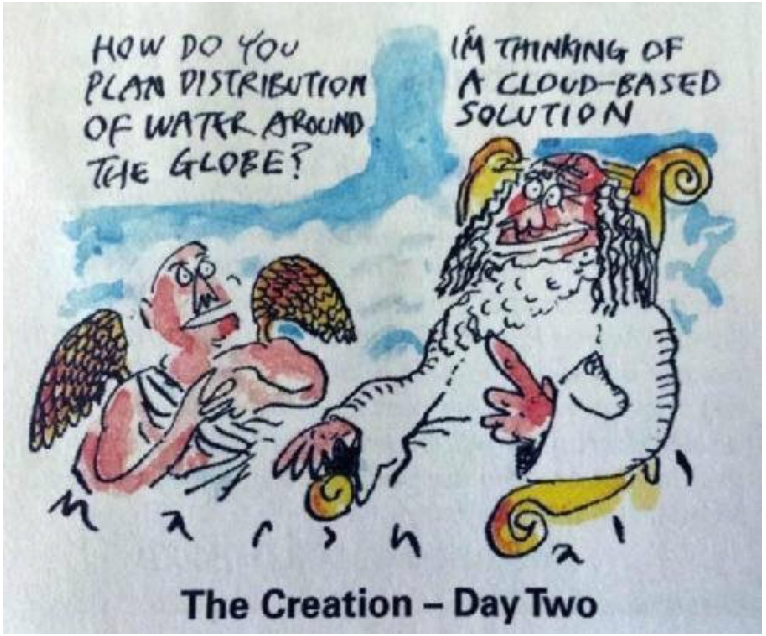
5|Wie sieht der Betrieb einer hybriden On-Premise und Multi-Cloud-Umgebung aus?

CLOUD-STRATEGIE

STRATEGISCHE ANSÄTZE – ZIELE UND TREIBER FÜR DEN CLOUD-EINSATZ

- „Wir gehen jetzt in die Cloud“ ….
  - Welche Ziele haben wir?
  - Welche Randbedingungen haben wir?
  - Welche Optionen gibt es?
  - Wie gehen wir am besten vor?

- Und was ist überhaupt „**die** Cloud“, in die wir uns bewegen wollen?
  - Und ist es tatsächlich nur eine – oder vielleicht diverse parallel?
  - Und was bleibt physisch im Haus – also „on premise“?



CLOUD ALS ALTERNATIVE ZUM EIGENEM DATACENTER
STRATEGISCHE ANSÄTZE – ZIELE UND TREIBER FÜR DEN CLOUD-EINSATZ

- Cloud-Einsatz – wesentlicher Teil einer unternehmensweiten Digital- und IT-Strategie
- Treiber einer Cloud-Strategie sind klassisch
  - Kostenvorteile (aber Vorsicht, auch Cloud ist nicht per se „billig(er)“)
  - Flexibilität (neue/geänderte Anforderungen)
  - Skalierbarkeit („Abdeckung von Spitzen“)
  - Sicherheit (User Management, Virenabwehr, Firewalls, Data Leak Prevention)
  - Mitarbeiterverfügbarkeit, Fachkräfte-Einsatz, Abdeckung 7x24-Services
  - Infrastruktur (Anforderungen an Data Center werden immer höher)

CLOUD ALS ALTERNATIVE ZUM EIGENEM DATACENTER
STRATEGISCHE ANSÄTZE – RAHMENBEDINGUNGEN FÜR DEN CLOUD-EINSATZ

- Bevor man sich eine Cloud-Strategie baut, benötigt man den **aktuellen** Stand zu:
  - Anwendungslandschaft und Architektur
    - Schnittstellen zwischen den Anwendungen und nach Außen!
  - Infrastruktur
    - Unternehmensstandorte
    - Rechenzentren
    - Lebenszyklus-Status der einzelnen Hardware-/Software-Komponenten
    - Datenarchitektur und Datenmengen
    - Kommunikation mit externen Partnern
  - Verträge mit Lieferanten und Service-Providern
  - Gesetze und Regulatorik
    - Welche davon sind zutreffend?

CLOUD ALS ALTERNATIVE ZUM EIGENEM DATACENTER
STRATEGISCHE ANSÄTZE – ROADMAP FÜR CLOUD-EINSATZ

- Die Cloud-Strategie sollte berücksichtigen:
  - Stakeholder / Sponsoren / Stellung der Fachbereiche
  - Priorisierung der Anwendungen
    - Womit fangen wir an?
    - Womit schaffen wir Vertrauen in den grundlegenden Ansatz?
  - Cloud Readiness Analyse
    - Wie sieht unsere Fähigkeit zur Umsetzung aus?
    - Haben wir schon Erfahrung mit der Auslagerung von IT-Services?
  - Grundsätzlicher Migrationsansatz
    - Teilmigration
    - Vollmigration
  - Erster (grober) Migrationsplan

CLOUD COMPUTING
CLOUD OPTIONEN – TECHNISCHE ASPEKTE

- Welche Cloud-Optionen gibt es überhaupt?
- Wie sehr verändern sie einen bestehenden on-premise-Ansatz?
- Wie viele Clouds benötigen wir?
  - Eine für alles? (Der Liebling der Anbieter, aber neuer Vendor-Lock-in?)
  - Eine pro Anwendung? (Der „Organisationswahnsinn“)
  - ⇨ I.d.R. mehr als eine, aber so wenige wie möglich (Der pragmatische Ansatz)

CLOUD COMPUTING

DEFINITION LAUT NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOY) - 2011

- Cloud Computing ist ein Modell für den On-Demand-Netzwerkzugriff auf einen gemeinsam genutzten Pool konfigurierbarer Computerressourcen (z. B. Netzwerke, Server, Speicher, Anwendungen und Dienste), die mit minimalem Verwaltungsaufwand oder Interaktion mit dem Dienstanbieter schnell bereitgestellt werden können.

Merkmale

- **On-demand self-service** – automatische Bereitstellung der Ressourcen
- **Broad Network Access** – durch Standardmechanismen für heterogene Plattformen
- **Resource Pooling** – Multi-Tenant Modell, dynamische Zuweisung der Ressourcen
- **Rapid Elasticity** **-** elastische, schnelle ggf. automatische Bereitstellung der Services
- **Measured Services** - automatisierte Überwachung und Optimierung der Resourcen

ABGRENZUNG KLASSISCHES IT OUTSOURCING - CLOUD COMPUTING
VERTRAGLICHE UND RECHTLICHE ASPEKTE

- Merkmale des klassischen IT-Outsourcings
  - Komplette gemietete Infrastruktur exklusiv für Kunden – Single Tenant Architektur
  - Verträge über längere Laufzeiten mit eingeschränkter Flexibilität
  - Arbeits-, Produktions- oder Geschäftsprozesse werden ausgelagert
  - Ggf. Transfer von Mitarbeitern („Arbeitnehmer-Übernahme“ nach §613a BGB)
- In Teilen entsprechen Cloud-Services dem klassischen IT-Outsourcing – es gibt aber Unterschiede
  - Nutzung von fremder Infrastruktur – Multi-Tenant Modell, skalierbare Ressourcen - Pay per Use Model
  - Optimierung der Ressourcen auch über mehrere Standorte oder Cloud-Anbieter
  - Steuerung der Cloud Dienste i.d.R. durch den Kunden selbstständig
  - Administration über Weboberfläche oder Schnittstellen
  - Wenig(er) persönliche Interaktion mit dem Provider

CLOUD COMPUTING
BEREITSTELLUNGS-MODELLE UND KOMBINATIONEN

- **Private Cloud -** Infrastruktur wird zur ausschließlichen Nutzung einer einzigen Institution betrieben, kann von Ihr selbst oder einem Dritten geführt werden.
- **Community Cloud** – eine mandanten-fähige Infrastruktur, die von einer Gruppe von Institutionen mit den gleichen Anforderungen gemeinsam genutzt wird.
- **Public Cloud** – Infrastruktur wird für die offene Nutzung durch die Allgemeinheit oder z.B. einer ganzen Branche von einem Anbieter bereitgestellt.

- **Hybrid Cloud** – Infrastruktur besteht aus zwei oder mehr unterschiedlichen Cloud-Infrastrukturen (private, community oder public), verbunden durch Technologien, standardisierte Schnittstellen, die Daten- und Anwendungsportabilität ermöglichen.
- **Multi Cloud** – Parallele Nutzung mehrerer Cloud-Infrastrukturen gleichen Typs.

CLOUD COMPUTING
SERVICE MODELLE – DIE ALTERNATIVEN

- **IaaS** – Infrastructure as a Service

Bereitstellung von Verarbeitungs-, Speicher-, Netzwerk- u. grundl. Computerressourcen. Der Cloud-Kunde kann beliebige Software darauf einsetzen, Betriebssysteme und Anwendungen, evtl. begrenzte Kontrolle über ausgewählte Netzwerkkomponenten .

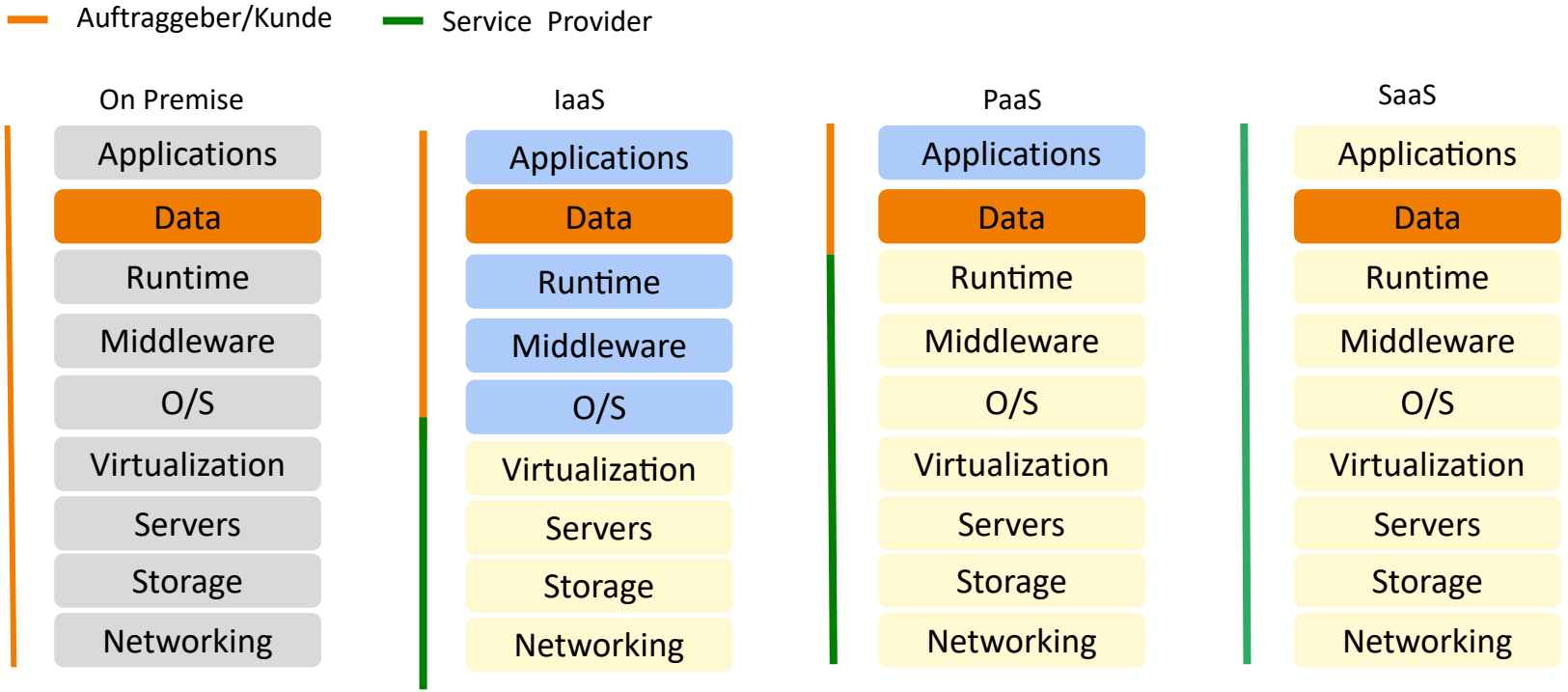
- **PaaS** – Platform as a Service

Komplette Infrastruktur steht bereit mit Ressourcen wie Rechenleistung, Speicher, Netzwerk, Middleware, Load Balancing, Datenbanken, Deployment-Automatismen, Entwicklungsumgebungen für Applikationen. Kein Zugriff auf Betriebssystem.

- **SaaS** – Software as a Service

Bereitstellung von mandantenfähigen Anwendungen, mit Zugriff über verschiedene Client-Geräte. Keine Verwaltung der Cloud-Infrastruktur oder Anwendungen. Ausnahme evtl. benutzerspezifische Anwendungskonfigurationseinstellungen.

VERANTWORTUNGSVERTEILUNG NACH INNEN UND AUSEN
AUFTRAGNEHMER - AUFTRAGGEBER



Verwaltung Auftraggeber / Kunde Verwaltung Auftragnehmer / Provider Eigentum des Auftragsgeber

Kontrollmechanismen: Verantwortlichkeit im Innenverhältnis, Dritten gegenüber bleibt immer der Cloud-Nutzer verantwortlich

BEDROHUNGEN - FÜR CLOUD INFRASTRUKTUR UND DIENST
GEFAHREN BEIM PROVIDER UND BEIM NUTZER

- CLOUD-INFRASTRUKTUR SELBST
- Datenverlust, Informationsabfluss
- Ausfall Internet- oder Netzverbindung
- DoS-Angriff auf Cloud-Anbieter
- Hohe Komplexität – Fehler in der Administration
- Beeinflussung der Nutzer in der public Cloud – Angriffe aus der Cloud selbst

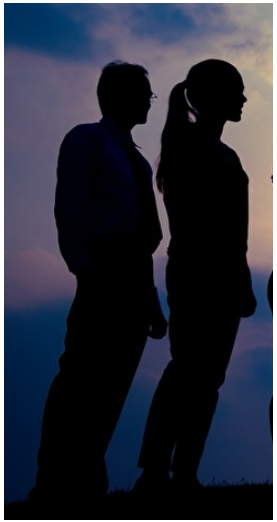
- KUNDEN-NUTZUNG VON CLOUD-DIENSTEN
- Identitätsdiebstahl, Missbrauch von Accounts
- Verlust der Schlüssel für die Daten
- Kontrollverlust über Daten, Anwendungen
- Verletzung von Richtlinien
- Schutz der Endgeräte für Cloud-Nutzung
- Abfangen und Ausspähen des Netz-Traffics

Top-Bedrohungen bei Cloud Computing
CSA Cloud Security Alliance 2022 - in Klammer Ranking 2019

1. Unzureichendes Identitäts-, Berechtigungs-, Zugangs- und Schlüsselmanagement (4)
2. Unsichere Schnittstellen und APIs (7)
3. Fehlkonfiguration und unzureichende Änderungskontrolle (2)
4. Fehlende Cloud-Sicherheitsarchitektur und -strategie (3)
5. Unsichere Software-Entwicklung
6. Ungesicherte Ressourcen von Drittanbietern
7. Systemschwachstellen (8)
8. Unbeabsichtigte Offenlegung von Cloud-Daten
9. Fehlkonfiguration und Ausnutzung von Serverless- und Container-Workloads
10. Organisierte Kriminalität/Hacker/APT (11)
11. Exfiltrierung von Cloud-Speicherdaten

PUBLIC CLOUD – KONTROLLE DER „SCHATTEN-IT“

UNABGESTIMMTE NUTZUNG VON PUBLIC CLOUD-DIENSTEN



Schatten-IT - Verwendung nicht autorisierter Services und Hardware

- sollen schnell Servicelücken ausfüllen
- Beliebt: File-Sharing, z.B. Dropbox, Google Drive, etc.
- Gefährlich für Compliance/Regulatorik: SaaS-Anwendungen

➢ „Sauber“ implementieren / Alternativen anbieten

➢ Bei hoher Gefährdung oder Rechtsproblemen Services abschalten

Risikomanagement erforderlich:

- Sicherheit (Datenabfluss, Eindringen Cyber-Kriminelle)
- Compliance (Privacy Shield)
- DSGVO
- Kosten: Mehrfachanschaffung, Lizenzverletzungen

ANFORDERUNGEN ZUR AUSWAHL VON CLOUD-PROVIDERN
GUTE QUELLEN FÜR DEN EINSTIEG

Orientierungshilfen:

- BSI Anforderungskatalog Cloud Computing C5
- BSI IT Grundschutz - Kompendium
- ISO 270xx -> speziell ISO 27018
- ECSA – EuroCloud StarAudit, Certification for Cloud Services
- Cloud Security Alliance (CSA) Security, Test & Assurance Registry (STAR): STAR Self Assess- ment, STAR Certification, STAR Attestation, C-STAR Assessment
- Kompetenznetzwerk Trusted Cloud e.V. (BMWi) – Label Trusted Cloud

GESETZLICHE REGELUNGEN UND REGULATORIK
DIE GESETZLICHE „BEDROHUNGSLAGE" – AUßEN- UND INNENWIRKUNG

- Der Gesetzgeber unterscheidet grundsätzlich nicht, wie ein Unternehmen seine Informationsverarbeitung technisch und organisatorisch betreibt.

- Es gelten die üblichen Gesetze
  - EU-DSGVO + (nachgeordnet) BDSG neu
  - EU Cybersecurity Act 2019/881 (die ENISA existiert seit 2004)
  - EU-Richtlinie 2016/943 + Geheimnisschutz-Gesetz (GeschGehG)
  - IT-Sicherheitsgesetz
  - BGB und HGB und darauf basierende Regelwerke
    - z.B. GOBD, AO
  - Strafrecht, z.B.
    - § 202a StGB – Ausspähen von Daten
    - § 303b StGB – Computersabotage

GESETZLICHE REGELUNGEN UND REGULATORIK
DIE GESETZLICHE „BEDROHUNGSLAGE" – IT-SICHERHEITSGESETZ 2.0

- IT-Sicherheitsgesetz neuer Stand
  - Ursprünglich aus 2009 („BSI-Gesetz"), Ausweitung 2015 („KRITIS"), Novellierung 2021
  - **IT-SiG 2.0** ist seit 07.05.2021 – trotz vieler Bedenken – verabschiedet
- Auswirkungen IT-SiG 2.0
  - Deutliche Ausweitungen der Kompetenzen des BSI
    - „Nebeneffekt": ca. 800 neue Stellen -> 75 - 100 Mio. EUR Mehrkosten (Personal/Sach-) p.a.
  - Gilt nun für noch mehr Unternehmen als bisher (neu: „Unternehmen im besonderen öffentlichen Interesse")
  - BSI hat mehr Einblicksrechte in technische Umgebung/Infrastruktur der Unternehmen
    - Sogar „Hacker-Methoden" dürfen vom BSI genutzt werden
- Basis bleiben die bekannten BSI-Standards und der IT-Grundschutzkatalog
  - BSI-Standards 200-1 (ISMS) bis 200-4 (BCMS)

GESETZLICHE REGELUNGEN UND REGULATORIK
DIE GESETZLICHE „BEDROHUNGSLAGE" – AUSEN- UND INNENWIRKUNG

- Seit Mai 2018 endgültig nicht mehr ignorierbar
  - EU-Verordnung 2016/679: Daten-Schutz-Grund-Verordnung (EU-DSGVO)
    - **Das** große Thema in vielen Unternehmen seit Mitte 2017 und noch bis heute
    - Erfordert(e) wesentliche Anpassungen an Organisation und Technik, enthält auch Anforderungen an IT-Security („TOM", Art. 25)
- Etwas "untergegangen", aber seit Juni 2018 ähnlich wichtig
  - EU-Richtlinie 2016/943: Schutz von Know-how und Geschäftsgeheimnissen
    - Ende der Übergangsfrist war 08.06.2018, Gesetz in D erst 26.04.2019 in Kraft
    - „Gesetz zum Schutz von Geschäftsgeheimnissen" (GeschGehG)
    - „Geschäftsgeheimnis" neuer Oberbegriff für Betriebsgeheimnis, Geschäftsgeheimnis, Know-how, wesentliches internes Wissen,…

GESETZE, REGULATORIK UND STANDARDS
VORGABEN DES GESETZGEBERS ZUM DATENSCHUTZ

- EU-DSGVO seit 05/2018:
  - Artikel 25: Datenschutz durch technische und organisatorische Maßnahmen
  - Artikel 28: Auftragsverarbeitung
  - Artikel 32: Sicherheit der Verarbeitung
    - Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit
  - Artikel 35: Datenschutzfolgeabschätzungen
  - Artikel 42: Zertifizierung der implementierten Maßnahmen
    - Nachweis zwar „freiwillig“, aber im Datenschutzverletzungsfall sicherlich hilfreich

GESETZE, REGULATORIK UND STANDARDS
DSGVO ET AL - WAS IST RELEVANT FÜR CLOUD-SERVICES?

- Bei zusätzlicher Nutzung von Cloud-Services
  - durch (tlw.) Verlagerung des eigenen Data Centers („Cloud-Migration“)
  - durch Einführung neuer Funktionen direkt auf Cloud-Basis

  sind alle vorhandenen Datenschutz- und Security-Funktionen zu überprüfen und anzupassen
  - Datenschutzfolgeabschätzungen nach DSGVO Art. 35 werden kritischer
- Bei vorhandener Zertifizierung nach ISO 27001 / BSI IT-Grundschutz
  - Überprüfung bzgl. ISO 27018 erforderlich
  - BSI-Grundschutzkatalog „OPS.2.2 Cloud-Nutzung“ muss abgedeckt werden
  - BSI-Handbuch „Anforderungskatalog Cloud Computing (C5)“

GESETZE, REGULATORIK UND STANDARDS
INTERNATIONALE UND NATIONALE GREMIEN ZUR STANDARDISIERUNG

- ISO/IEC 2700x – international anerkannter Standard zur Implementierung eines ISMS
  - Zertifizierung nach ISO/IEC 27001 in vielen Bereichen heute Standard
  - ISO/IEC 27001:2017 – Aufbau und Wartung eines ISMS
    - Plan-Do-Check-Act-Ansatz: Konzept, Implementierung, Überprüfung, Optimierung
- IT-Grundschutz (BSI)
  - Umsetzung des IT-Sicherheitsgesetzes (BSIG) durch entsprechende Standards (200-1 bis 200-*4*) und diverse Handlungsempfehlungen
  - ISO 27001-Zertifizierung auf Basis von BSI-Standard- und -Kernabsicherung
- Weitere Standards der Wirtschaftsprüfer
  - AICPA American Institute of CPAs® SOCx
  - IDW PS330 / RS FAIT

GESETZE, REGULATORIK UND STANDARDS
WAS DAVON IST RELEVANT FÜR CLOUD-SERVICES?

- Was ist davon Cloud-relevant?
  - Einfache Antwort: **Grundsätzlich alles**!
- Cloud-Services gelten als (wesentliche) Auslagerung
  - Vertraglich abzusichern sind wie in jedem Outsourcing-Vertrag:
    - Genaue Verteilung der Aufgaben und Verantwortlichkeiten zwischen Nutzer und Provider (je nach Service-Modell IaaS, PaaS, SaaS)
    - Sicherstellung der Einhaltung aller Gesetze und Standards beim Provider mit periodischen Nachweisen und externen Bestätigungen
    - Audit-Möglichkeiten des Kunden beim Provider
- Gegenüber den Kunden und Behörden bleibt der Cloud-Nutzer weiterhin juristisch Verantwortlicher insbesondere bei Datenschutzverletzungen

MIGRATIONS-OPTIONEN

WIE BRINGT MAN BESTEHENDE ANWENDUNGEN IN „DIE CLOUD“?

- Auf Basis des bestehenden Anwendungskatalogs entscheiden:
  - Anwendung wird nicht mehr benötigt, kann „weg“
    - Billigste Alternative
    - Aber Achtung: Rechtliche Archivierungsregeln nicht vergessen
  - „Lift and Shift“ – möglichst ohne Änderungen in Cloud-Umgebung verlagern
    - aka „Re-Hosting“
  - „Re-Platforming“: Auf neuer technischer Basis in Cloud re-implementieren
    - Z.B. Datenbank, andere Middleware-Komponenten
  - Anwendung durch Standardsoftware ersetzen / „SaaS“-Lösung statt on-premise
  - Kompletter Neuaufbau mit Cloud-Architektur und -Entwicklungsmethoden
    - „Cloud native“
    - „Low code“, „Citizen Developer“

MIGRATIONS-THEMEN
WIE BETREIBT MAN EINE MULTI-CLOUD-UMGEBUNG?

- Betriebsaspekte einer hybriden On-premise / reinen (Multi-) Cloud-Umgebung
  - Welche Funktionen müssen auf jeden Fall im Unternehmen bleiben
  - Wer steuert die Gesamtumgebung
    - Technisch
    - Organisatorisch
    - Compliance/Governance
  - Wie sieht das zentrale User Help Desk aus?
    - Welche Kompetenzen werden dort benötigt?
    - Wie sieht second/third level Support bzgl. der einzelnen Services aus?
  - User Management
    - Onboarding (in den notwendigen Anwendungen)
    - Offboarding (was muss in welchen Clouds gelöscht werden oder sogar erhalten bleiben?

AUSBLICK

Themen weiterer Webinare zum Thema Cloud Migration

1. Access Management – IAM und CIAM –Voraussetzung für sichere Cloud-Nutzung
   am 07.12.2022, 14.00 – 15.00 Uhr

2. Cloud-Migration - Projektstart, Projektbeteiligte, Organisation, Vertragsgestaltung
   In Planung für Anfang 2023

3. Weitere in Planung

KONTAKT

cat out

Dipl.-Betriebsw. Marina Döhling
Executive Consultant

M. +49 (0) 172 43 00 429
marina.doehling@cat-out.com

cat out

Dipl.-Math. Jens Borchers
Executive Consultant

M. +49 (0) 174 88 99 675
jens.borchers@cat-out.com

cat out gmbh
info@cat-out.com
www.cat-out.com