carmasec

security. done. right.

Das „Shared Responsibility Model“ in der Praxis

CCX2021 – Cloud Computing Conference

14.09.2021, Carsten Marmulla

CCX2021: Das „Shared Responsibility Model“ in der Praxis

Referent: Carsten Marmulla

Carsten Marmulla
Managing Partner &
Senior Trusted Advisor
carmasec GmbH & Co. KG

Profile im Netz:

- linkedin.marmulla.net
- xing.marmulla.net
- twitter.marmulla.net

Projekt- und Themenschwerpunkte (Auszug):

- IT-GRC: IT-Governance, IT-Risikomanagement, IT-Compliance (inkl. Datenschutz); Informationssicherheitsmanagement (ISO 27001, BSI IT-Grundschutz, ISIS12), IT-Servicemanagement gemäß ITIL v3
- Risikoanalysen/Sicherheitskonzepte/Informationssicherheitsrichtlinien, Schutzbedarfsfeststellungen
- Organisatorische Reifegradermittlung; Durchführung von Schwachstellen-/ Risiko- und Business Impact Analysen (BIA); Identifizierung und Steuerung der Maßnahmen
- Konzeption, Aufbau und Einführung von Managementsystemen für Informationssicherheit gemäß ISO 27001 und Zertifizierungsvorbereitung; Konzeption und Implementierung von Kennzahlensystemen (KPI)
- Optimierung der IT-Wertschöpfung im Rahmen der IT-Governance (COBIT); Überprüfung der Einhaltung der IT-Compliance und der Datenschutzanforderungen

Harte Fakten:

- > 20 Jahre IT-Branchenerfahrung (Projektmanagement- und IT-Beratungserfahrung)
- Zertifizierungen: Certified Information Security Manager (CISM), ITIL v3, ISO 27001 Auditor (ISMS), ISIS12, COBIT-Practitioner, PRINCE2-Practitioner

Agenda

- Themeneinführung: „Shared Responsibility Model“
  - Überblick Service- & Delivery-Modelle
  - Sicherheits- und Compliance-Anforderungen
  - „Security of the cloud“ vs. „Security in the cloud“
  - Integration ins Risikomanagement
- Praxisbeispiele: „Ist die Cloud sicher?“
- Diskussion, Fragen & Antworten

Teilnehmerumfrage: Shared Responsibility

carmasec

Kennen Sie das „Shared Responsibility Model“ und wenden Sie es bereits für Ihre ausgelagerten IT-Komponenten an?

A: Ist nicht bekannt

B: Ist bekannt, aber nicht in Anwendung

C: Ist bekannt und bereits in Anwendung

Themeneinführung

- „Shared Responsibility“ ist ein Modell zur Abbildung von gemeinsamen bzw. geteilten Verantwortlichkeiten in komplexen IT-Umgebungen
- Insbesondere bei Nutzung von Cloud-Dienstleistungen kommt das „Shared Responsibility Model“ bei nahezu jedem Cloud Service Provider zum Einsatz
- Ein Verständnis des Modells und das Bewusstsein über die eigenen und fremden Verantwortlichkeiten ist essentiell für die korrekte Umsetzung von Sicherheits- und Compliance-Anforderungen

„With great power
comes great responsibility.”

—

Stan Lee

Übersicht Service-Modelle

carmasec

- Bei der Nutzung von Cloud-Service-Modellen unterscheidet man grundsätzlich mindestens drei Kategorien:
  - Infrastructure as a service (IaaS)
  - Platform as a service (PaaS)
  - Software as a service (SaaS)
- Die Einordnung in eine oder mehrere Kategorien (je nach Komplexität der Infrastruktur) ist für die Zuordnung von Verantwortlichkeiten zwischen Cloud-Betreiber und Cloud-Nutzer elementar wichtig

Sicherheits- und Compliance-Anforderungen

carmasec

- Bedrohungslage: Zunehmende Cyberangriffe auf Unternehmen bspw. durch gezielte Datenabflüsse oder Ransomware-Attacken
- Regulatorische Anforderungen durch den Gesetzgeber werden strenger und/oder komplexer
- Datenschutzanforderungen zum Schutz von (sensiblen) personenbezogenen Daten sind gestiegen
- Kunden- und/oder Zuliefererанforderungen sind oftmals ebenfalls Auslöser
- Wirksamkeitsprüfungen und Kontrollen müssen regelmäßig durchgeführt werden

Teilnehmerumfrage: Shared Responsibility

carmasec

Wer ist für die Erfüllung von Sicherheits- und Compliance-Anforderung bei ausgelagerten IT-Komponenten verantwortlich?

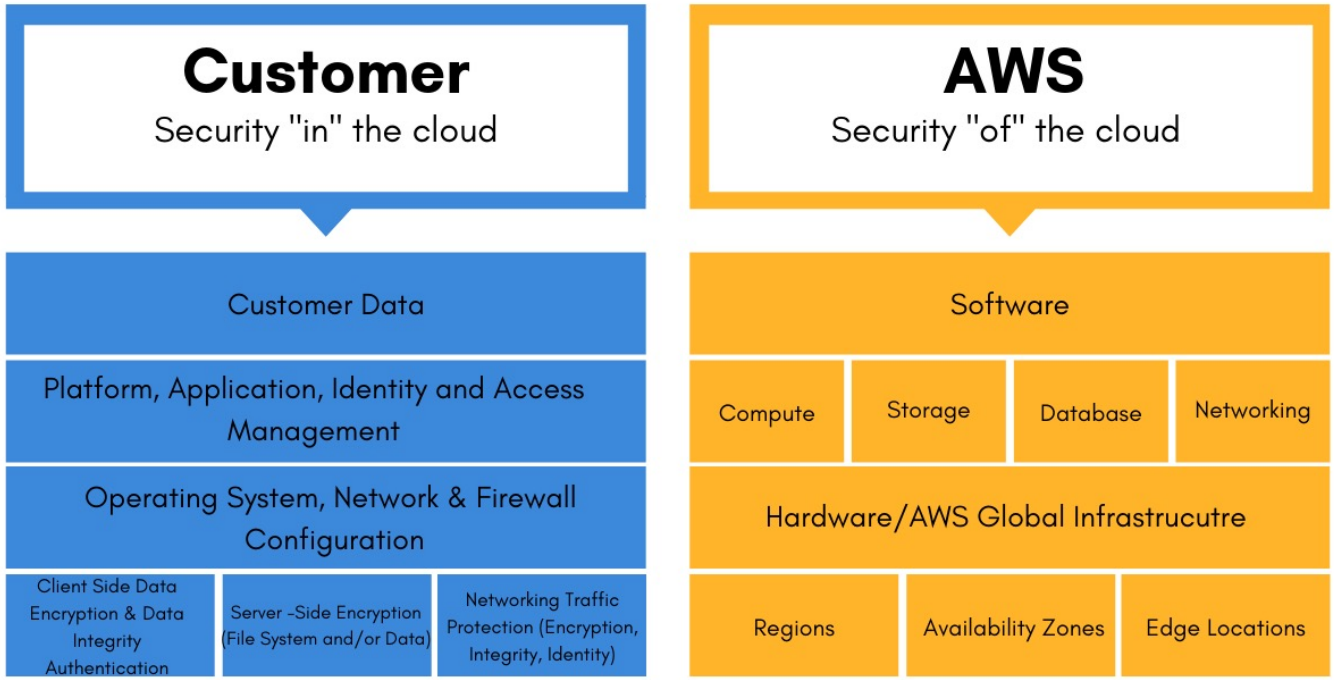
A: Ausschließlich der Betriebsdienstleister

B: Ausschließlich der Auftraggeber

C: Beide, abhängig vom Service-Modell für unterschiedliche Ebenen und Komponenten der verwendeten Infrastruktur

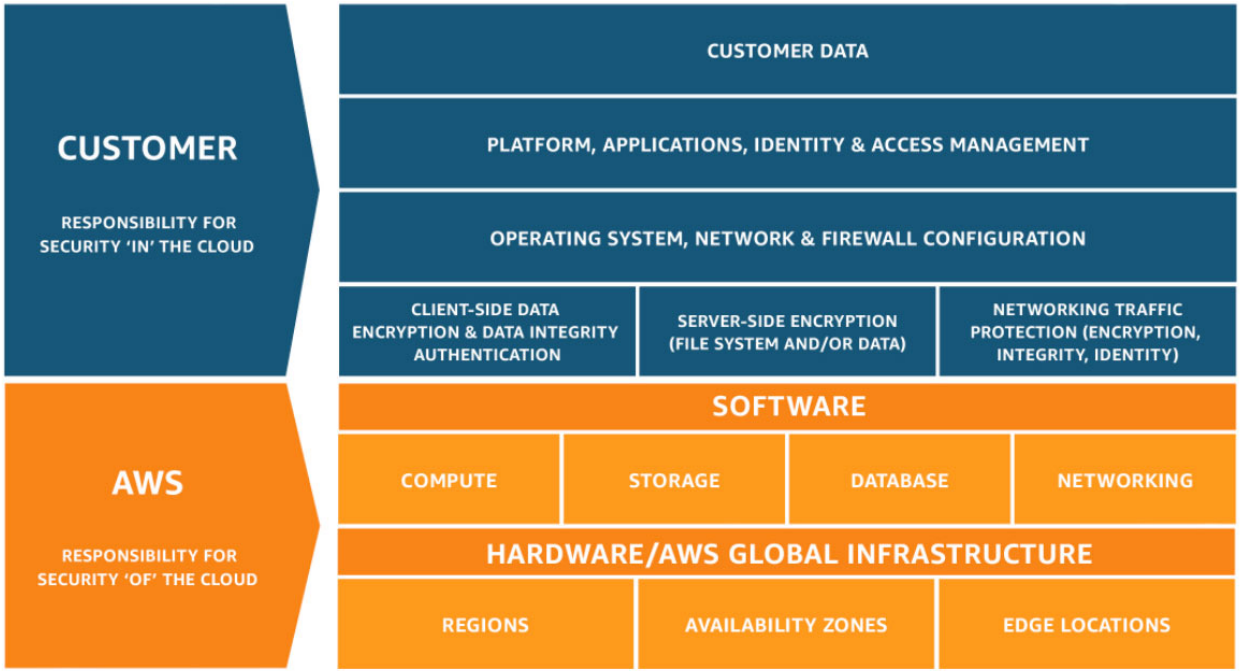
Security „in“ or „of“ the cloud?

carmasec



Security „in“ or „of“ the cloud?

carmasec



CCX2021: Das „Shared Responsibility Model“ in der Praxis

Matrix: „Shared Responsibility Model“

carmasec

Integration ins Risikomanagement

carmasec

- Dokumentation der gemeinsamen/geteilten Verantwortung: so detailliert wie möglich – bspw. auf Ebene von Geschäfts-/IT-Prozessen
- Grundverständnis: Delegation von Aufgaben vs. Delegation von Verantwortung
- Definition von Service Level Agreements zwischen Auftraggeber und Dienstleister/Betreiber
- Gemeinsames Verständnis zu Haftungsfragen bei Service-Einschränkungen oder Minder-/Mängelleistungen

„Technology trust is a good thing,
but control is a better one.”

—

Stephane Nappo

carmasec

Praxisbeispiele: Ist die Cloud sicher?

Wie kann ich das prüfen?

Praxisbeispiele: Operative IT-Prozesse

carmasec

- Patch Management
- Datensicherung (und -wiederherstellung)
- Verschlüsselung, Schlüsselmanagement
- Daten-Anonymisierung/Pseudonymisierung
- Zugriffs- & Berechtigungsmanagement
- Sicherheitsüberprüfungen (z.B. Penetrationstests)
- ...

Praxisbeispiele: Organisatorische Themen

carmasec

- Audit-Berichte, Audit-Trail & Evidenzkette
- Kontrollaudits
- Sicherheitsüberprüfungen (z.B. Risk Assessments)
- Auskunftspflichten
- Meldepflichten
- ...

Teilnehmerumfrage: Audit & Kontrolle

carmasec

Prüfen und kontrollieren Sie regelmäßig den Betriebsdienstleister für Ihre ausgelagerten IT-Komponenten hinsichtlich erfüllter Sicherheits- und Compliance-Anforderungen?

A: Nein, wir führen gar keine Überprüfung durch

B: Wir führen nur Stichprobenkontrollen durch

C: Wir prüfen systematisch und regelmäßig

Praxisbeispiele: Was kann schief gehen?

carmasec

- Unklarheiten über Zuständigkeiten & Verantwortlichkeiten
- Lücken im Audit-Trail (Evidenzkette ist unterbrochen)
- Mangelhafte oder fehlende Prüfung der Compliance
- Fehlende Dokumentation im Risikomanagement
- Unkenntnis über umzusetzende Maßnahmen
- Betriebsunterbrechungen
- Haftungsrisiken & Bußgelder

carmasec

Diskussion / Fragen & Antworten

Vielen Dank für die Aufmerksamkeit!

„Security is always too much,
until the day it is not enough.“

—

William H. Webster
(Former Director, FBI)

Quellen & Links

carmasec

- https://cloudsecurityalliance.org/blog/2020/08/26/shared-responsibility-model-explained/
- https://www.cisecurity.org/blog/shared-responsibility-cloud-security-what-you-need-to-know/
- https://aws.amazon.com/de/compliance/shared-responsibility-model/
- https://docs.microsoft.com/de-de/azure/security/fundamentals/shared-responsibility
- https://openvpn.net/blog/shared-responsibility-model/

CCX2021: Das „Shared Responsibility Model“ in der Praxis

Vorstellung carmasec GmbH & Co. KG

Gegründet im Jahr 2018 mit umfassender Expertise aus **über 30 Jahren einschlägiger Beratererfahrung** und **über 100 erfolgreichen Projekt-abschlüssen**.

Leistungsbereiche:
Managementberatung, **Projektmanagement**, **Technologieberatung** in den Themenfeldern Cybersicherheit, Cyber-Resilienz & IT-GRC

Stand- und Einsatzorte:
Essen und **Köln**, deutschlandweite Projekteinsätze bei Großunternehmen und im gehobenen Mittelstand

Branchenkenntnisse (Auszug):
Telekommunikation, Logistik/Transport, Banken/ Versicherungen, Gesundheitswesen, Energie, Informationstechnologie, u.a.

Melden Sie sich für unseren Newsletter an: www.carmasec.com/newsletter

Hauptsitz:
carmasec GmbH & Co. KG
Ruhrallee 185
45136 Essen
Germany

Niederlassung:
carmasec GmbH & Co. KG
Im Mediapark 5
50670 Köln
Germany

Telefon: +49 (0) 201 426 385 900
Fax: +49 (0) 201 426 385 909
Web: www.carmasec.com
Email: contact@carmasec.com