UMSTIEG IN DIE CLOUD... *mit Sicherheit*

TEIL 1 VON 3

Die Verlagerung interner IT-Dienste auf virtuelle Systeme, wie sie beispielsweise von Unternehmen wie Microsoft oder der T-Systems in Form sogenannter „Cloud-Dienste" angeboten werden, haben sich fest am Markt etabliert und einen hohen Reifegrad erlangt. Verfahren und Prozesse gelten mittlerweile aus „ausgereift" und bieten den Unternehmen zahlreiche Vorteile.

Wer interne Server und IT-Infrastruktur betreibt, muss dafür sorgen, dass für alle Anfragen und Aufgaben stets bedarfsgerecht Rechenleistung und Speicherplatz zur Verfügung stehen. Werden Cloud-Services verwendet, kann der aktuelle Bedarf, selbst wenn unerwartet oder sprunghaft, hinzugebucht werden.

Neben einer höheren Skalierbarkeit partizipieren Unternehmen durch die Übernahme zusätzlicher zeit- und arbeitsintensiver Aufgaben wie einer kontinuierlichen Sicherung der Daten und der Aktualisierung von Soft- und Hardware. Der Dienstleister übernimmt auch die permanente „Härtung" von Hard- und Software. So können auch zukünftig immer aktuelle Gefahren über das Internet abgewehrt und Unternehmensdaten gegen Cyber-Angriffe abgesichert werden. Der Wechsel von Diensten und Services in die Cloud und damit die Verschiebung von Verantwortung bietet in punkto Informationssicherheit also Vorteile und sogar viele neue Möglichkeiten zur Verbesserung.

Nicht allen ausgelagerten Services sollte jedoch blind vertraut werden, selbst wenn sie über relevante Zertifizierungen verfügen. Wichtige Punkte müssen im Vorfeld trotzdem untersucht werden, denn es bleibt die essenzielle Aufgabe der eigenen Organisation, sich ausreichend zu schulen und mit verbleibenden Risiken detailliert auseinander zu setzen. Natürlich ist das detaillierte Vorgehen in der Praxis zusätzlich auch individuell auf Unterschiede der unterschiedlichen Cloud-Modelle wie Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) oder Infrastructure-as-a-Service (IaaS) abzubilden.

Dieser Beitrag zeigt aus Sicht der Informationssicherheit einen möglichen Pfad für eine anstehende Auslagerung von Diensten und Services in die Cloud. Der generelle Ablauf wird keine Überraschungen darstellen, ähnelt er doch sehr dem Change und der Untersuchung bei allen neuen Systemen im Unternehmen.

Im ersten Schritt führt der verantwortliche Sicherheitsbeauftragte mit den beteiligten Fachbereichen, der IT und weiteren Verantwortlichen eine gemeinsame Bestandsaufnahme bestehender und neuer Dienste durch. Ein dokumentiertes Anforderungsmanagement ist bei dem Umstieg ein wichtiger Erfolgsfaktor. Zu betrachtende Aspekte sind sowohl technischer als auch organisatorischer Natur und benötigen im Vorfeld ggf. einen „Übersetzer", der beide Aspekte verbindet.

Für jeden zu betrachtendem Dienst könnten die nachfolgenden Aspekte untersucht und bearbeitet werden:

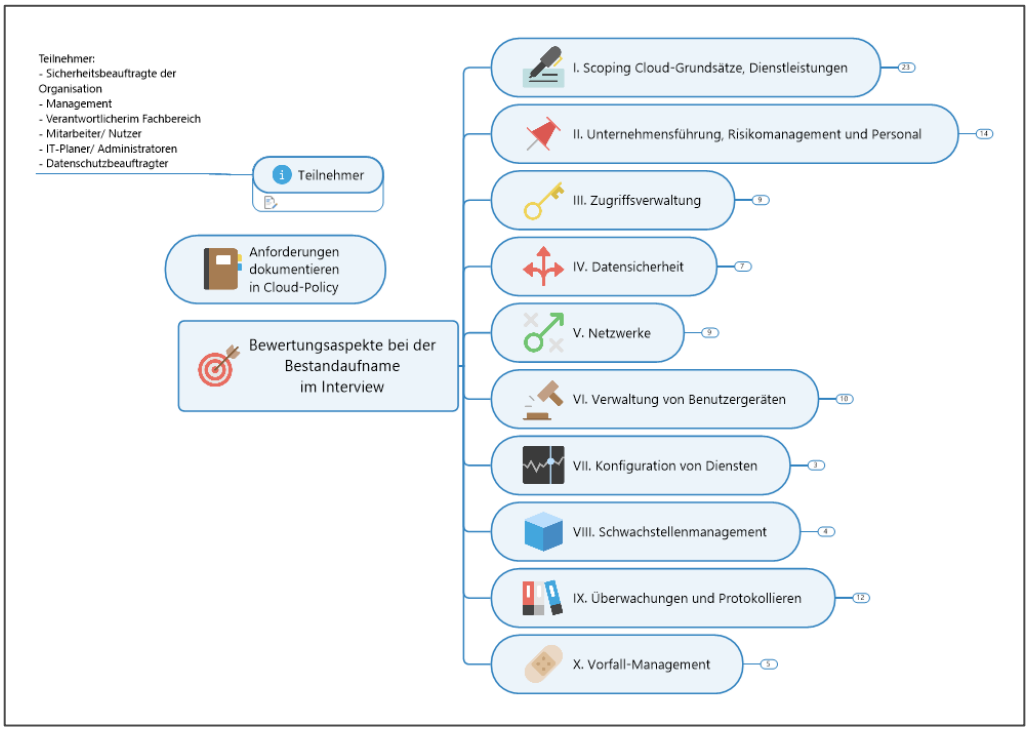

Abbildung 1 Aufnahme der Anforderungen

Ergebnisse, Beiträge der Beteiligten sowie diskutierte und ermittelte Risiken und Chancen sollten bereits unmittelbar in einem dokumentierten Anforderungsmanagement gesammelt und grob zur späteren Aufnahme in eine Cloud-Policy berücksichtigt werden.

Die einzelnen Punkte können in der vorgeschlagenen oder auch einer anderen Reihenfolge bearbeitet werden und werden im Folgenden detaillierter vorgestellt. Neben einer detaillierteren Darstellung der Ziele werden die Bereiche im Anschluss durch mögliche Kontrollfragen ergänzt, die einen sinnvollen und ersten Einstieg in das Thema liefern, jedoch zusätzlich unternehmensspezifisch ergänzt werden müssen.

AUS DEM INHALT

1 SCOPING[1] CLOUD-GRUNDSÄTZE, DIENSTLEISTUNGEN

Die Verantwortung zum Betrieb verbleibt im eigenen Unternehmen und kann nicht vollständig delegiert werden, was dazu führt, dass bei Auslagerung einige Aufgaben in der internen Organisation verbleiben. Diese Aufgaben müssen untersucht und adressiert werden. Daher ist es wichtig, schon im Vorfeld der Analyse immer wieder zu prüfen, welche Verantwortlichkeiten betroffen sind. Die Verantwortlichen sollten in den Prozess mit einbezogen werden. Soweit noch nicht vorhanden, könnte eine Cloud-Policy für die Organisation entstehen, die entsprechend dem hier gezeigten Vorschlag strukturiert werden könnte.

Wie in der Leitlinie auch, so sind zunächst grundsätzliche Aspekte an den Cloud-Dienst zu untersuchen. Diese betreffen organisatorische sowie technische Gesichtspunkte. Schließlich muss der Cloud-Dienst in die definierte Umgebung passen.

Eine weitere Reihe von Anforderungen ergeben sich ggf. durch regulatorische Anforderungen, die ebenfalls mit zu betrachten sind.

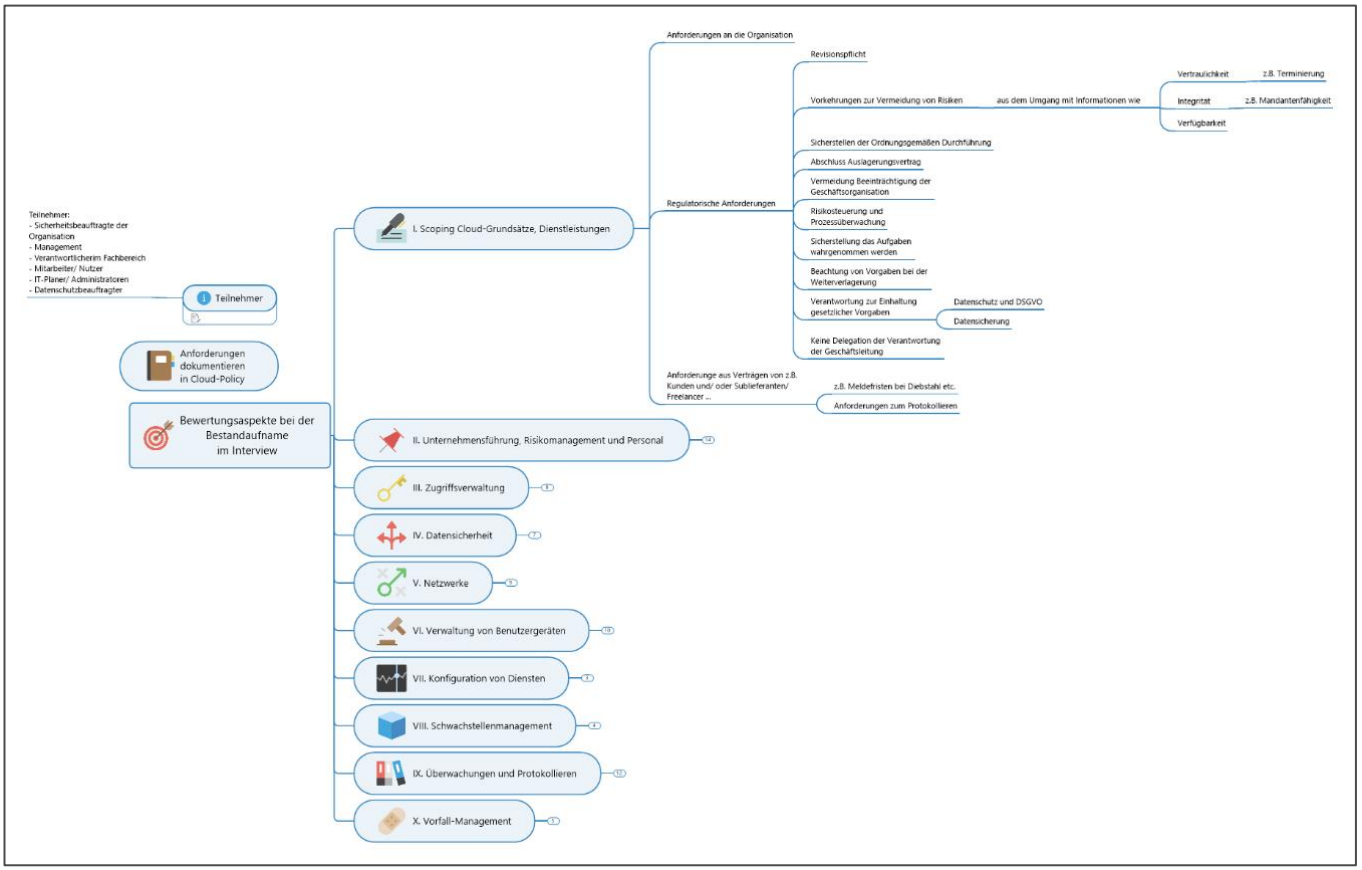

Abbildung 2 Scoping Cloud-Grundsätze und Dienstleistungen

Im Rahmen der Untersuchung ist es sinnvoll, bestehende Abhängigkeiten zu anderen Aspekten zu analysieren und zu dokumentieren. Eine entsprechende Übersicht findet sich ergänzend zum Ende jedes Kapitels.

Mögliche Kontrollfragen können hier sein:

- Passt ein zukünftiger organisationsfremder Betrieb von Diensten / Services in die aktuelle Unternehmensstrategie?
- Sind Aspekte der Informationssicherheit ausreichend verankert und Risiken beherrschbar oder starten wir auf der „grünen Wiese"?
- Welche gesetzlichen / regulatorischen / vertraglichen Anforderungen sind zu erfüllen?
- Welche Anforderungen an Vertraulichkeit / Integrität sowie auch Verfügbarkeit bestehen?
- Passen die Anforderungen auch noch mittel- und langfristig?

[1] ***Scoping*** *ist die Definition von Aufgaben- oder Untersuchungsumfängen in komplexen Planungs-, Management- und Herstellungsprozessen. Das Wort leitet sich aus dem englischen Wort „scope" ab, was die Bedeutungen Umfang, Abgrenzung, Raum, Aufgabenbereich, Spielraum u.ä. haben kann. (Quelle: Wiki)*

2 UNTERNEHMENSFÜHRUNG, RISIKO UND PERSONAL

Unter den Aspekten der Unternehmensführung müssen organisationsfremde Services und Dienste mit den Unternehmenszielen vereinbart sein oder werden oder sie sind zukünftig zu ergänzen. Neben der Erstellung einer Cloud-Policy sollten Risiken und Chancen sorgfältig abgewogen werden. Welchen Nutzen bringt der Einsatz der Lösung tatsächlich und welchen Risiken ist dieses gegenüber zu stellen?

Ein wichtiger Aspekt bei der Vorbereitung ist, dass eigenes Personal über eine ausreichende Ausbildung verfügt. Beispielsweise benötigen die internen IT-Systemadministratoren / Koordinatoren, die bislang vielleicht die interne IT gemanagt haben, zukünftig weiterhin – wenn auch in einem anderen veränderten Rahmen –zunächst ein Know-How-Update, denn zukünftig kann nur ein Teil der Verantwortung an den neuen Dienstleister abgetreten werden.

Schulung ist ein kontinuierlicher Prozess, sowohl für die Fachbereiche und Administratoren sowie auch für die IT und das Sicherheitspersonal. Gerade dieser Bereich ist eng mit anderen Aspekten verknüpft.

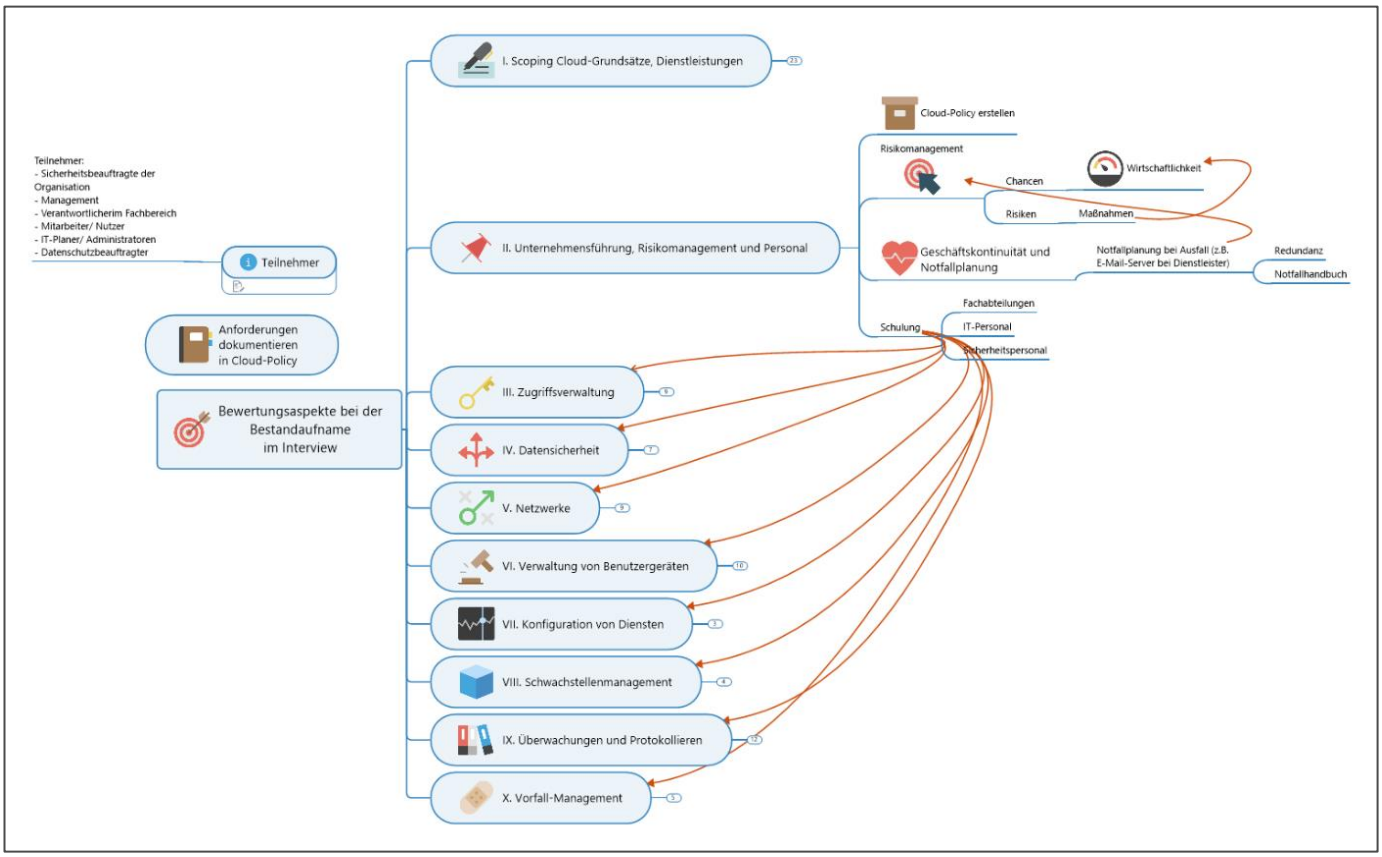

Abbildung 3 Unternehmensführung, Risiko und Personal

Mögliche Kontrollfragen können hier sein:

- Verfügt das interne Personal über ausreichend eigenes Know-How?
- Sind grundsätzliche Anforderungen aus den Punkten 2-10 erfasst, entsprechende Risiken und Maßnahmen ermittelt und definiert sowie Kosten / Nutzen sichergestellt?
- Inwieweit ist die Organisation dem Serviceprovider nach einem Umstieg zukünftig „ausgeliefert" bzw. verbleibt die Möglichkeit mit vertretbarem wirtschaftlichem Aufwand den Anbieter auch wieder zu wechseln, z.B. für Dienste wie Outlook 365, etc.? (Dieses Risiko sollte unbedingt mit in das Risikomanagement seitens einer Fallback-Lösung aufgenommen werden.)

3 ZUGRIFFSVERWALTUNG

Ein wesentlicher Aspekt bei der Betrachtung betrifft die zukünftige „Zugriffsverwaltung", die stets als originäre Aufgabe der eigenen Organisation betrachtet werden sollte und sich damit schwer ausgliedern lässt. Insbesondere ist sicher zu stellen, dass es ausreichend interne Richtlinien und Genehmigungsverfahren zur Autorisierung als auch zur Authentifizierung von Zugängen zu zukünftig ausgelagerten Diensten und Recheninstanzen bestehen.

Wichtige Aspekte sind hier aktuelle Anforderungen an Benutzer und ggf. auch Systembediener (Administratoren) sowie die Klarheit, welche Privilegien und Rollen benötigt werden:

Wie und wer im eigenen Unternehmen verwaltet zukünftig das benötigte Rechtemanagement?

Reichen die bisherigen Richtlinien in Bezug Passwort / Zertifikat / Token zukünftig aus oder sind Erweiterungen erforderlich, wie z.B. eine Mehrfaktor-Authentifizierung, die zusätzlich berücksichtigt werden muss?

Erfolgen ausreichende und regelmäßige Überprüfungen der Benutzerrechte und Ressourcen?

Existieren ausreichende Genehmigungs- und Protokollierungsprozesse oder Kontrollen, die unautorisierte Fernzugriffe verhindern, z.B. auch von außerhalb des Unternehmens?

Inwieweit kann der Cloud-Provider auf meine Daten zugreifen, z.B. in Form des Lesens von E-Mails durch den Provider selbst?

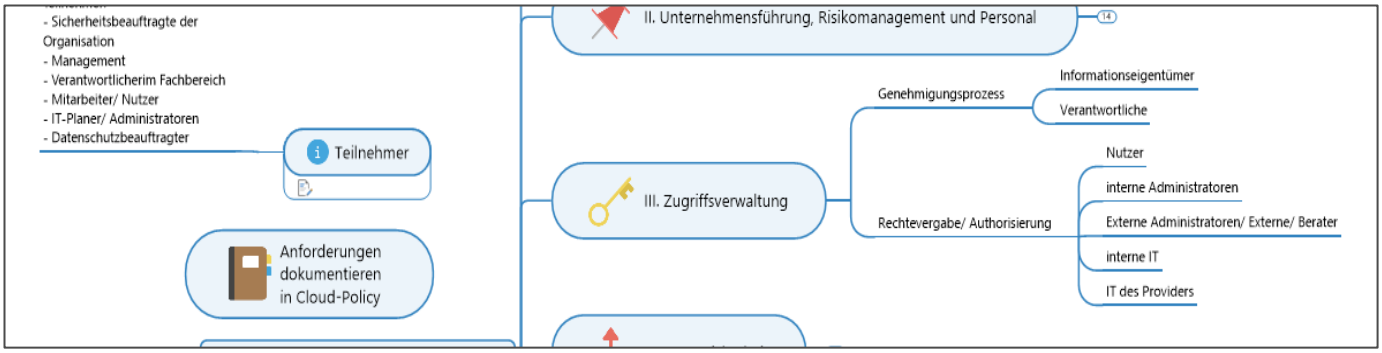

Abbildung 4 Zugriffsverwaltung

Mögliche Kontrollfragen können hier sein:

- Gibt es ausreichende Richtlinien, die Verfahren für die Verwaltung des Zugangs regeln?
- Ist das Active Directory auch zukünftig die einzige Quelle des Codes?
- Ist der Zugriff durch geeignete Authentifizierungsverfahren (z.B. Multi-Faktor-Authentifizierung) abgesichert?
- Wer hat Zugriff auf die Erstellung und Löschung von Benutzerkonten?
- Sind ausrechende Genehmigungs- und Protokollierungsprozesse und Kontrollen installiert, die einen unautorisierten Zugriff oder auch Fernzugriff verhindern (vielleicht auch durch den Service-Provider selbst)?
- Ist gewährleistet, dass sich der Zugriff seitens der Benutzer auf den Cloud-Dienst ausschließlich auf die Geschäftsfunktion beschränkt?
- Ist ausreichend sichergestellt, dass Zugangskontrollen durch z.B. Firewalls des Dienste-Anbieters selbst auch tatsächlich funktionieren und ggf. Risiken vertraglich abgesichert sind?

4 DATENSICHERHEIT

Der Aspekt der Datensicherheit benötigt grundlegend das eindeutige Verständnis darüber, welche Art und welche Informationen in Relation zur Datenkritikalität zukünftig in der Cloud abgespeichert werden. Dieses gilt sowohl für vom Kunden überlassene Daten aus einem Kundenauftrag sowie auch für interne Daten der Organisation, z.B. Kalkulation, Patente oder auch Informationen mit Personenbezug, wie die Ablage von Protokollen in Terminen, die auch vertrauliche Informationen wie Personen und/ oder Entscheidungen von Kunden beinhalten können. Welche Auswirkungen entstehen, wenn die Informationen bekannt werden?

Uneingeschränkt gilt die Empfehlung, alle als geheim oder streng vertraulich eingestuften Daten auf organisationseigenen Geräten, also eigenem „Blech", zu speichern und die Transportwege der Cloud zu vermeiden, soweit die Daten nicht so mit eigenen Kennwörtern Ende-zu-Ende verschlüsselt sind, sodass sie von den Administratoren des Diensteanbieters nicht eingesehen werden können.

Im Rahmen der aktuellen Diskussion zum Datenschutz sollte ferner untersucht werden, wo personenbezogene Daten in der Cloud tatsächlich physisch abgespeichert sind bzw. ist dieses auch mit dem Diensteanbieter vertraglich festzulegen.

Betreiben wir eine externe Schulungsplattform, in der zukünftig unsere Mitarbeiter mit Personenbezug auf einem Server außerhalb Europas abgespeichert sind und welche Risiken verbinden sich damit bzw. welche Anforderungen an Verschlüsselung, Signierung oder rechtliche Anforderungen sind zu berücksichtigen?

Hat vielleicht auch der Administrator des Systembetreibers selbst einen Zugriff auf abgespeicherte Daten, da die Schlüssel vielleicht vom Provider selbst generiert wurden, wie dieses u.U. bei z.B. Outlook 365 der Fall ist?

Oder auch grundsätzlich die Frage, welche Features bietet meine zukünftige Schatten-IT zum Schutz meiner Daten nach außen?

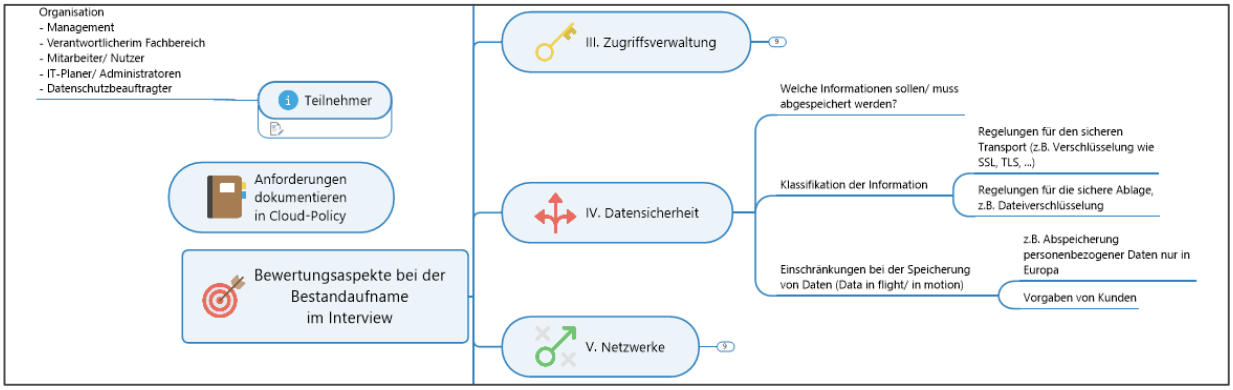

Abbildung 5 Datensicherheit

Mögliche Kontrollfragen können hier sein:

- Ist ausreichend verstanden, wo sich zukünftig die eigenen Daten befinden und wie sie übertragen werden ("Data in flight" versus "in motion")?
- Sind die Datenschutzanforderungen der Lösung ausreichend verstanden?
- Sind auch die Sicherheitsanforderungen, die seitens der eigenen Kunden an den Schutz von Informationen gestellt werden, ausreichend verstanden und berücksichtigt?
- Ist definiert, welche Informationen zukünftig im Dienst abgespeichert werden?
- Durch welche Maßnahmen stellt die eigene Organisation sicher, dass nur bestimmte Daten abgespeichert werden?
- Durch welche bestehenden Mechanismen erfolgt ggf. eine ausreichende Verschlüsselung der Daten – z.B. auch zum Schutz vor dem Zugriff durch den Service-Provider selbst?
- Ist ausreichend sichergestellt, dass personenbezogene Daten innerhalb Europas abgespeichert werden?

Sind Risiken im betriebseigenem Risiko-Management berücksichtigt und gibt es ausreichende Kontrollen (z.B. der seitens des Diensteanbieters-eigenen APIs)?

Fortsetzung des Fachbeitrages mit Teil 2 in Folge 9…

Der Autor Bernd Schart ist seit 2009 Mitarbeiter der OS und beschäftigt sich im Fachgebiet Security & Audit seit 2011 als Auditor mit dem Thema Informationssicherheit in der Automobilindustrie. Bernd Schart betreibt seit 2020 einen eigenen, freien und unabhängigen Podcast (WWW.ISITALK.DE) zu Themen der Informationssicherheit, speziell auch den Anforderungen des VDA ISA im Rahmen von TISAX® Assessments.

TISAX® ist eine eingetragene Marke der ENX Association. TISAX steht für „Trusted Information Security Assessment Exchange" und ist der Standard für Informationssicherheitsbewertungen in der Automobilindustrie. TISAX® schafft Wettbewerb unter akkreditierten Prüfdienstleistern und ermöglicht eine gemeinsame Anerkennung von Prüfergebnissen innerhalb der Automobilbranche. Nähere Informationen finden Sie unter WWW.TISAX.NET.