TeleTrusT "IT-Sicherheitsrechtstag 2023"

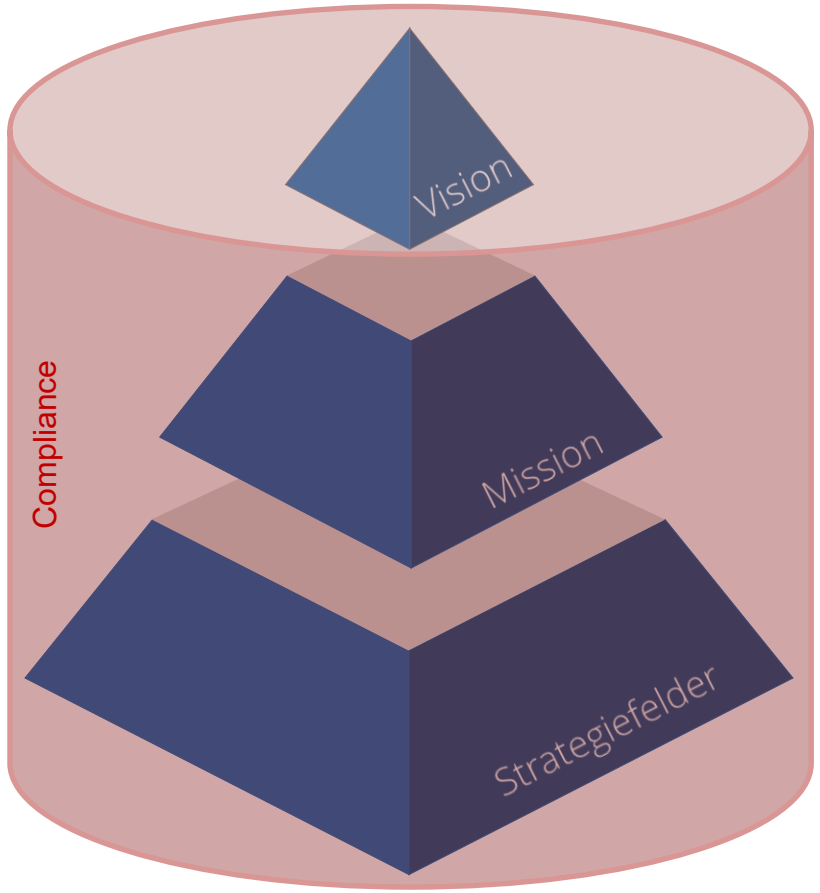
Berlin, 28.09.2023

Sicherheitsstrategie für cloudbasierte Services bei einem Finanzdienstleister

Tomasz Lawicki

Capgemini, Regional Head Cybersecurity, Security Architect Director
Bundesverband IT-Sicherheit e.V. (TeleTrusT), Leiter AK "Stand der Technik"

Die Strategie-Pyramide



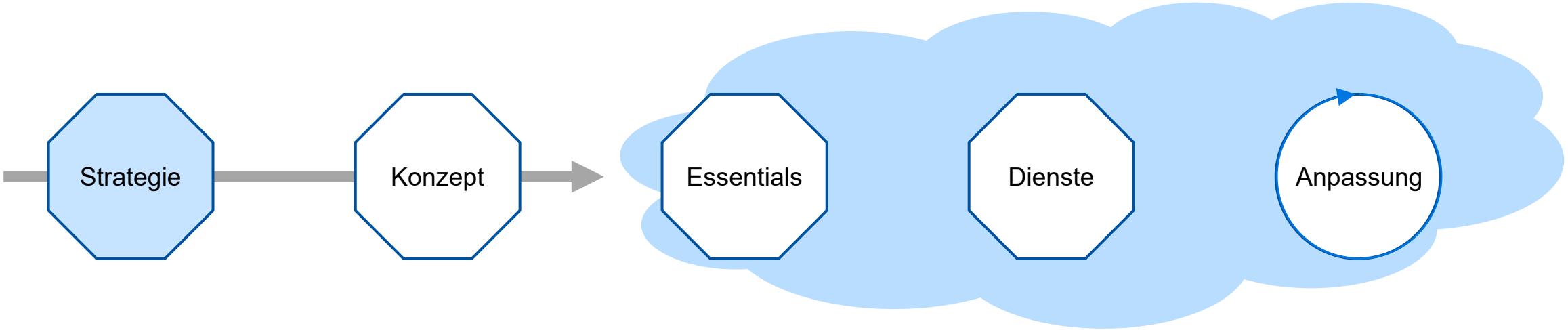
- In der Strategieplanung ist die Vision ein imaginäres Zukunftsbild des Unternehmens und beantwortet die Frage nach „**WO** wollen wir hin?“. Sie hat eine Orientierungsfunktion für alle Beteiligten und wird oft als Slogan formuliert.

- Die Mission wird von der Vision abgeleitet und legt fest auf welche Art die Vision erreicht werden soll. Sie beantwortet somit die Frage „**WAS** tun wir, um die Vision zu erreichen?“.

- In den Strategiefeldern wird der Weg festgelegt, um die Vision zu erreichen. Sie haben starke Auswirkung auf die Ziel-ausrichtung des Unternehmens in der die Frage beantwortet wird „**WIE** können wir die Vision erreichen?“

- Üblicherweise werden die Vision und Mission auf der Vorstandsebene für das gesamte Unternehmen aufgestellt. Aber sie können ebenfalls für den jeweiligen Bereich definiert werden, um die Bereichsstrategie zu verfestigen.

Der Weg in die Cloud beginnt lange bevor die Cloud-Dienste genutzt werden



- Eigenen Bedarf kennen
- Übergreifende Cloud Strategie festlegen
- Kritische Daten und Prozesse kennen
- Schutzbedarf analysieren

- Cloud Konzept erstellen
- CSP auswählen
- Aufgabenverantwortung klären
- CSP Sicherheitsmaßnahmen kennen und Lücken identifizieren
- Ergänzende externe Sicherheits-Maßnahmen identifizieren
- Vertragliche Themen klären

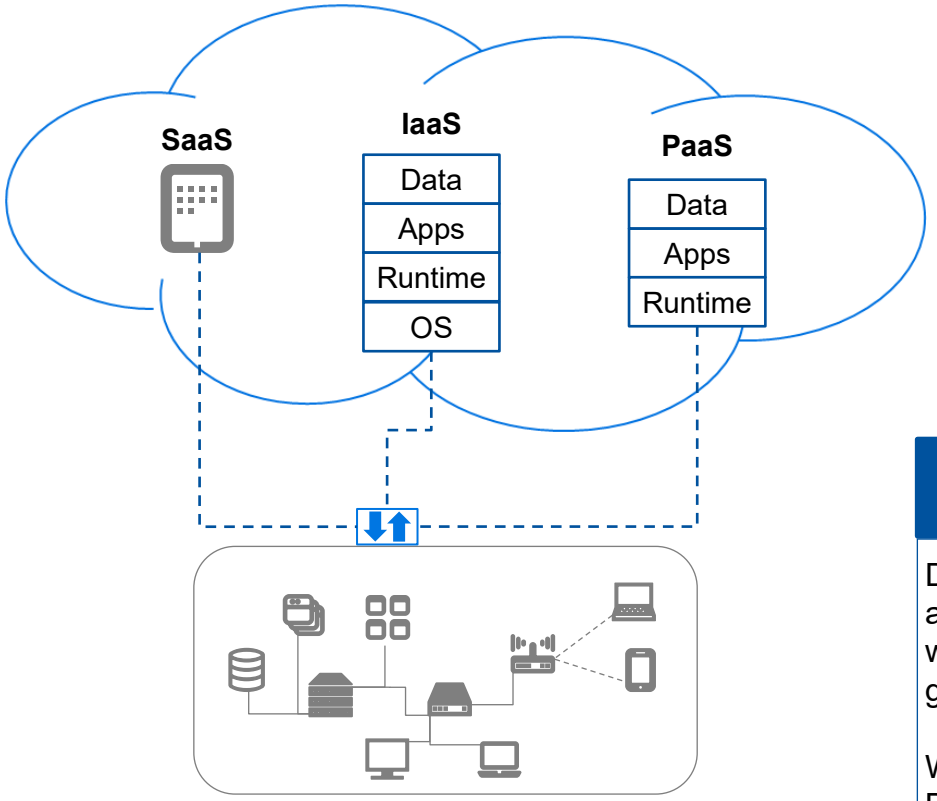
- Cloud Umgebung konfigurieren (Security Essentials)
- CSP Sicherheitsmaßnahmen aktivieren
- Bei Bedarf durch externe technische Maßnahmen ergänzen
- Monitoring aktivieren

- Erst jetzt werden die ersten Dienste/Services genutzt oder bestehende Apps umgezogen.

- Cloud Security ist ein Prozess.
- Es genügt nicht, die Maßnahmen einmalig aufzusetzen. Sie müssen überwacht und ggfs. angepasst werden.

Die Herausforderung (… vieler Unternehmen)

- Bisherige Infrastruktur basiert auf klassischem Ansatz (on-premises)
- Gewünscht ist flexble Erweiterung, um zusätzliche Kapazitäten nutzen zu können verbunden mit der Modernisierung einzelner Anwendungen in ausgewählten Bereichen



Nutzung von Infrastructure-Services

Für die Entwicklung eigener Anwendungen sollen Services der Hyperscaler genutzt werden.

Zuerst sollen nur Anwendungsfälle mit normalen Schutzbedarf, später mit hohem Schutzbedarf in der Cloud verarbeitet werden.

Nutzung von SaaS-Diensten

Die Office-Kommunikation ist strategisch auf Microsoft ausgerichtet. Microsoft Teams wurde bereits eingeführt. Später soll das gesamte M365 umgesetzt werden.

Weitere Cloud Dienste (SaaS) sollen nach Bedarf beschafft werden.

Definition zur Abgrenzung von Cloud Diensten

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

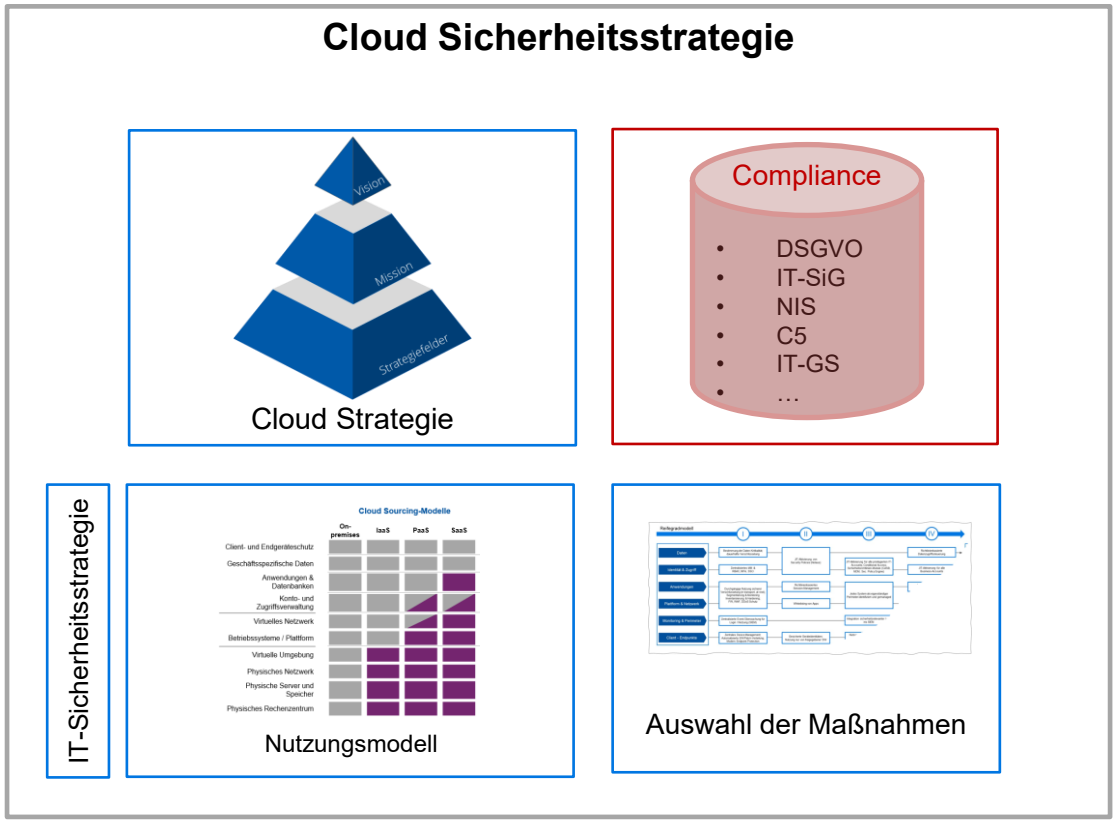
- Gemäß Definition von **TeleTrusT** ist „Cloud Computing (…) ein Ansatz, der den bequemen On-Demand Netzwerk-Zugriff auf einen gemeinsamen Pool konfigurierbarer Rechner-Ressourcen (z. B. Netzwerke, Server, Speichersysteme, Anwendungen und Dienstleistungen) ermöglicht, die mit nur geringem Management-Aufwand oder Eingriff eines Service-Anbieters schnell bereitgestellt und freigegeben werden können.“

- Zudem nennt **NIST** (**) fünf Kriterien, die Cloud Computing ausmachen:
  1. Automatisierte Bereitstellung mit bedarfsorientierter Zugriffsmöglichkeit
  2. Breitbandiger Netzwerkzugriff
  3. Pooling von Ressourcen
  4. Vollständige Elastizität und Skalierbarkeit
  5. Nutzungsabhängige Zahlung („Pay per use“-Prinzip)

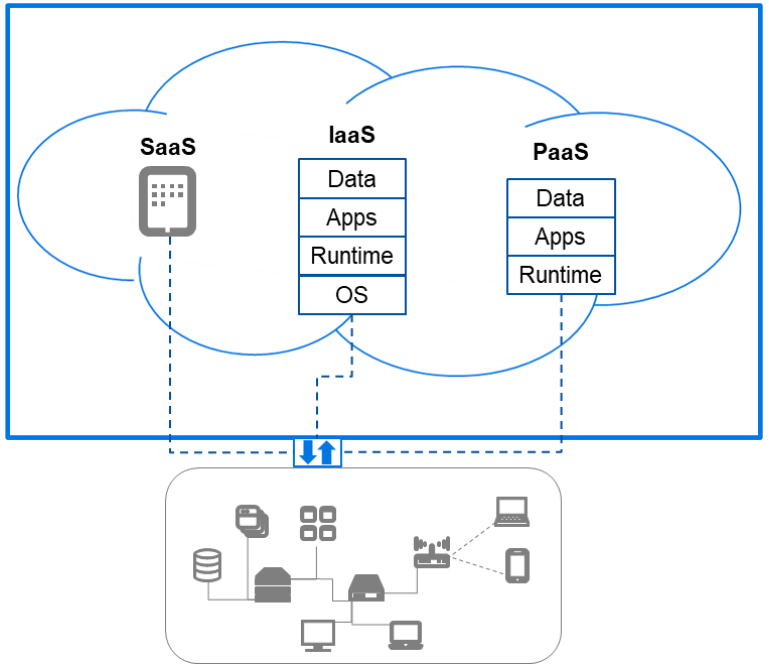
(*) TeleTrusT – Bundesverband IT-Sicherheit e.V. - https://www.teletrust.de/publikationen/broschueren/cloud-security

(**) NIST- National Institute of Standards and Technology, 2011, The NIST Definition of Cloud Computing, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

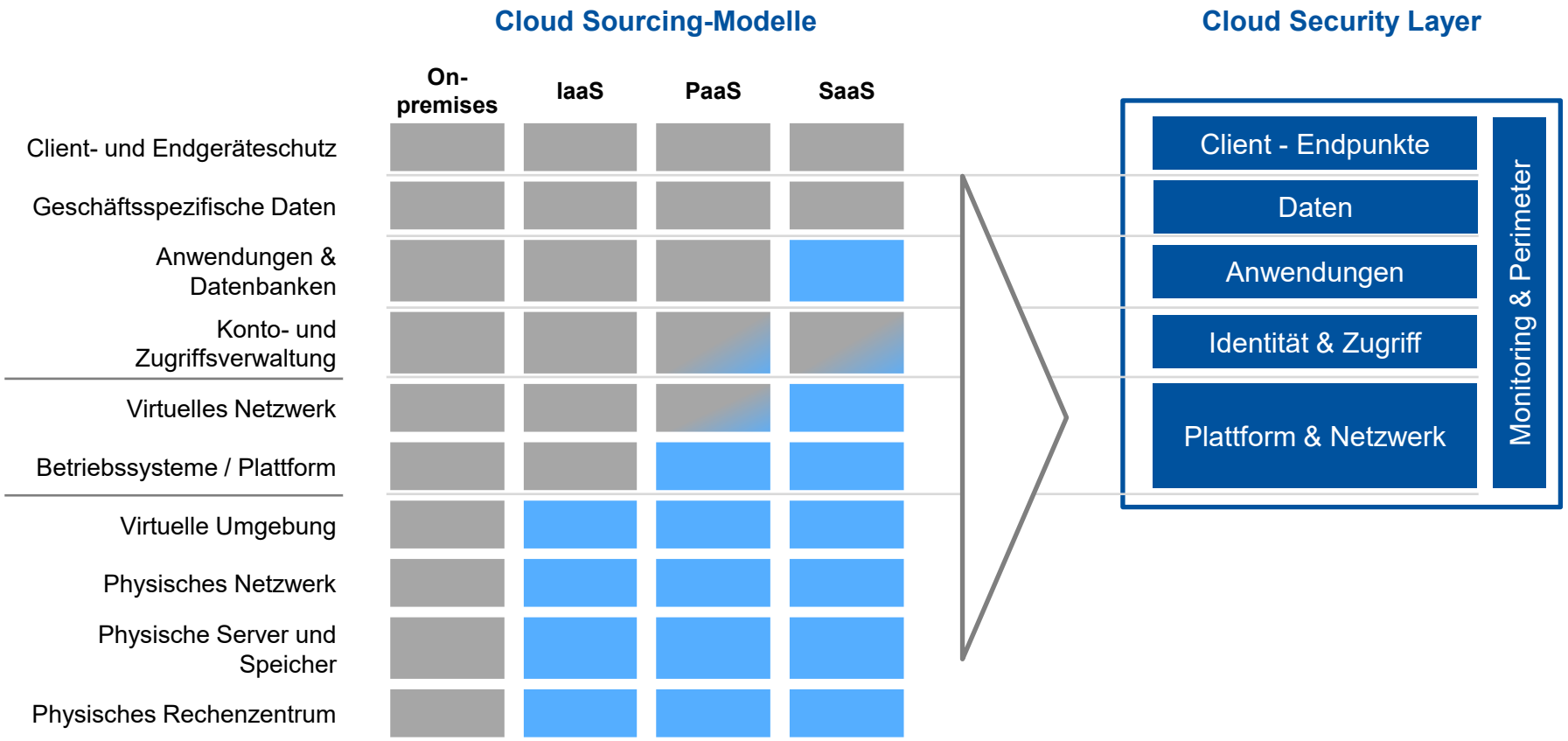
Die Sicherheitsstrategie muss Leitplanken für sichere Nutzung der Cloud-Dienste festlegen



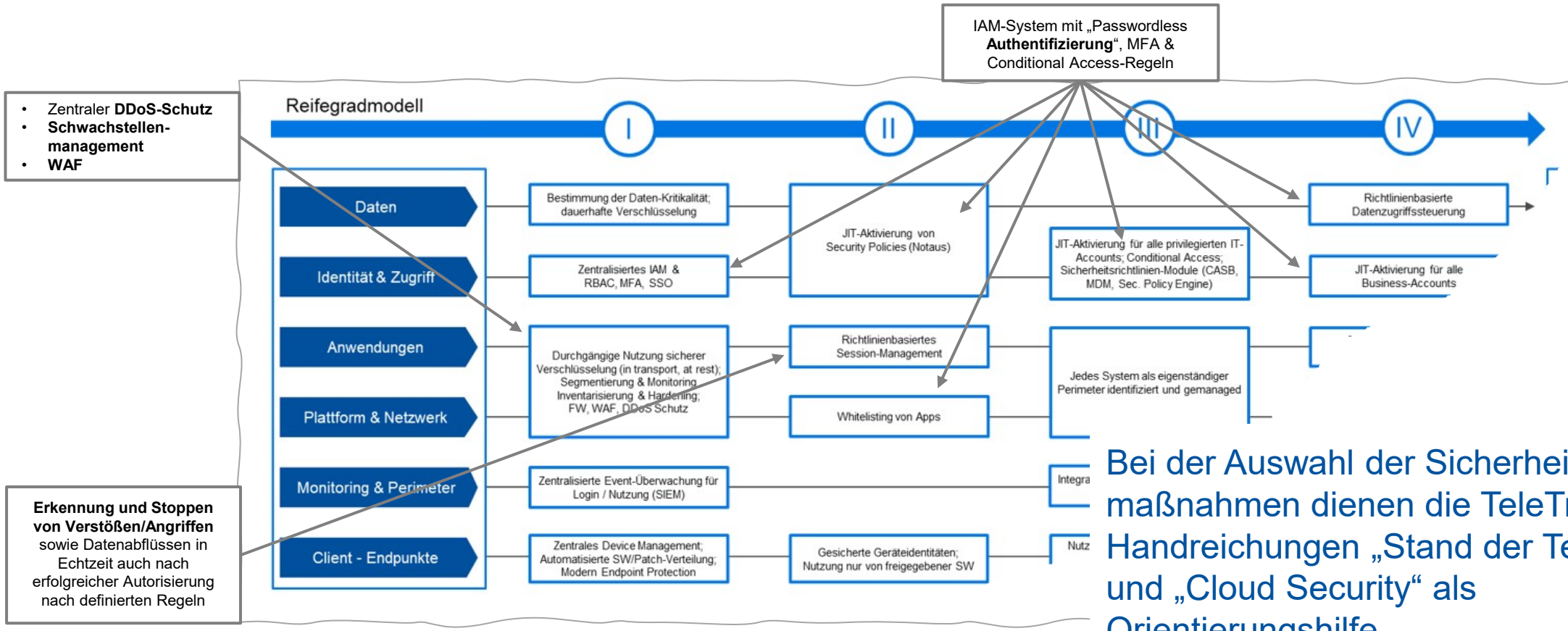
Roadmap



Cloud Security Layer als Rahmen für die Sicherheitsstrategie



Für eine sichere Cloud-Nutzung müssen moderne Sicherheits-maßnahmen eingesetzt werden

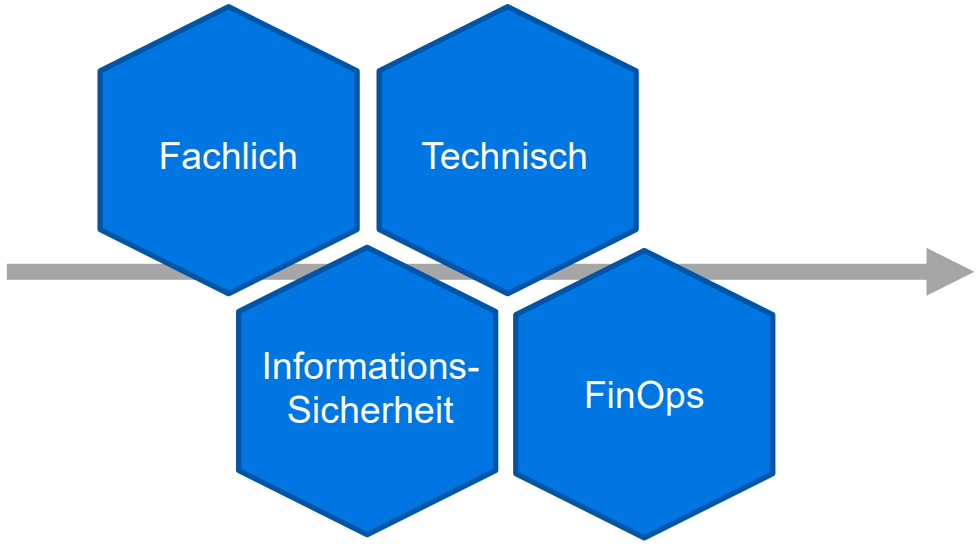


Bei der Auswahl der Sicherheits-maßnahmen dienen die TeleTrusT Handreichungen „Stand der Technik“ und „Cloud Security“ als Orientierungshilfe.

Cloud Center of Excellence als entscheidender Baustein in der Umsetzung einer Cloud Sicherheitsstrategie

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

Das Cloud Center of Excellence (CCoE) agiert als interdisziplinärer Ansprechpartner für alle Fragen rund um Cloud-Themen und deren Umsetzbarkeit.



Kritische Erfolgsfaktoren

- Offizielles Mandat der GF
- Selbstidentifikation und Vertretung nach Außen als Business Enabler und Partner
- Eindeutige Aufgaben-Verantwortung
- Gutes Verständnis für die Unternehmens-Strategie
- Interdisziplinäre Aufstellung, um die Komplexität zu managen
- Weitblick und Erfahrung der Beteiligten
- Vorgabe pragmatischer und realistischer Standards und Richtlinien
- Proaktive Steuerung des organisatorischen Wandels
- Unterstützung bei der Qualifizierung & Weiterbildung der Organisation

Dokumentation der Massnahmen

Rechtsgrundlage	Gesetzestext	Themenbereich	Maßnahmen (Beispiele)
§ 8a Abs. 1 BSIG	"Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, **Integrität**, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind."	Integrität	Direkte Maßnahmen zur Sicherstellung der Integrität sind beispielhaft: • fortgeschrittene/qualifizierte Signatur (auch Code Signatur), • Genehmigungsverfahren, Zwei-Personen-Prinzip Weitere Maßnahmen werden als Beispiele genannt: • Änderungen an Systemen müssen dokumentiert werden • Unberechtigte Zugriffe müssen detektiert werden • Systeme und Anwendungen sollten immer die aktuellen Sicherheitsupdates erhalten • es müssen Maßnahmen zur Erkennung von Schadsoftware eingesetzt werden • es müssen Maßnahmen zur Sensibilisierung der Mitarbeiter umgesetzt und wiederkehrend wiederholt werden

Empfehlungen in der TeleTrusT Handreichung "Stand der Technik“

Welche Schutzziele werden durch die Maßnahme abgedeckt?

- ☐ Verfügbarkeit
- ☒ Integrität
- ☒ Vertraulichkeit
- ☒ Authentizität

ID	Cloud Security Layer	Security Function	Kategorie	Anforderung	IaaS	PaaS	SaaS
3	Abschnitt		Sichere Konfiguration von Unternehmensressourcen und Software	*Einrichten und Pflegen einer sicheren Konfiguration von Unternehmens-Assets (Geräte für Endbenutzer, Netzwerkgeräte, IoT-Geräte und Server) sowie Software (Betriebssysteme und Anwendungen)*	x	x	x
3.1	Anwendungen	Protect	Erstellen und Pflegen einer Konfigurationsdokumentation	Erstellen und pflegen Sie ein Dokument zur sicheren Konfiguration der genutzten Cloud Services. Unabhängig vom gewählten Cloud Service Modell (IaaS, PaaS, SaaS) bleibt die DeKa immer für die sichere Konfiguration der genutzten Services verantwortlich. Die Dokumentatzion der Konfiguration ist regelmäßig und bei jeder wesentlichen Änderung zu aktualisieren.	x	x	x
3.2	Netzwerk	Protect	Implementieren und Managen einer Firewall oder vergleichbarer Dienste	Implementieren und verwalten Sie eine Firewall bzw. andere vergleichbare, Cloud-Anbieter-spezifische Netzwerksicherheitsmaßnahmen (z.B. Network Security Groups, NSG) zur Herstellung der Perimetersicherheit.	x	x	
3.3	Netzwerk	Protect	Sichere Verwaltung von Unternehmens-Assets und Software	Verwalten Sie Unternehmens-Assets und Software auf sichere Art und Weise. Dazu gehören idealerweise die Ablage von Konfigurationen als Infrastructure as Code in Versionsverwaltungs-Tools. Die administrative Nutzung von Benutzerschnittstellen erfolgt ausschließlich über sichere Übertragungsprotokolle, wie z.B. Secure Shell (ssh) und Hypertext Transfer Protocol Secure (https) nach akutellen Sicherheitsstandards. Verwenden Sie keine als unsicher geltenden Protokolle wie telnet oder http.	x	x	

Q & A