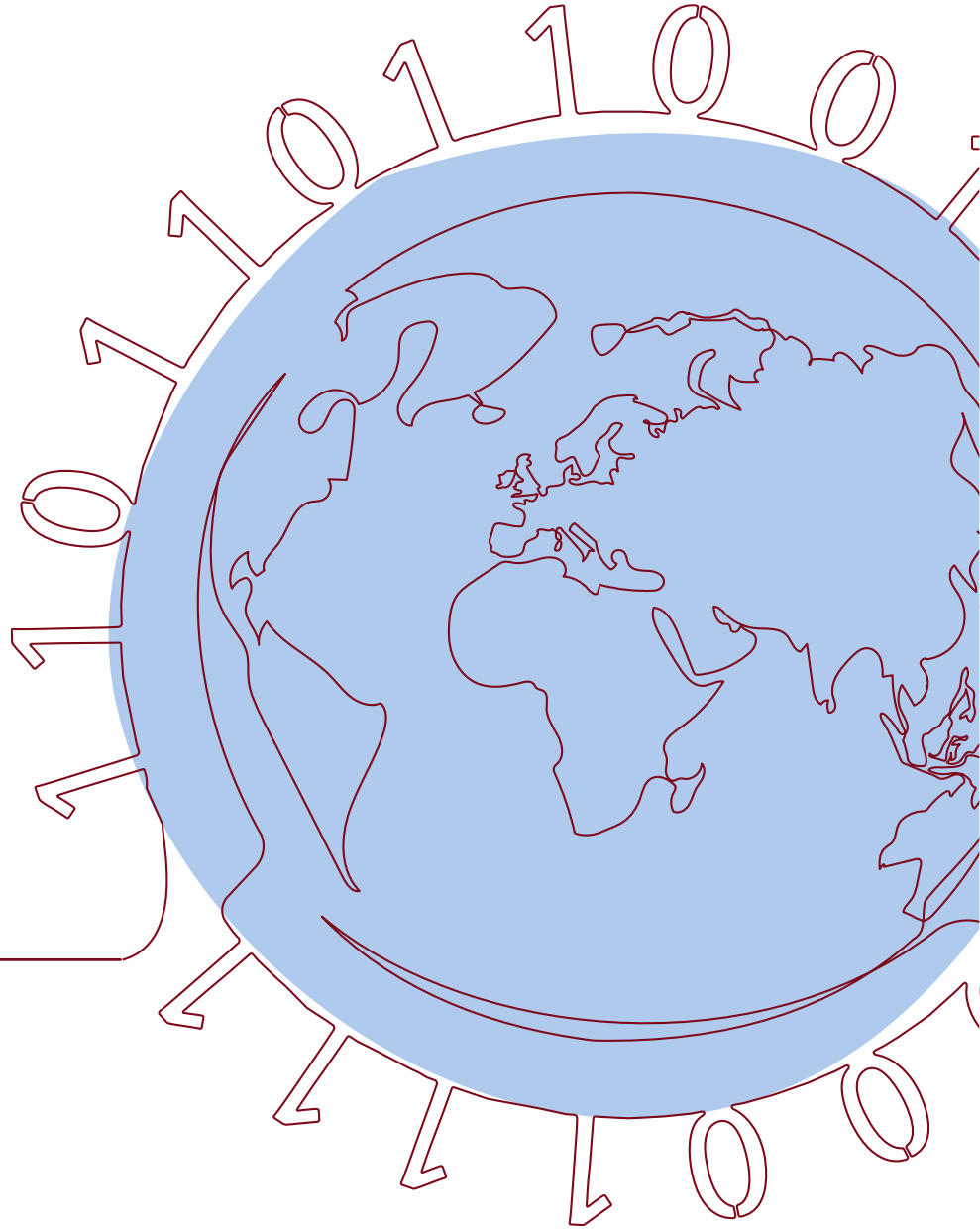
bankenverband

Mögliche Auswirkungen der EUCS-Aspekte auf die Nutzung von Cloud-Diensten in der Finanzindustrie



Cloud-Workshop BdB/Ministerien am 1. Juni 2023

Warum nutzen europäische Banken die Public Cloud Infrastrukturen?

1 Innovationsfähigkeit

- In den Bereichen der **Rechenzentren**, der **Software** und den Technologien wie Sprachmodellen, Dokumentenanalyse, Datenbanken, **Künstlicher Intelligenz und Machine-Learning Modellen** findet die Entwicklung und Innovation vorrangig über die Cloud-Systeme statt.

2 Wirtschaftlichkeit

- Die im Pay-per-Use abgerechneten Clouddienste sind in diesen Bereichen **up-to-date**, zudem hoch **verfügbar** und **skalierbar** (reagieren elastisch auf Zugriffe).
- Die bislang erforderlichen **Reservekapazitäten** für **Resilienz und Nutzungsintensität** werden in der Cloud diversifiziert (solidarisiert) und können erheblich **reduziert** werden.

3 Risikomanagement

- Risikoreduktion durch die **Hochverfügbarkeit regionaler Rechen-zentren** und möglicher **Kombination mehrerer Regionen** mit unterschiedlichem Risikoprofil.

4 War for Talents

- Junge Entwicklerinnen und **Entwickler erwarten eine moderne IT-Infrastruktur**.
- Rahmenbedingungen und Leitplanken in der Cloud ermöglichen **größere Eigenverantwortung für Mitarbeiter**.

5 Sicherheit & Resilienz

- Legacy-Systeme sind größerer Gefahr durch Cyber-Attacken ausgesetzt.
- Jetzige Cloud-Lösungen bieten einen sehr hohen **Sicherheitsstandard und erhöhen die Cyber-Resilienz!**

Derzeit sehen wir keinen europäischen Cloud-Dienste-Anbieter, der die vorgenannten Entscheidungskriterien erfüllt!

Mögliche Auswirkungen von Immunitätskriterien

Situation

- **Deutsche** und **Europäische Banken** nutzen Cloud Services verschiedener internationaler Anbieter, insbesondere Hyperscaler aus den USA.
- **Technischer Fortschritt** und **breite Service-Landschaft** der amerikanischen Hyperscaler erlauben die **Erstellung innovativer Finanzprodukte.**
- **Innovationskraft, Verfügbarkeit** und **Skalierbarkeit** amerikanischer Cloud-Dienstleister sind mittlerweile auch **Basis für europäische Plattformen** wie Gaia-X.
- Über vertragliche sowie technische und organisatorische Maßnahmen (TOM) wird hierbei ein **sehr hohes Maß an Sicherheit** erreicht und **regulatorische Konformität** hergestellt.
- Die **Sicherheit spielt** bei der Auswahl des geeigneten Cloud-Providers eine **entscheidende Rolle**.
- Wenn Banken SaaS-Lösungen für ihre Kunden anbieten, sind sie **per Definition auch Cloud-Service-Provider**.
- Die Banken **begrüßen** die **Ziele** der **Standardisierung, Zertifizierung** und **Erhöhung der Sicherheit**, die über SCC, DORA, Cloud Rulebook und EUCS angestrebt werden.

Auswirkungen

- Unklare Abgrenzung der EUCS-Sicherheitslevel lässt für Banken zukünftig das höchste Sicherheits-Level „high+“ vermuten.
- Mit Einführung der Souveränität und Immunitätskriterien im EUCS-Draft drohen **sehr negative Auswirkungen** für **europäische Banken** als Nutzer und z.T. Anbieter von Cloud Services.
  - **Fokus auf die Standortwahl** zu legen, ist **keine Garantie für mehr Sicherheit**. Im Gegenteil, in Bedrohungslagen würde ggf. sogar ein Wechsel in andere Regionen sinnvoll sein**.**
  - **Auswahl eines Cloud-Dienste-Anbieters** könnte nicht ausschließlich auf Basis der **besten Services und des besten Schutzniveaus** erfolgen.
  - **Fehlender Wettbewerb europäischer Anbieter** im Bereich der PaaS und SaaS schränken die Wahlmöglichkeit hiesiger Banken stark ein - mit Implikation auf das Serviceangebot.
  - Beschränkungen bezüglich Datenspeicherung, Zugriff und Verarbeitung auf EU-Ebene würden **sämtliche Off-Shoring-Strategien gefährden**, inkl. das Nutzen von Tech-Support und Ressourcen aus Drittländern – 24/7-Infrastrukturadministration wäre wirtschaftlich nicht möglich.
  - **Enorme Auswirkungen auf organisatorische und operative Strukturen** der Banken, unter anderem auch auf die zur **Verfügungstellung der kritischen Versorgungsdienstleistungen**.

- **Verweis auf die EUCS-Draft-Kriterien in NIS-Richtlinie & Cyber Resilience Act zeigt, dass die Anforderungen mandatorisch werden könnten.**
- **Zur Erhaltung der Wettbewerbsfähigkeit des deutschen und europäischen Bankensektors sind Services global agierender CSPs unabdingbar.**

Zusammenfassung

Das Zertifizierungsschema darf in der Konsequenz nicht zum Ausschluss von US-Anbietern führen.

1. In der **aktuellen Fassung könnte das ENISA EUCS die Cloudnutzung** für den deutschen und europäischen Finanzsektor und die Wirtschaft stark behindern oder **grundsätzlich in Frage stellen**.
2. Cloud-Services sind bereits heute in erheblichem Maß in Bankinfrastrukturen integriert und auch weiterhin als wichtiger Baustein für eine **Wettbewerbsfähigkeit europäischer Banken** unabdingbar.
3. Die mögliche Konsequenz - bei der Verarbeitung von Kundendaten auf rein europäische Anbieter („presence of headquarters in the EU“) unter Beibehaltung des Serviceangebotes zu wechseln, würde **erhebliche negative Auswirkungen** haben.
4. Ein **geopolitisches Problem** sollte nicht mit einem technischen Sicherheitsstandard gelöst werden. Fokus sollte vielmehr auf technischen Schutzmaßnahmen wie Verschlüsselung, Datenmaskierung und Anonymisierung liegen. Diese sorgen für den erforderlichen Schutz vor Datenzugriffen.
5. **Tiefgreifende Analyse der Auswirkungen** von Souveränität- und Immunitätskriterien für die EU-Wirtschaft notwendig.
6. **Intensive und transparente Einbindung** aller betroffenen Stakeholder in **die politische Entscheidungsfindung.**