PHOENIX

Confidential Computing

Die unverzichtbare technologische Grundlage für die Erreichung echter digitaler Souveränität im Zeitalter der Künstlichen Intelligenz

Thomas Taroni
Executive Chairman
Phoenix Technologies

07.05.2025

Datensouveränität und ihre Auswirkungen

Datensouveränität ist nicht verhandelbar

Datensouveränität wird nicht als Option betrachtet, sondern ist der einzige Weg zum Erfolg in der Künstlichen Intelligenz.

KI und Ethik – ein gesellschaftlicher Imperativ

Eigentum und Kontrolle über KI-Trainingsdaten haben tiefgreifende Auswirkungen auf Datenschutz, Sicherheit und ethische Überlegungen. Ein verantwortungsvoller Umgang mit KI-Daten ist daher ein „gesellschaftlicher Imperativ“.

Souveränität als Verantwortung

Souveränität wird nicht nur als Kontrolle definiert, sondern als Verantwortung für Tech-Leader, die Integrität ihrer Systeme und die Privatsphäre ihrer Nutzer zu schützen.

Streben nach souveräner und vertraulicher KI

Strategische Autonomie im digitalen Raum

Eine Notwendigkeit, die durch die zunehmende Abhängigkeit von digitalen Technologien und die Dominanz globaler Akteure immer dringlicher wird

Förderung von Transparenz, Vertrauen und Innovation

Open Source ermöglicht die Inspektion des Quellcodes, was Vertrauen in Sicherheitsmechanismen aufbauen kann. Dies ist sowohl für Confidential Computing als auch für die Verifizierung von Souveränitätsansprüchen entscheidend.

Die Verknüpfung von Vertraulichkeit, Souveränität und Offenheit

Digitale Souveränität erfordert Offenheit. Systeme sollten mit offenen Standards kommunizieren, um Interoperabilität und Innovation zu ermöglichen.

Agentic AI

Agentic AI in Unternehmen

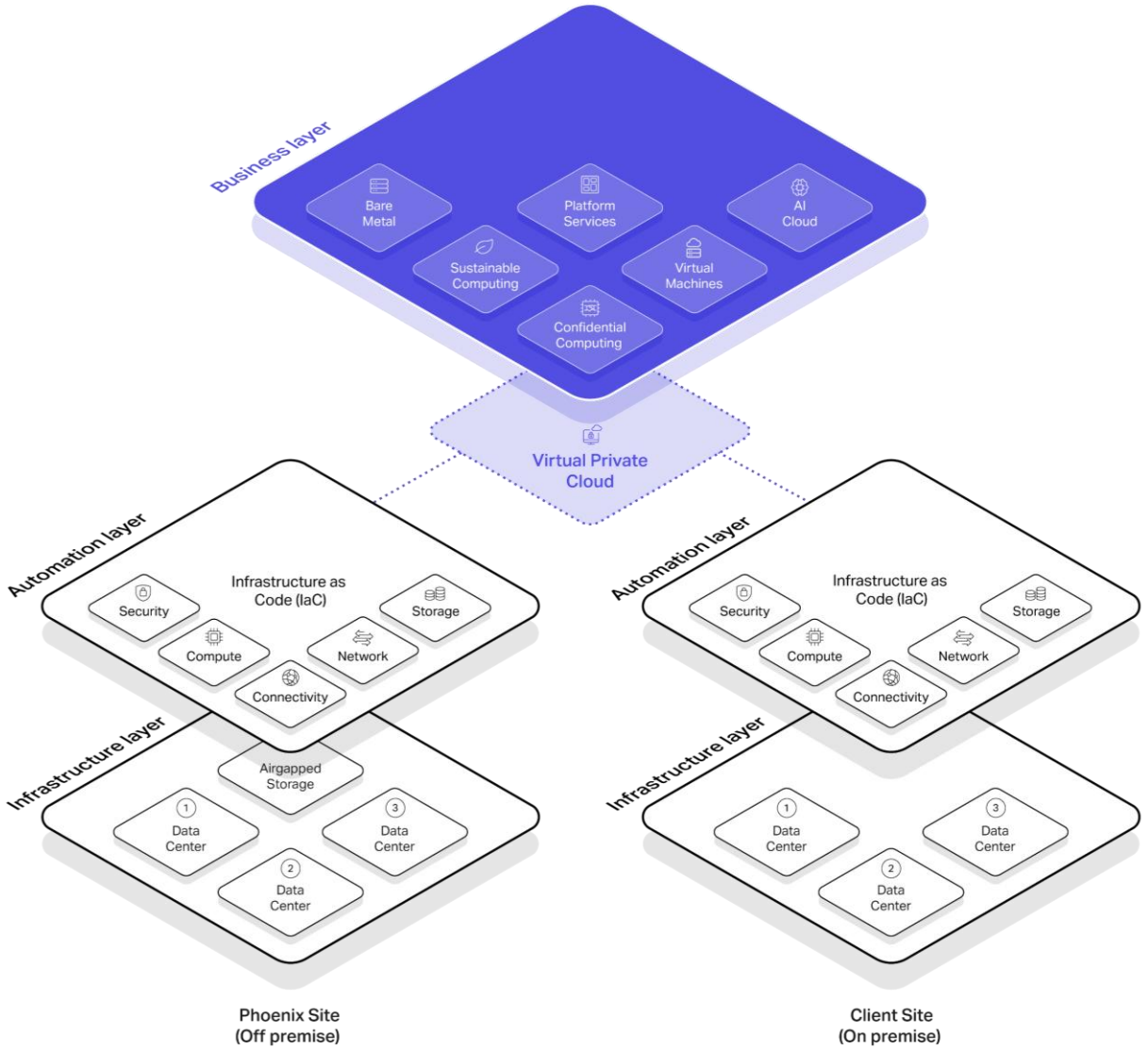
Wenn wir dieses Konzept auf ein Unternehmen anwenden, können sich die Dynamiken unterscheiden, aber das zugrunde liegende Prinzip bleibt dasselbe. Das KI-System muss genau so handeln wie das Unternehmen. Wenn eine Führungskraft möchte, dass das KI-System Entscheidungen im Namen des Unternehmens trifft, muss es exakt den Regeln, Richtlinien, Werten und der Historie des Unternehmens agieren.

In diesem Szenario repräsentiert das KI-System im Wesentlichen die aktuelle Geschäftslogik des Unternehmens und verkörpert alle seine Werte. Wir können uns alle die erheblichen Auswirkungen auf die nationale Verteidigung oder Regierungsoperationen vorstellen, wenn Daten kompromittiert oder unzugänglich werden. Dies ist der kritische Faktor.

Introducing kvant AI

Das Fundament der digitalen Souveränität

- **Business Layer:** Betreiben Sie Ihre eigenen Anwendungen, Dienste oder Ihre KI-Cloud.
- **Automation Layer:** Mit Infrastructure as Code (IaC) werden Infrastrukturressourcen durch Code und Skripte definiert, bereitgestellt und verwaltet, anstatt durch manuelle Prozesse.
- **Infrastructure Layer:** Sie können einen unserer Rechenzentrumsstandorte wählen oder Ihre kvant Private Cloud in Ihrem eigenen Rechenzentrum aufbauen.



PHOENIX

Contact Us

contact@phoenix-technologies.ch

Phoenix Technologies AG
Bahnhofstrasse
CH-6300 Zug
www.phoenix-technologies.ch