Whitepaper

Wie wird die Cloud von Morgen aussehen?

- So sicher, dass sie souverän genutzt werden kann
- Minimaler CO_2-Ausstoß
- Einfache Nutzung

BetterEdge
Verifiable Sovereign Computing

Whitepaper:
Wie wird die Cloud von Morgen aussehen?

real-cis GmbH
München und Frankfurt
Rheinstr. 5, D-63225 Langen

https://betteredge.de

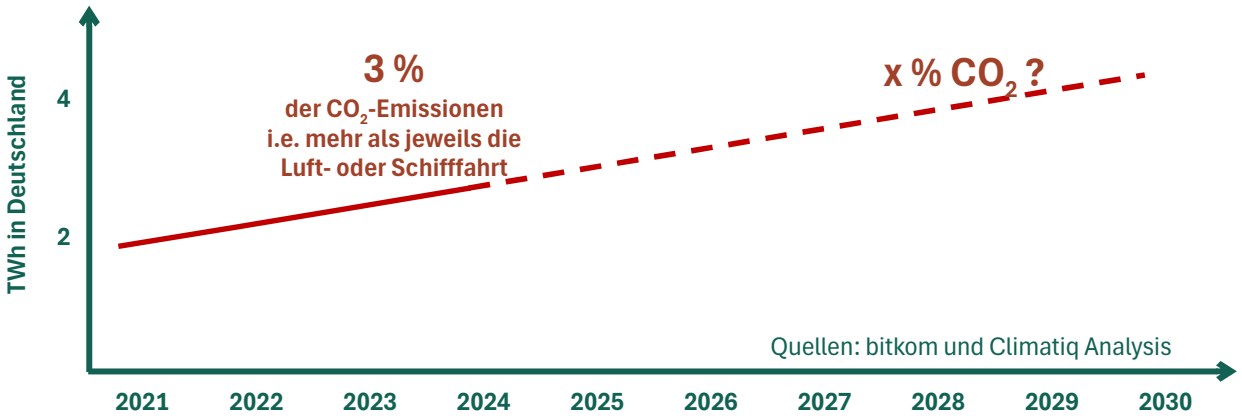
Stand: 05.09.25

Inhaltsverzeichnis

1. Probleme des Cloud Computing

1.1 Enormer Energiebedarf und CO_2-Ausstoß

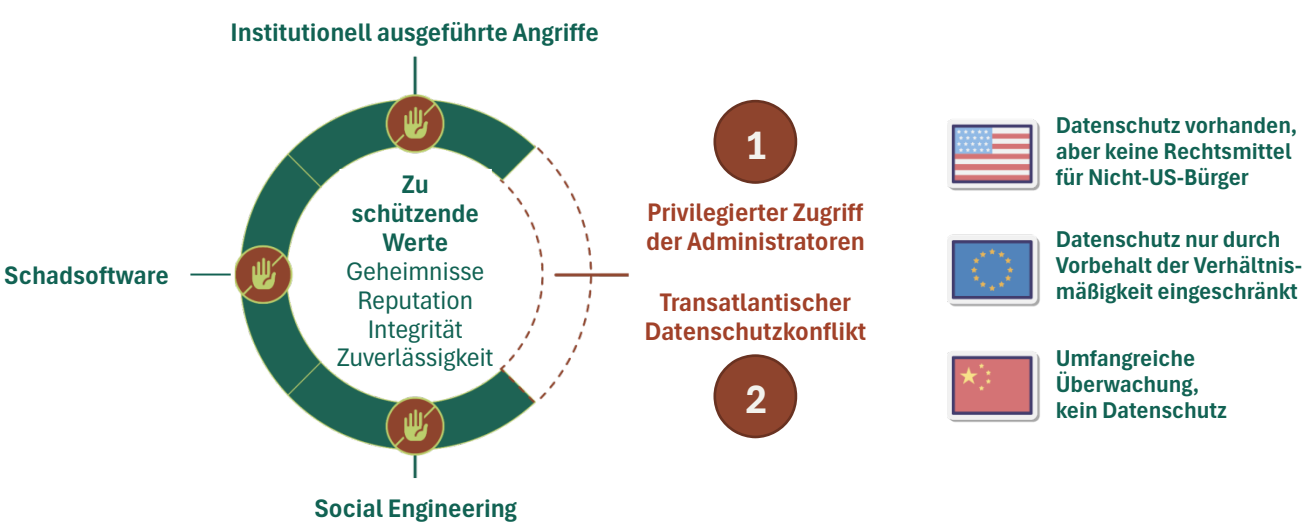
Trotz exponentiell sinkendem Energiebedarf je Rechenaufgabe, ein Fortschritt, der durch die anhaltende Miniaturisierung in der Mikroelektronik möglich ist, verdoppelt sich der Energie- und Elektrizitätsbedarf der Rechenzentren - auch ohne die Verbrauche der Kryptowährungen - innerhalb von 10 Jahren. Die Erzeugung und Verteilung des elektrischen Stromes sowie die Herstellung der notwendigen Hardware macht inzwischen bereits mehr als 3 % des ausgestoßenen Treibhausgases CO_2 aus.



So sehr IT und künstliche Intelligenz für Effizienzsteigerungen benötigt werden, trägt die Nutzung der Cloud-Technologie doch einen erheblichen Teil zur Klimakatastrophe bei. Die Ausstöße von Treibhausgasen durch das Cloud-Computing müssen auf das technisch mögliche Minimum reduziert werden.

1.2 Fehlende digitale Souveränität

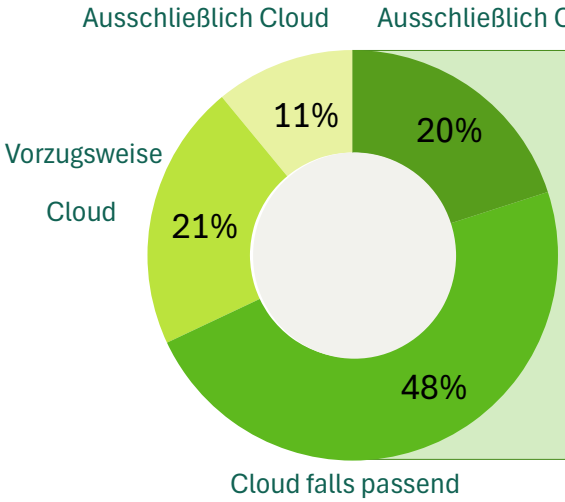
Datensouveränität ist einerseits durch Sicherheitslücken bei der Technik und andererseits durch nicht zueinander passende Rechtssysteme in den USA und Europa nicht gegeben. Cloud-Betreiber und Administratoren haben vielfach unnötig privilegierten Zugriff auf Daten und Code der Nutzer - nicht weil diese besonders vertrauenswürdig wären, sondern weil herkömmliche Technik diesen Zugriff nicht ausschließen kann. Nach zwei Urteilen des EuGH besteht unverändert ein ungelöster transatlantischer Datenschutzkonflikt.



2. Cloud-Strategien und -Bedarfe

2.1 Cloud-Zurückhaltung und On-Premises Server

Der Bitkom-Verband hat 2024 bei einer Befragung von Unternehmen in Deutschland folgende Anworten auf die Frage erhalten: Welcher der folgenden Ansätze trifft am ehesten auf die Cloud-Aktivitäten in Ihrem Unternehmen zu?



Gründe für die Zurückhaltung bei mehr als 50% der Unternehmen:

- Sorge, dass vertrauliche Daten abgegriffen und missbraucht werden
- Sorge vor Abhängigkeit bzgl. Nutzungsfähigkeit der Daten und Dienste
- Sorge vor „Vendor Lock-In“ und hohen Preisen

Gesucht: Angebot, das die Vorteile der Cloud mit den Vorteilen von On-Premises verbindet

2.2 Nachweisbare digitale Souveränität

Definition „Digitalen Souveränität“
durch das Bundesministeriums für Digitales: Die Nutzer sollen ihre Rollen im Digitalen

- selbständig
- selbstbestimmt
- sicher

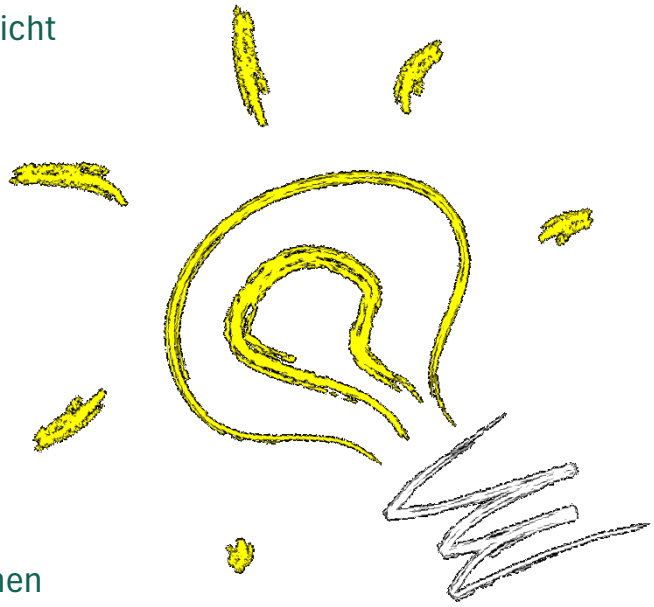
ausüben können.

Solche Definitionen sind für die Praxis zu unverbindlich

Definition „Verifizierbare Digitale Souveränität“ konkretisiert:

1. Manipulationssicherer Schutz der Vertraulichkeit und Integrität (Confidential Computing)
2. Hoher Schutz gegen Datenverlust (anbieterunabhängiger Backup und kryptografische Resilienz)
3. Hohe Verfügbarkeit des Dienstes und testbare Wechselmöglichkeit zu anderen Anbietern (Anwendungen mit Vorteil in Open Source Software)

3. Lösungsansätze und EU-Innovation



Im Bereich Cloud können einige der Fachleute nicht daran glauben, dass Innovationen außerhalb der großen Player (Amazon Web Services, Microsoft Azure, Google Cloud, die alle aus den U.S.A. stammen, und Alibaba aus China) erfolgsversprechend sein könnten. Der technische Vorsprung, der sich durch die Finanzkraft dieser Unternehmen ergebe, sei schlicht zu übermächtig. Man habe sich nun mal mit der stets vorhandenen Möglichkeit von Wirtschaftsspionage und Überwachung zu arrangieren.

Andere Akteure im Bereich Datenschutz versuchen auf dem Rechtsweg europäische Datenschutzstandards durchzusetzen. Insbesondere durch die Urteile des Europäischen Gerichtshofs, Schremms I und Schremms II, müssen jeweils die Regelungen zum transatlantischen Datenaustausch neu definiert werden.

Wir können zeigen, dass durch mutiges Entwickeln von innovativer Cloud-Technik und dem Aufbau eines neuartigen Betriebskonzepts wettbewerbsfähige Cloud-Plattformen geschaffen werden können. Mit solchen Innovationen können die Nachfrage nach besonders nachhaltigem Computing befriedigt und der Bedarf an Infrastruktur zur Verarbeitung besonders schutzbedürftiger Daten gedeckt werden.

3.1 Wir denken, für diese Innovationsaufgabe müssen Sektorengrenzen überwunden werden, um neue Hebel für Wettbewerbsfähigkeit zu schaffen.

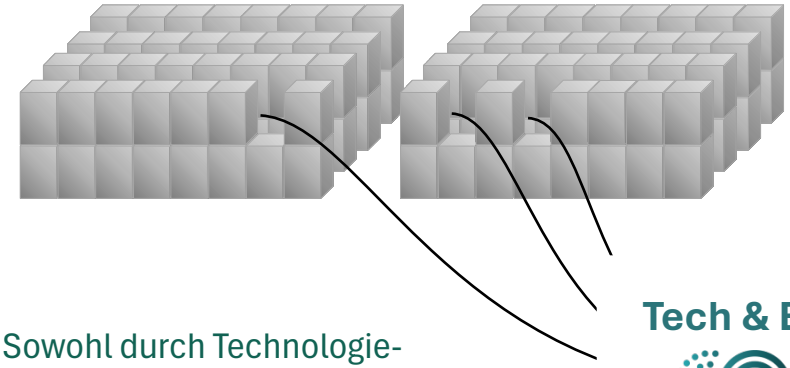
3.2 Wir binden in unsere Lösungen Open Source Software ein, um die Kräfte der gesamten Industrie zu nutzen.

3.3 Wir versuchen bereits die technische übernächste Generation zu antizipieren, um unseren technischen Vorsprung zu halten.

» Cloud-Server sollten dort betrieben werden, wo deren Abwärme mit hohen Wirkungsgraden genutzt werden kann und regenerativ erzeugter Strom zu günstigen Konditionen, d.h. nicht primär über das Stromnetz, zur Verfügung steht.

Dr. Hubert Jäger, Mitgründer und Geschäftsführer der real-cis GmbH

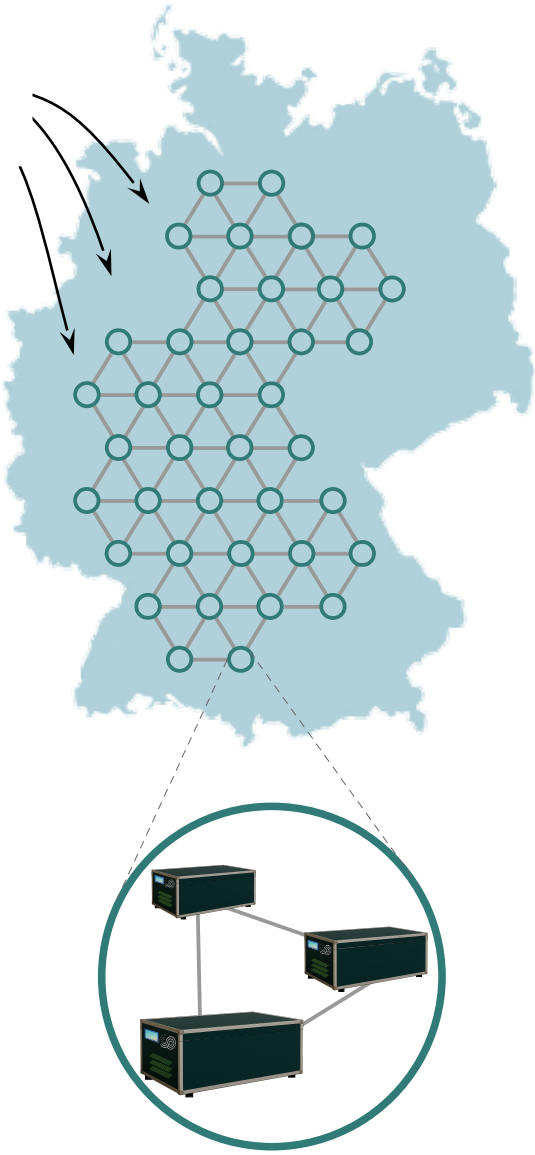
4. Verteilung der Server in der Fläche



Rechenzentren mit tausenden von Servern werden nicht mehr die einzige Infrastruktur für Cloud-Dienste sein.

Tech & Biz Innovation

Sowohl durch Technologie- als auch Geschäftsinnovationen steht immer mehr Rechenleistung am „Edge“ (am Rand) des Netzes zur Verfügung: Es bilden sich „Cluster of Clusters“ aus hunderten neuartiger, hochsicherer und nachhaltig betreibbarer Edge Cloud Module.



4.1 Neuartiger Zugriffsschutz schafft Vertrauen

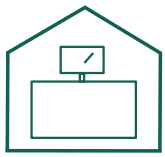
Da die Server außerhalb der Rechenzentren nicht mehr durch Zutrittskontrollen geschützt sind, ist für diese Edge Cloud Module ein neuartiger physischer Zugriffsschutz mit einem so genannten kryptografischen Perimetersiegel notwendig. Dieser Schutz vereitelt selbst raffinierteste Angriffsversuche auf die Integrität der Server.

4.2 Neuartige Edge Cloud Module

Die neuartigen Edge Cloud Module sind so ausgestattet, dass eine völlig unkomplizierte Plug & Play-Installation im Feld möglich ist.

Cluster aus mehreren Edge Cloud Modulen

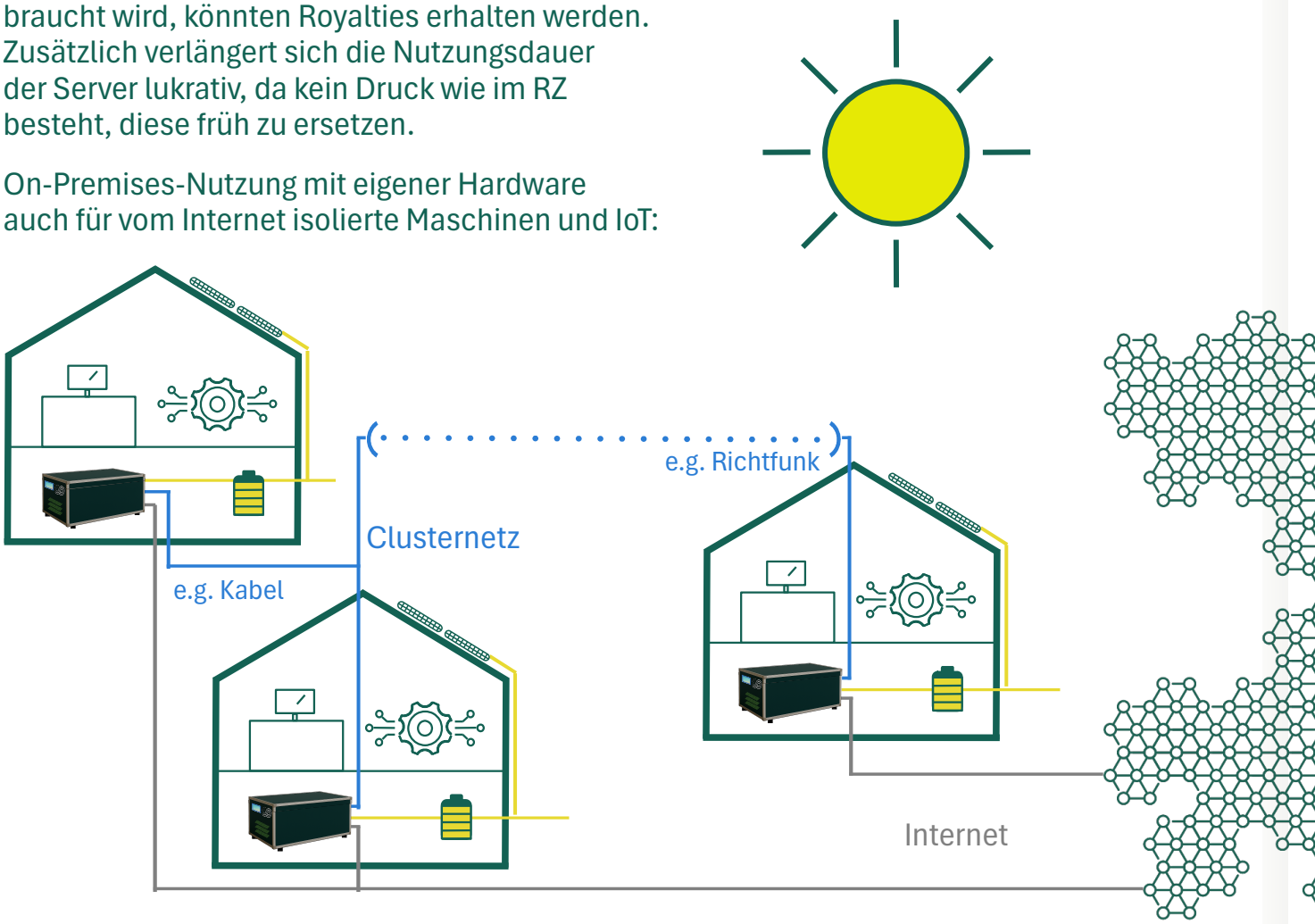
4.3 Symbiose der Module mit Photovoltaik



Nutzung der Edge Cloud über das Internet ohne eigene Hardware

Die beste Lösung, um Computing nachhaltig zu machen, ist, die Cloud-Server direkt dort zu betreiben, wo regenerative Elektrizität lokal zur Verfügung steht, sodass das Stromnetz weder belastet wird, noch bezahlt werden muss. Mehr noch, für Elektrizität, die durch fremde Workload verbraucht wird, könnten Royalties erhalten werden. Zusätzlich verlängert sich die Nutzungsdauer der Server lukrativ, da kein Druck wie im RZ besteht, diese früh zu ersetzen.

On-Premises-Nutzung mit eigener Hardware auch für vom Internet isolierte Maschinen und IoT:



4.4 Best Practice Confidential Computing

Die größte Bedrohungen der Vertraulichkeit und Integrität der Daten und der Ausführungslogik geht nicht von physischen Manipulationen der Infrastruktur, sondern von den Cyber-Angriffen aus, die über Schwachstellen im Betriebssystem und/oder der Anwendungssoftware möglich sind. Solche Sicherheitsschwachstellen sind entweder noch nicht lange Zeit entdeckt und noch so neu, dass sie bislang nur den Angreifern bekannt sind („zero day exploits“). Oder die Schwachstellen sind schon länger bekannt, aber noch nicht durch Software-Korrekturen beseitigt.

Der beste Schutz gegen die Bedrohungen durch diese Schwachstellen ist das so genannte Confidential Computing, bei dem nicht nur die Daten während ihrer Übertragung zu den Servern und bei der Festspeicherung verschlüsselt werden, sondern auch während der Verarbeitung im Arbeitsspeicher und auf den Systembussen. So wird den Angreifern, selbst wenn sie die logische Herrschaft über die Server erlangen können, der Zugriff zu der die Daten verarbeitende Software und den Daten der Nutzer verwehrt.

4.5 Schlüssel sicher und resilient bereitstellen

Zum „Best Practice Confidential Computing“ gehört, dass nicht nur alle Daten außerhalb der Prozessor-Chips verschlüsselt sind, sondern auch die Systemsoftware für Confidential Computing nicht manipuliert werden kann und die Schlüssel zum Schutz der im Festspeicher abgelegten Daten für niemand zugänglich sind. Um diese Standards auch für hochverfügbare Cloud-Dienste in redundanten Strukturen erfüllen zu können, sind eine gemeinsame, besonders vertrauenswürdige Quelle für Schlüssel und ein Dienst zur kryptografischen Attestierung erforderlich. Da auch bei ihrer Initialisierung niemand Kenntnis von kryptografischen Geheimnissen erlangen und für höchste Resilienz die Quelle hoch skalieren kann, wird sie als „BetterKey.Cloud“ bezeichnet.

4.6 Kryptografische Verifikation der Integrität

Bislang kann sich ein Nutzer eines Cloud-Dienstes nur mit den Erklärungen des Cloud-Anbieters und der zum Dienst passenden Internetadresse von der Vertrauenswürdigkeit und Integrität des Dienstes überzeugen. Die so genannte „Attestierung“ beim Confidential Computing eröffnet den Nutzern die Möglichkeit, sich mit kryptografischer Verlässlichkeit davon zu überzeugen, dass auf sicheren Prozessoren tatsächlich die den Nutzern bekannte, nicht-manipulierte Anwendungssoftware ausgeführt wird.

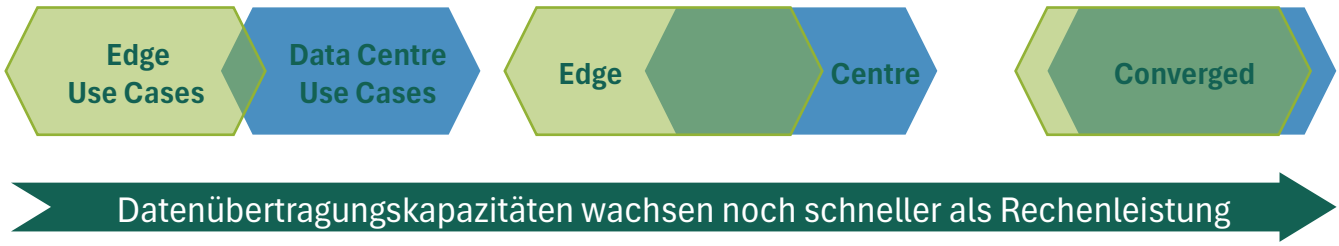
4.7 Automatisierung senkt Personalkosten

Da die Server-Module zentral gefertigt und nach einem Lebenszyklus überarbeitet werden, ist im Feld vor Ort kein Einsatz von IT-Personal zur Inbetriebnahme oder zum Austausch notwendig. Die Module fügen sich automatisch in ein Netz von Modulen ein. Die kryptografische Versiegelung der Module garantiert Sicherheit gegen Manipulation.

5. So sieht die Zukunft der Cloud aus

5.1 Mehr verteilte Recheninfrastruktur mit sektorübergreifend optimierter Nachhaltigkeit

5.2 Auf die Vernetzung kommt es an



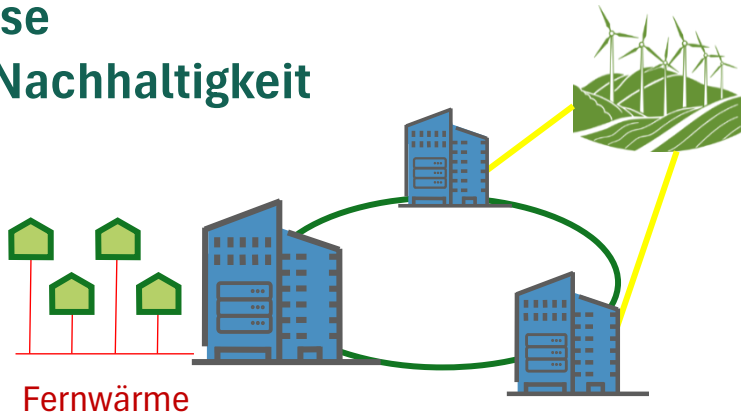
Die Verteilung der Cloud-Server auf geografisch verteilte Immobilien bietet die genannten energetischen und ökonomischen Vorteile, stellt aber auch Herausforderungen an die Vernetzung der Server-Infrastruktur. Mittel- und langfristig ist von einem für die Verteilung vorteilhafterem Verhältnis von digitaler Übertragungskapazität zu Rechenkapazität auszugehen als dies heute der Fall ist, da die Rechenleistung je gleiche Kosten mit dem so genannten „Moore‘schen“ Gesetz wächst, also eine Verdopplung in zwei Jahren erfolgt. Die digitale Übertragungskapazität je Kosten verdreifacht sich im selben Zeitraum sogar.

Praktisch werden in Edge Clouds mehrere Module als Cluster innerhalb eines Standorts miteinander vernetzt, wobei die Module in Räumen mit möglichst unabhängiger Stromversorgung und in unterschiedlichen Feuerzonen aufgestellt werden.

weniger Rechenzentren, diese allerdings mit verbesserter Nachhaltigkeit

Nachhaltigkeit

kann nur begrenzt gesteigert werden



Cloud-Dienste können mit solch neuartigen Edge Clouds wie gewöhnliche Cloud-Dienste angeboten werden, sofern die durch die Vernetzung der Module miteinander gegebenen Skalierungsmöglichkeit nicht überschritten wird.

5.3 Resilienz kritischer Infrastruktur steigern

Ein weiterer Vorteil einer Verteilung und Vernetzung der Rechenressourcen besteht in der Vermeidung von Risiken durch die starke Konzentration kritischer Infrastruktur in ein oder zwei Rechenzentren. Durch die Verteilung der Ressourcen wird die Resilienz gestärkt.

5.4 Ihre Vorteile, heute schon zu starten

BetterEdge
Verifiable Sovereign Computing

- Ist strukturell kostengünstiger als eine Rechenzentrums-Cloud
- Bietet verifizierbare Souveränität über Daten und Rechenressourcen
- Räumt Sicherheitsbedenken aus (Confidential Computing)
- Gewährleistet mit „cloud native“-Schnittstellen Portabilität
- Ist so nachhaltig wie irgend möglich

5.3 Ihre Vorteile, heute schon zu starten (Fortsetzung)

Fall 1:
Sie betreiben heute aus Sicherheitsgründen Software On-Premises:

→ Sie vereinfachen Ihre Installationsprozesse und erhöhen weiter die Sicherheit
→ Sie verbessern den Ausnutzungsgrad der Hardware und sparen so Serverkosten
→ Sie können Ihre Workload vergleichbar mit einer Rechenzentrums-Cloud skalieren und erhalten Royalties für Kapazitäten Ihrer Server, die Sie für Dritte freigeben

Fall 2:
Sie wollen keine eigene Hardware installieren, suchen aber Rechenkapazität, die als Green Asset geltend gemacht werden kann:

→ Die Reduktion von CO_2-Emissionen durch IT- und Cloud-Server kann sofort beginnen
→ Sie registrieren Ihr fortschrittliches Handeln bei Ihrer Bank als „Green Asset“
→ Sie führen die Nachhaltigkeit (Klimafreundlichkeit und Sicherheit) als Leistungsmerkmal für Ihre Kunden an

Fall 3:
Sie wollen keine eigene Hardware installieren, suchen aber Rechenkapazität, die höchsten Sicherheitsanforderungen genügt und souverän betrieben werden kann:

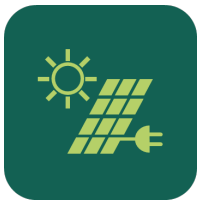
→ Best Practice Confidential Computing schließt den Betreiber technisch aus
→ Sie können ein unabhängiges Datenbackup mit kryptografischer Resilienz einrichten
→ Sie können die Vertraulichkeit und Integrität der Software und der durch sie verarbeiteten Daten Ihren Kunden kryptografisch hart nachweisen

Betreiber kann nicht mitlesen

EU-Recht uneinge-schränkt durchsetzbar

Sicherheit gegen Manipulation

Wärme aus der Cloud



Symbiose mit Photovoltaik

CO_2-Sparen durch Langlebigkeit

BetterEdge

Verifiable Sovereign Computing

Trusted Execution Domains (TEDaaS)

Mit ”Confidential Computing“ geschützte “Virtual Machines” als sichere Ausführungs-umgebungen für IT-Anwendungen oder Software für SaaS-Angebote

In Zukunft weitere Dienste

- Database as a Service
- Backup as a Service
- Functions as a Service
- Acceleration as a Service

Häufig gestellte Fragen:

Welche konkreten Möglichkeiten zur Evaluation des Angebots bestehen bereits?

→ Prototypischer **Betrieb einer Workload** (einer Software, einer Anwendung, ggf. eines Partners) für eine vereinbarte Zeit mit abgestimmten „Service Level Agreements“

→ Prototypischer **Betrieb der Confidential Computing Systemsoftware** in Ihrem Rechenzentrum. Betrieb beliebig vieler gesicherter Ausführungsumgebungen

→ Prototypischer **Betrieb eines luftgekühlten Edge Cloud Moduls**, prototypischer Betrieb von Workload auf dieses Modul

→ Prototypischer **Betrieb eines wärmekoppelnden Moduls**, prototypische Einbindung in die Heiz-infrastruktur und prototypischer Betrieb von Workload auf dieses Modul

→ Planung von **Immobilienentwicklungen**

Welche Geschäftsmodelle kommen für Partner in Frage?

→ Buchung von Cloud-Rechenleistung bei real-cis

→ Kauf von Edge-Cloud-Modulen, die real-cis für Sie betreibt, lukrative Royalties auf Cloud-Dienste, die mit Hilfe Ihrer Hardware für Dritte geleistet werden (1€/kWh)

→ Betrieb einer eigenen Edge Cloud für „Verifiable Sovereign Computing“

Definitionen:

„Cloud“	Bereitstellung von Rechenleistung über das Internet als Dienstleistung
„Data Centre Cloud“	Bereitstellung von Rechenleistung als Dienst aus Rechenzentren
„Edge Computing“	Rechenleistung außerhalb Rechenzentren oder in Geräten wird genutzt
„Edge Cloud“	Bereitstellung von Rechenleistung als Dienst, von außerhalb von Rechenzentren
„Cloud Edge Continuum“	Cloud mit Ressourcen innerhalb und außerhalb von Rechenzentren
„IaaS“	Infrastructure as a Service
„PaaS“	Platform as a Service
„XaaS“	X-things as a Service (Database as a Service, Functions as a Service, etc.)
„SaaS“	Software (IT-Anwendungen) as a Service
„cloud native“	Weitgehende Abstraktion der Infrastruktur durch Cloud-Dienste für den Betrieb skalierbarer Anwendungen
„Hyperscaler“	Höchstskalierende Cloud Service Provider (CSP)

BetterEdge

Verifiable Sovereign Computing

real-cis GmbH
München und Frankfurt
Rheinstr. 5, D-63225 Langen
info@real-cis.com, www.real-cis.com
+49 6103 90298-0