

MÜNCHEN, 06.05.2025

SICHERE CLOUD-NUTZUNG EINE KRYPTOLOGISCHE PERSPEKTIVE

Dr. Matthias Minihold (Referatsleiter Kryptologie)
Agentur für Innovation in der Cybersicherheit GmbH

DAS CLOUD-ZEITALTER

„CLOUD COMPUTING IST DAS RÜCKGRAT DER DIGITALISIERUNG“

DIGITALISIERUNG IM CLOUD-ZEITALTER BEDEUTET:

- ⊕ EXPONENTIELLER **DATENZUWACHS** (INDUSTRIE, MEDIZIN, VERWALTUNG, ...)
- ⊕ VERLAGERUNG **SENSIBLER DATEN IN GEMEINSAM GENUTZTE CLOUDS**

ANFORDERUNGEN: VERTRAULICHKEIT, INTEGRITÄT UND VERFÜGBARKEIT

KERNFRAGE: WIE BLEIBT **SICHERHEIT UND DATENSCHUTZ** GEWAHRT?



ZIEL: SICHERE SPEICHERUNG, NUTZUNG & VERARBEITUNG IN DER CLOUD.

ZIELE FÜR EUROPA / DEUTSCHLAND

SOUVERÄNITÄT, ENTWICKLUNG & RECHT

1. TECHNOLOGISCHE SOUVERÄNITÄT

- ⊕ MINIMIERUNG DER ABHÄNGIGKEITEN (**VON TECH-GIGANTEN**)
- ⊕ AUFBAU EIGENER **KRYPTOGRAPHISCH** ABGESICHERTER CLOUDLÖSUNGEN
- ⊕ FÖRDERUNG NATIONALER UND EUROPÄISCHER **SICHERHEITSSTANDARDS**

2. ZUKUNFT & ENTWICKLUNG

- ⊕ INTENSIVIERUNG **INTERDISZIPLINÄRER FORSCHUNG** (FÜR BEDARFSTRÄGER)
- ⊕ VERBINDUNG **AKADEMISCHER FORSCHUNG & INDUSTRIEANWENDUNG**

3. RECHTLICHER & REGULATORISCHER RAHMEN

- ⊕ RECHTSSICHERHEIT BEI **SENSIBLER** DATEN-VERARBEITUNG IN DER CLOUD
- ⊕ GARANTIE & **DSGVO-KONFORMITÄT** KRYPTOGRAPHISCHER PROTOKOLLE







WOZU KRYPTOGRAPHIE

„DAS KLASSISCHE **VERTRAUENSMODELL BRICHT** IN DER CLOUD ZUSAMMEN“

KLASSISCH: PERIMETERSCHUTZ, ZUGRIFFSKONTROLLE & INFORMATIONSSICHERHEIT

CLOUD: DATEN „AUßERHALB EIGENER KONTROLLE“ → VIELE, NEUARTIGE RISIKEN

KRYPTOGRAPHIE BILDET DAS FUNDAMENT:

-  **SCHUTZ** UNABHÄNGIG VOM ORT DES **SPEICHERS** 
-  **SICHERUNG** DER ÜBERTRAGUNG IM **NETZWERK** 
-  **SICHERHEIT** AUCH WÄHREND DER **VERARBEITUNG** 

WAS IST ENCRYPTED COMPUTING?

...UND WARUM IST ES EINE INNOVATIVE CLOUD-TECHNOLOGIE?

	Speicherung (data at rest)	Übertragung (data in transit)	Berechnung (data in use)
„Klassische“ Kryptographie	✓	✓	✗
Encrypted Computing	✓	✓	✓

TECHNOLOGIEN (AUSWAHL):

- ① TRUSTED EXECUTION ENVIRONMENT (TEE)
- SICHERE MEHR-PARTEIEN BERECHNUNG (MPC)
- VOLL-HOMOMORPHE VERSCHLÜSSELUNG (FHE)

BEISPIELE FÜR ZIVILE ANWENDUNGEN

(Auszug)



MEDIZINISCHE FORSCHUNG

- GENOMIK, GESUNDHEITSDATEN (Z. B. MELLODDY-PROJEKT)



FINANZWESEN

- PRIVATSPHÄRE-ERHALTENDE KREDITWÜRDIGKEIT- & BETRUGSERKENNUNG



INDUSTRIE & INTERNET-OF-THINGS (IOT)

- SCHUTZ GEISTIGEN EIGENTUMS VERTEILTER INDUSTRIEPROZESSE

HERAUSFORDERUNGEN FÜR ENCRYPTED COMPUTING

SKALIERUNG, VERTRAUEN UND RECHTSLAGE

1. EFFIZIENZ & SKALIERUNG



HOMOMORPHE VERSCHLÜSSELUNG: **ALGORITHMISCH EFFIZIENZ STEIGERN**



SICHERE MEHR-PARTEIEN BERECHNUNG: **KOMMUNIKATIONSAUFWAND SENKEN**

2. VERTRAUENSWÜRDIGE UMGEBUNG & KRYPTOAGILITÄT



NOTWENDIGKEIT **AUDITIERBARER & OFFENER IMPLEMENTIERUNGEN**



MATHEMATISCHE ERKENNTNISSE, **KRYPTANALYSE** & SEITENKANALANGRIFFE

3. RECHTSLAGE & DATENFLÜSSE



INTERNATIONALE **CLOUDANBIETER** ↔ **DATENSCHUTZ** EUROPÄISCH & NATIONAL

ENTWICKLUNGEN IM BEREICH ENCRYPTED COMPUTING

„CLOUD-NUTZUNG IST BALD **UNVERZICHTBAR**, SIE MUSS ABER **SICHER** SEIN.“

KURZFRISTIG (0–3 JAHRE 🧙)

- ⊕ EINSATZ VON STANDARDS DER **POST-QUANTUM-KRYPTOGRAPHIE** (NIST PQC)
- ⊕ IM **CLOUD-BACKEND**: VERBREITUNG VON TRUSTED EXECUTION ENVIRONMENTS (TEE)
- ⊕ IN **CLOUD-FRONTENDS**: ERWEITERUNG UND **KRYPTOGRAPHISCHER APIs**

MITTELFRISTIG (3–5 JAHRE 🧙🧙)

- ⊕ HYBRIDE **KOMBINATIONEN** VON ENCRYPTED COMPUTING (HE, MPC) MIT TEES
- ⊕ **ERSTE MARKTFÄHIGE LÖSUNGSSZENARIEN** (FÜR SPEZIALFÄLLE)

LANGFRISTIG (5–10 JAHRE 🧙🧙🧙)

- ⊕ **VERSCHLÜSSELTE DATENVERARBEITUNG** DURCH KI UND FÖDERIERTE LERNMODELLE
- ⊕ **GENERELLERE LÖSUNGEN** & UMBAU KRITISCHER **INFRASTRUKTUR FÜR PQC & EC**

ZWISCHENFAZIT

... ZUKÜNFTIGER **CLOUD-SICHERHEITSKONZEPTE** UND ZU **ENCRYPTED COMPUTING**

BISHER:

ANWENDUNG KLASSISCHER **SICHERHEITSKONZEPTE & KRYPTOGRAPHIE**

DOCH:

„**CLOUD COMPUTING** IST DAS **RÜCKGRAT DER DIGITALISIERUNG.**“

„DAS KLASSISCHE **VERTRAUENSMODELL BRICHT** IN DER CLOUD **ZUSAMMEN.**“

„CLOUD-NUTZUNG IST BALD **UNVERZICHTBAR**, SIE MUSS ABER **SICHER** SEIN.“

DAHER:

ENTSCHIEDENES, INNOVATIVES & DISRUPTIVES SECURITY-BY-DESIGN!