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?

TIEL: 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
- Garantien & DSGVO-Konformität kryptographischer Protokolle

WOZU KRYPTOGRAPHIE

"Das klassische Vertrauensmodell bricht in der Cloud zusammen"

Klassisch: Perimeterschutz, Zugriffskontrolle & Informationssicherheit

CLOUD: DATEN "AUBERHALB EIGENER KONTROLLE" → VIELE, NEUARTIGE RISIKEN

KRYPTOGRAPHIE BILDET DAS FUNDAMENT:



SCHUTZ UNABHÄNGIG VOM ORT DES SPEICHERS 🗀





SICHERUNG DER ÜBERTRAGUNG IM NETZWERK



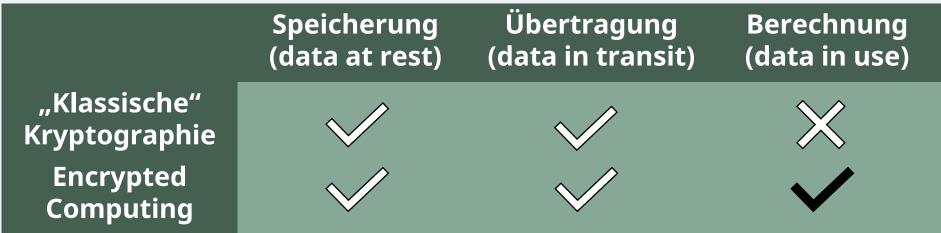


SICHERHEIT AUCH WÄHREND DER VERARBEITUNG X



WAS IST ENCRYPTED COMPUTING?

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



TECHNOLOGIEN (AUSWAHL):

- 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. EFFIZENZ & 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** s

KURZFRISTIG (0–3 JAHRE (2))

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