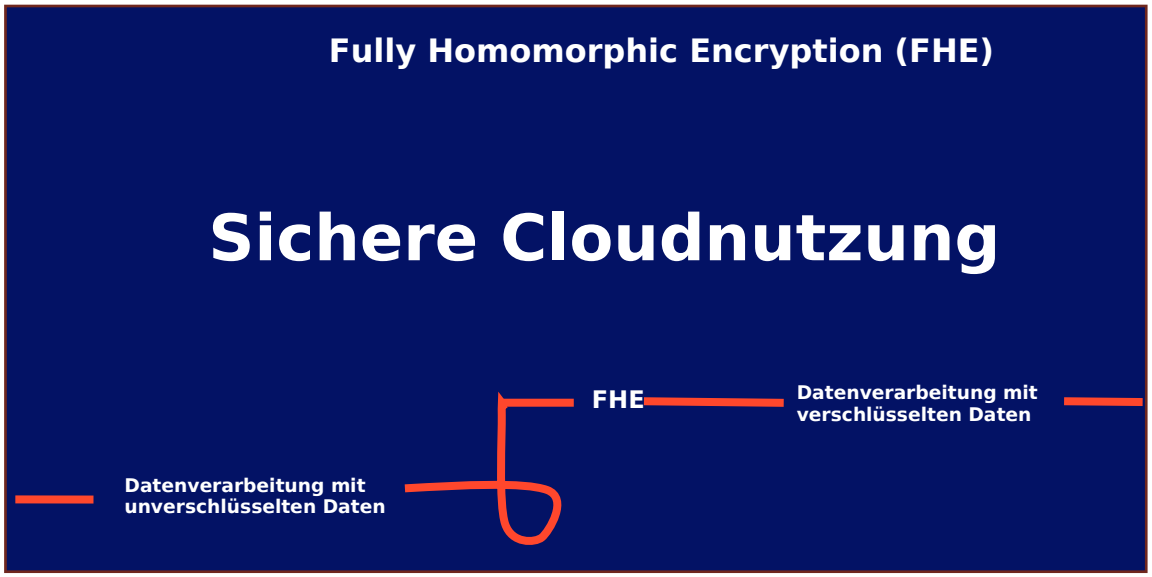
Cloud meets Security - Public Cloud Nutzung ohne Risiken

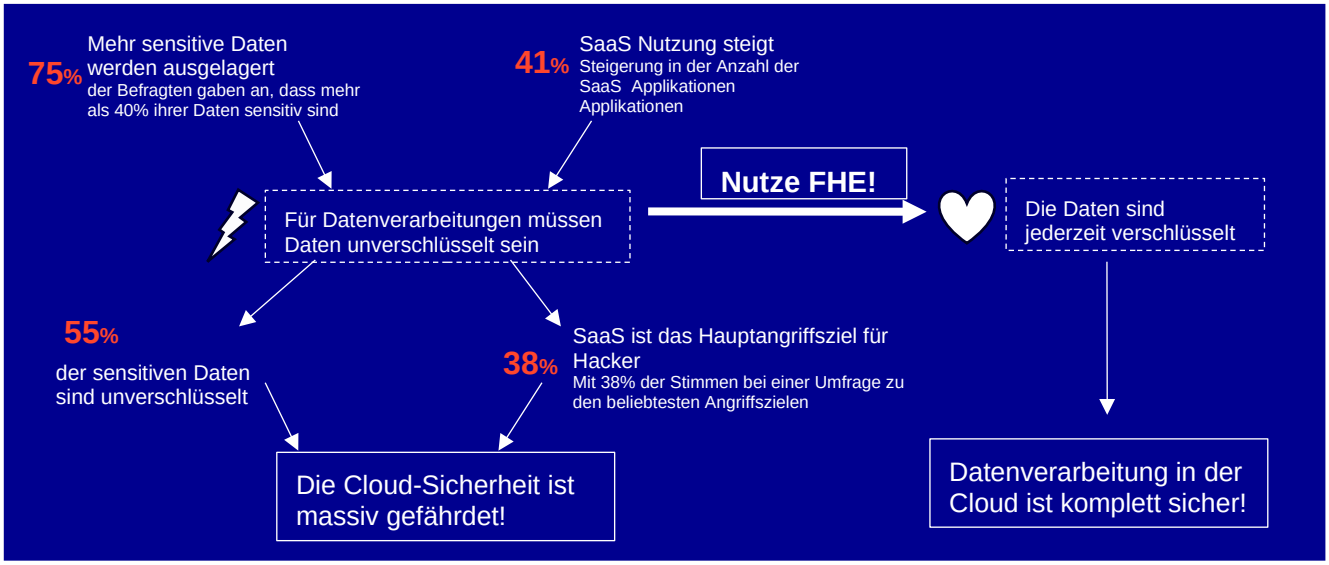


1 Kurzversion

Fully Homomorphic Encryption (FHE) ermöglicht Berechnungen auf quantensicher verschlüsselten Daten – ohne jemals die Verschlüsselung aufzuheben! Das bedeutet, dass beispielsweise Machine-Learning-Analysen jetzt sicher in der wettbewerbsintensiven Cloud durchgeführt werden können. Kostenbewusst und ohne Risiko.

2 Die Public Cloud ist unsicher

Aktuelle Verschlüsselungstechniken erlauben es *nicht* Berechnungen auf *verschlüsselten Daten* durchzuführen. Werden also aktuell Software as a Service Anwendungen in der Cloud genutzt, müssen die Daten dafür im Klartext in der Cloud vorliegen. Hacker können also *unverschlüsselte* Daten abgreifen!



3 Fully Homomorphic Encryption löst das Sicherheitsproblem der Cloud

Fully Homomorphic Encryption ermöglicht mit Encryption at Processing revolutionäre Anwendungen von verschlüsselten Daten in der Public Cloud. Sensible Daten müssen damit nicht mehr für eine Berechnung in der Cloud entschlüsselt werden. Stattdessen werden sie verschlüsselt in die Cloud übertragen, *verschlüsselt verarbeitet* und verschlüsselt zurückgesendet. Die Daten sind also zu jedem Zeitpunkt sicher vor Angreifern.

4 Wie entwickelt sich die Technologie in der Zukunft weiter?

Obwohl Fully Homomorphic Encryption derzeit noch anspruchsvolle Anforderungen an Rechenleistung und Speicher stellt, bleibt die Entwicklung nicht stehen. Intensive Forschung und kontinuierliche Hardware-Verbesserungen deuten auf vielversprechende Fortschritte in der Zukunft hin. FHE eröffnet die Tür zu vielfältigen Anwendungsmöglichkeiten, einschließlich der Evaluation von Machine Learning Modellen, auf verschlüsselten Daten in der Cloud. Dies gewinnt an Bedeutung in einem Umfeld, in dem Cloud-Anbieter im Preiskampf und unter starkem Wettbewerbsdruck stehen, um effiziente und kostengünstige Lösungen anzubieten.

In Zukunft eröffnen sich mit Multi-Key-FHE spannende Anwendungsfelder, in denen sichere Datenanalysen zwischen nicht vertrauenden Parteien ermöglicht werden. Dies ermöglicht insbesondere kundenübergreifende Datenanalysen, ohne dass Daten eines Kunden von einem anderen Kunden eingesehen werden können.

5 Wie kann die Technologie aktuell genutzt werden?

Datenanalysen mittels Machine Learning können jetzt auf verschlüsselten Daten ohne Datenschutzbedenken in die kostengünstige Public Cloud ausgelagert werden. Damit kann nicht nur die extreme Flexibilität und Skalierbarkeit, sondern auch der enorme Preiskampf in diesem Markt bestmöglich genutzt werden.

6 Unsere Website als erste Anlaufstelle

Guckt gerne auf unserer Website zu dem Thema vorbei. Dort findet ihr Vorträge, Codebeispiele und eine ausführliche Ausarbeitung.