Edgeless Systems

Confidential Computing für den öffentlichen Sektor

Souverän und sicher in die Public Cloud

Problemstellung

IT-Sicherheit und Datenschutz sind zentrale Hürden für die Nutzung von Cloud-Services im öffentlichen Sektor

Public Clouds bedeuten, dass IT-Dienste aus Rechenzentren Dritter bereitgestellt werden. Diese Infrastruktur wird mit anderen Nutzern geteilt und – selbst in Deutschland – von unbekannten Personen verwaltet.

Herkömmliche Sicherheitskonzepte basieren auf Zugriffskontrollen und der Verschlüsselung von Daten während Speicherung und Übertragung. Diese Maßnahmen verhindern jedoch keinen Zugriff Dritter über die Cloud-Infrastruktur, weil Daten für die Verarbeitung in der Cloud im Klartext vorliegen müssen. Anbieter und potenzielle Angreifer könnten daher Zugriff auf die Daten erlangen. Ein Cloud-Administrator könnte beispielsweise seinen Zugriff missbrauchen oder ein Mitnutzer könnte Sicherheitslücken ausnutzen und unbefugt auf Daten anderer Mandanten zugreifen.

Public Clouds sind wegen ihrer Skalierbarkeit und Resilienz, besonders angesichts des IT-Fachkräftemangels, zentral für die Digitalisierung des öffentlichen Sektors. Wie können sie souverän und sicher genutzt werden?

Lösung

Confidential Computing ermöglicht eine nachweisbar verschlüsselte Datenverarbeitung in der Cloud – unabhängig vom Cloud-Anbieter

Confidential Computing kombiniert Funktionen moderner Hardware mit optimierter Software. Der Prozessor verhindert ein Auslesen der Daten durch durchgehende Verschlüsselung, auch während der Verarbeitung (Laufzeitverschlüsselung) und stellt ein kryptografisches Zertifikat aus, das Vertraulichkeit, Integrität und Authentizität der Daten bestätigt (Fernattestierung).

Die für Confidential Computing optimierte Software von Edgeless Systems verschlüsselt und attestiert komplette Kubernetes-Cluster. Dies garantiert Datensicherheit und Integrität in jeder Cloud, unabhängig vom Anbieter. Als Open-Source-Software ist sie vollständig transparent und überprüfbar.

In Übereinstimmung mit den Zielen der Deutschen Verwaltungscloud-Strategie sowie der Cloud-Strategie des BSI ist die Confidential-Computing-Software von Edgeless Systems:

- ✓ Secure-by-Design
- ✓ Cloud-agnostisch, ohne Anbieter-Lock-In
- ✓ Konform mit Standards (z.B. Kubernetes)
- ✓ Open-source
- ✓ Made in Germany

Edgeless Systems bietet zum Beispiel mit Constellation die einzige für Confidential Computing optimierte und von der Cloud Native Computing Foundation zertifizierte Kubernetes-Distribution.

Ergebnis

Überprüfbarer Schutz vor Datenzugriffen aus der Infrastruktur

Mit Confidential Computing sind Daten jederzeit geschützt – während der Speicherung, der Übertragung und der Verarbeitung. Dieser Schutz bleibt auch bei physischem oder virtuellem Zugriff auf die Infrastruktur durch Unbefugte bestehen. Zudem stellt Confidential Computing eine Mandantentrennung sicher, sodass Nutzer nicht auf die Daten anderer zugreifen können.

Laut einem aktuellen Datenschutzgutachten kann Confidential Computing bei richtiger Umsetzung als Methode zur Anonymisierung personenbezogener Daten betrachtet werden.

Anwendungsbeispiele

Elektronische Patientenakte: Sichere Daten für Millionen Versicherte

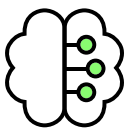
In Deutschland muss jede Krankenkasse ihren Kunden eine elektronische Patientenakte (ePA) bereitstellen. Über eine App sind alle Daten, wie Medikationshistorien und Untersuchungsberichte, zugänglich. Aufgrund der Sensibilität dieser Daten fordert die Gematik einen strikten Betreiberausschluss mittels „vertrauenswürdiger Ausführungsumgebung“. Durch den Einsatz von Confidential-Computing-Hardware und Software von Edgeless Systems wird gewährleistet, dass Backend-Infrastrukturanbieter auf keine Patientendaten zugreifen können.

OpenDesk: Der souveräne Arbeitsplatz sicher in der Cloud

Die deutsche Regierung gründete 2022 das Zentrum Digitale Souveränität (ZenDiS) zur Koordination von Open-Source-Projekten in der öffentlichen Verwaltung. ZenDiS betreut openDesk, eine souveräne Arbeitsplatzlösung mit Tools für E-Mail, Videokonferenzen und Projektmanagement. OpenDesk kann mit Confidential-Computing-Software von Edgeless Systems nachweisbar sicher in Public Clouds betrieben werden. Auch die Verarbeitung eingestufter Daten bis VS-NfD könnte so möglich werden.

Mandantentrennung und Multi-Cloud für IT-Dienstleister der Verwaltung

Die IT-Dienstleister des Bundes und der Länder haben strikte Anforderungen an eine klare Trennung der Systeme einzelner Kunden. Eine physische Trennung ist dabei aufwändig im Betrieb und erfordert viel zusätzliche Hardware. Mittels Confidential-Computing-Software können Mandanten nachweisbar voneinander isoliert werden – sogar innerhalb von Kubernetes-Clustern. Außerdem können öffentliche IT-Dienstleister Public-Cloud-Leistungen mittels Confidential Computing ohne Abstriche bei Datenschutz und -sicherheit anbieten.



Sichere KI-Anwendungen in der Cloud für die öffentliche Verwaltung

Edgeless Systems bietet mit Continuum AI die erste Lösung, die führende Open-Source-Sprachmodelle (LLMs) während der Verarbeitung vollständig verschlüsselt. Dadurch bleiben sowohl Prompts als auch Antworten zu jedem Zeitpunkt vor Zugriffen durch den Modell- oder Cloud-Anbieter geschützt. Dies ermöglicht es auch Behörden, die Vorteile leistungsstarker KI-Tools sicher zu nutzen, ohne eigene Infrastruktur aufbauen oder auf die Flexibilität und Skalierbarkeit der Cloud verzichten zu müssen.

Weitere Informationen finden Sie unter edgeless.systems

Über Edgeless Systems

Edgeless Systems ist ein Cybersecurity-Unternehmen, das die Public Cloud zum sichersten Ort für sensible Daten macht. Mit weltweit führenden Open-Source-Lösungen für Confidential Computing hebt Edgeless Systems Datensicherheit für Cloud- und KI-Anwendungen auf ein neues Niveau und ermöglicht verschlüsselte Verarbeitung sensibler Daten mit hoher Skalierbarkeit.

Edgeless Systems arbeitet mit renommierten Firmen wie Capgemini, Thales, Nvidia und der Schweizer Börse zusammen. Das Unternehmen veranstaltet die jährliche Open Confidential Computing Conference (OC3) mit Top-Führungskräften von Microsoft, Google, AMD, Intel und ist Mitglied des Confidential Computing Consortiums.