Herausforderung Multi-Cloud im Behördenumfeld

Public Clouds bieten der deutschen Verwaltung die Möglichkeit, IT-Dienste effizienter und skalierbarer über externe Rechenzentren bereitzustellen. Insbesondere die Auslagerung von Cloud-nativen Anwendungen an IT-Dienstleister und Cloud Service Provider (CSP) verspricht den technologischen Fortschritt der Behörden. Doch gerade in einem hochregulierten Umfeld wie dem öffentlichen Sektor in Deutschland entstehen dadurch erhebliche Herausforderungen.

Traditionelle Sicherheitsmaßnahmen, wie Zugriffskontrollen und die Verschlüsselung von Daten während der Übertragung und Speicherung, sind zwar essenziell, bieten jedoch keine ausreichende Sicherheit, wenn Daten in

Vollständige Verschlüsselung in Multi-Cloud-Umgebungen mit Confidential Computing

der Cloud verarbeitet werden. Hier liegen sie oft im Klartext – also unverschlüsselt vor, was Administratoren oder externen Angreifern die Möglichkeit bietet, auf die Daten zuzugreifen. Gerade in einem Multi-Cloud-Umfeld, in dem Behörden mehrere Cloud-Anbieter parallel nutzen, steigt das Risiko von Sicherheitslücken und Fehlkonfigurationen, die von Angreifern ausgenutzt werden könnten.

Um die Vorteile von Public Clouds zu nutzen, müssen die Daten von Behörden dort durch dieselben Sicherheitsstandards geschützt werden wie auf der eigenen Infrastruktur. Dies führt in einem Multi-Cloud-Szenario zu einer besonders komplexen Situation, da Behörden nicht nur die Kontrolle über ihre Daten behalten müssen, sondern auch sicherstellen müssen, dass keine unberechtigten Dritten – sei es durch den CSP oder externe Angreifer – Zugriff auf sensible Informationen erhalten.

Die Nutzung von Public Clouds muss somit im Behördenumfeld so gestaltet werden, dass die Souveränität und Sicherheit der IT-Systeme stets gewährleistet bleibt. Dies bedeutet, dass selbst auf geteilter Infrastruktur Mechanismen vorhanden sein müssen, die sicherstellen, dass Daten immer geschützt sind und nur von den zuständigen Behörden selbst entschlüsselt und verwaltet werden können. Diese Herausforderungen sind

besonders im deutschen Kontext mit seinen strengen Geheim- und Datenschutzanforderungen – etwa durch die DSGVO und das IT-Sicherheitsgesetz – von entscheidender Bedeutung.

Trotz dieser regulatorischen und technischen Komplikationen bleibt die Nutzung von Cloud-Diensten entscheidend für die digitale Transformation der deutschen Verwaltung. Die Herausforderung besteht darin, diese Technologie in Einklang mit den notwendigen Sicherheits- und Souveränitätsanforderungen zu bringen, ohne auf die Effizienz und Flexibilität von Cloud-nativen Anwendungen zu verzichten.

Was ist Confidential Computing?

Confidential Computing ist eine Technologie, die Workloads vor ihrer Umgebung schützt und Daten selbst während der Verarbeitung verschlüsselt hält. Wie können sensible Daten auf einem möglicherweise kompromittierten Computer sicher verarbeitet werden? Für diese sehr relevante, aber bisher ungelöste Problemstellung bietet Confidential Computing eine innovative Lösung, unabhängig davon, ob der Computer von Ihnen selbst, Ihrem Unternehmen oder einem Dritten – wie einem Cloud-Anbieter – betrieben wird.

Die sichere Datenverarbeitung in der Cloud ist hierbei der Aspekt, der die meisten Menschen in Bezug auf Confidential Computing begeistert. Das ist wenig überraschend, da man bei der Ausführung von Workloads in der Cloud dem Anbieter zwangsläufig alle Daten anvertrauen muss. Darüber hinaus muss man auf eine korrekt ausgeführte Datenverarbeitung durch den Cloud-Anbieter vertrauen. Einem Cloud-Anbieter zu vertrauen, bedeutet insbesondere, dass man seinen Mitarbeitern und Systemen vertraut. Zudem muss man sich darauf verlassen, dass der Anbieter sich bei der Datenverarbeitung an geltende Gesetze und Regulierungen hält. Obwohl diese Vertrauensanforderung in einigen Fällen akzeptabel ist, gibt es viele Branchen und sensible Daten, für die das nicht infrage kommt. Dies kann in den meisten Fällen entweder auf ein hohes Risikobewusstsein oder auf strenge regulatorische Anforderungen zurückgeführt werden. Infolgedessen halten Unternehmen weiterhin an ihren veralteten und oft kostspieligen „On-Prem“-Rechenzentren vor Ort fest. Auch Endnutzer verzichten teilweise darauf, Cloud-basierte Dienste zu verwenden, die nicht als privat genug gelten. Confidential Computing löst dieses Vertrauensproblem der Cloud und ermöglicht neue Formen innovativer Anwendungen auf Basis öffentlicher Cloud-Infrastruktur – z.B. im Kontext von Künstlicher Intelligenz (KI).

Confidential Computing beschränkt sich jedoch keinesfalls auf die vertrauliche Nutzung von KI oder einzelnen Applikationen. Durch die Bereitstellung einer sogenannten Vertrauenswürdigen Ausführungsumgebung („Trusted Execution Environment“), können Betreiber von Rechenzentren von der Dateneinsicht oder Verarbeitung vollständig ausgeschlossen werden (sog. technischer Betreiberausschluss). Dies findet bereits in der Praxis Anwendung, etwa bei der elektronischen Patientenakte.

Fallstudie: Die elektronische Patientenakte " ePA" In Deutschland muss jede Krankenkasse ihren Kunden eine digitale Gesundheitsakte namens ePA (kurz für " ePatientenakte") zur Verfügung stellen. Alle Daten, wie verschriebene Medikation und Facharztberichte, sind über eine App zugänglich. Da Patientendaten äußerst sensibel sind, schreibt der Gesetzgeber eine strikte " Betreiber Ausschlussklausel" vor, die Backend-Anbieter den Zugriff auf Patientendaten untersagt. Dies wird durch den Einsatz von Confidential Computing, einschließlich Intel SGX, sowie Software von Edgeless Systems erreicht. Diese Technologien ermöglichen Remote Attestation und erleichtern das Skalieren der Enklaven-Anwendung auf Kubernetes.

Edgeless Systems: Kubernetes mit Ende-zu-Ende Vertraulichkeit

Edgeless Systems entwickelt führende Infrastruktur-Software für Confidential Computing, die einen ganzheitlichen Einsatz der Technologie in Multi-Cloud-Szenarien ermöglicht.

Constellation von Edgeless Systems ist eine fortschrittliche, CNCF-zertifizierte Kubernetes-Engine, die auf Confidential Computing basiert und vollständige Vertraulichkeit für containerisierte Workloads in Public- und Private-Cloud-Umgebungen bietet. Durch den Einsatz von Confidential Virtual Machines (CVMs) werden sämtliche Daten im Speicher sowie zur Laufzeit isoliert und verschlüsselt. Dies gewährleistet, dass weder Cloud-Anbieter noch Administratoren auf sensible Informationen zugreifen können.

Für den öffentlichen Sektor bedeutet dies eine erhebliche Stärkung der Datensicherheit und Kontrolle. Hier bietet Constellation eine flexible und sichere Plattform zur Verarbeitung sensibler Workloads. Diese können auf Clouds migriert werden, ohne die Vertraulichkeit der Daten zu gefährden.

Constellation baut auf der bewährten Kubernetes-Infrastruktur auf, fügt jedoch zusätzliche Sicherheitsfeatures hinzu, indem es die komplette Umgebung durch Confidential VMs schützt. Diese isolieren das Kubernetes-Cluster von der Cloud-Infrastruktur und verschlüsseln jede Interaktion – selbst auf Ebene des Betriebssystems. Diese Verschlüsselung erstreckt sich über den gesamten Speicherinhalt der VM, wodurch die Daten selbst für privilegierte Cloud-Administratoren oder Angreifer, die Zugriff auf die Infrastruktur erhalten, unlesbar bleiben. CVMs isolieren somit nicht nur die Kubernetes-Cluster, sondern schützen die Integrität und Vertraulichkeit der Daten im gesamten Zyklus der Datenverarbeitung.

Durch diese Isolation und Verschlüsselung bietet Constellation eine einzigartige Sicherheitsarchitektur, die für Cloud-native Anwendungen optimiert ist und zugleich höchste Vertraulichkeit garantiert, ohne Kompromisse bei der Leistung einzugehen.

Constellation verwendet Cilium als Container Network Interface (CNI) und nutzt eBPF für eine feingranulare Kontrolle des Netzwerkverkehrs zwischen Containern. Durch die Integration der WireGuard-Funktion von Cilium wird der gesamte Datenverkehr zwischen den Nodes im Cluster verschlüsselt. Dadurch werden Kubernetes-Cluster vollständig von der zugrunde liegenden Infrastruktur isoliert, was eine durchgängige Verschlüsselung und Sicherheit innerhalb der Cluster gewährleistet, ohne Zugriffsmöglichkeiten durch die Netzwerkumgebung des Host-Systems.

Ganzheitliche Architektur von UCS – lokal bis in die Cloud

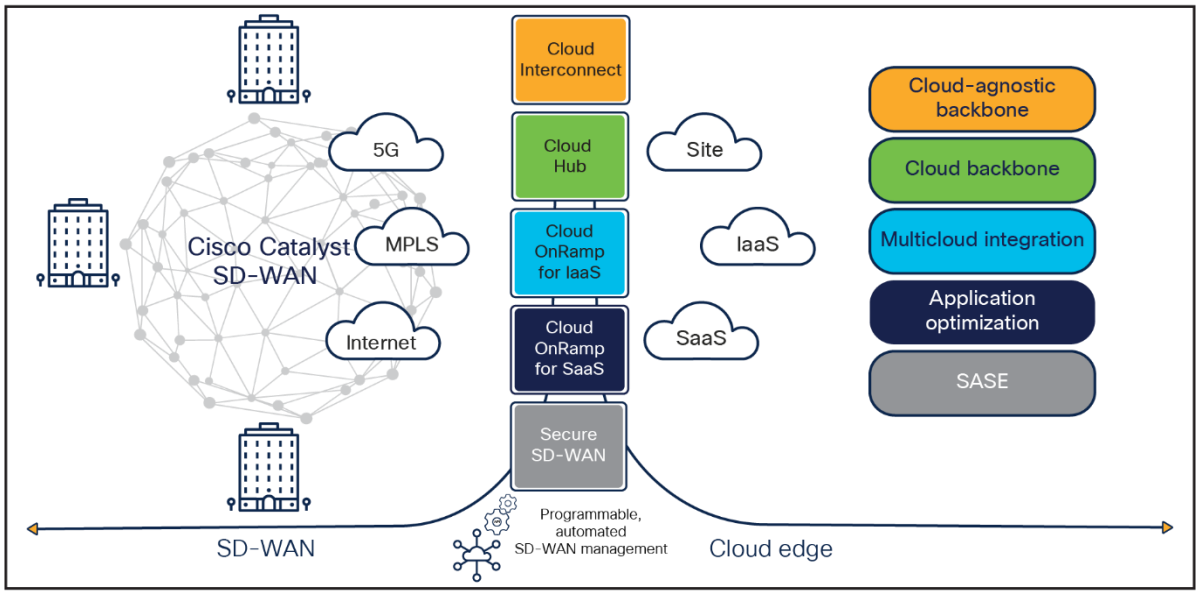
Die Technologie hinter Cilium wurde von Isovalent entwickelt, einer Firma, die ein Teil von Cisco ist. Damit ergeben sich gerade auch im lokalen Rechenzentrum interessante neue Anwendungsfälle für die eigene Serverinfrastruktur.

Cisco‘s UCS-Serverlösung zeichnet sich nicht nur mit Effizienzvorteilen beim Stromverbrauch aus, sondern ebenso bei operativen Themen wie der Verkabelung auf Grund der Unified IO Ports.

Das Thema Energieverbrauch kommt vor allem in der Betrachtung bei der Verschlüsselung durch Constellation zum Tragen: Die Energieeffizienz der UCS-Blade-Systeme ist deutlich höher als der geringe Mehrverbrauch, welcher durch die Verschlüsselung entsteht.

Im Kontext einer Multi-Cloud-Strategie für Confidential Computing ist eine Ende-zu-Ende-Betrachtung wichtig. Hierzu muss der gesamte Pfad vom eigenen Rechenzentrum bis in die Cloud abgesichert werden, da nur dann durchgehende Vertraulichkeit gewährleistet ist.

Cisco SD-WAN Cloud On-Ramp bietet dafür gerade im öffentlichen Umfeld die perfekte Grundlage. Von Haus aus ist die Lösung transportunabhängig, es ist also egal, welche Zugangstechnologie die Behörde nutzt, um ihre Clouddienste zu erreichen (klassisches Internet, MPLS, 5G, uva.).



Durch die Transportunabhängigkeit ergeben sich weitere Vorteile in Bezug auf die Anbindung mehrerer Standorte sowie die automatische Auswahl des besten Übertragungsweges bei redundanten Pfaden.

Cisco SD-WAN Cloud On-Ramp geht jedoch noch einen Schritt weiter und automatisiert nicht nur den Weg in die Cloud, sondern auch innerhalb dieser. Dadurch kann eine Konnektivität in die Cloud Infrastruktur bis zum Virtualisierungs-Layer direkt erfolgen. Außerdem werden Richtlinien und Sicherheitsmerkmale normalisiert, behalten aber Gültigkeit bis in die Cloud. Damit ist Cloud On-Ramp die perfekte Ergänzung zu Confidential Computing in Multi-Cloud-Umgebungen.

Fazit

Die Einführung von Multi-Cloud-Lösungen durch Nutzung von Confidential Computing und Produkten wie Constellation und Cloud On-Ramp bietet Behörden in Deutschland erhebliche Vorteile. Sie können flexibel verschiedene Infrastrukturen nutzen, während gleichzeitig eine Ende-zu-Ende-Verschlüsselung die Datensicherheit in allen Phasen gewährleistet – ob bei Speicherung, Übertragung oder Verarbeitung. Behörden haben trotz des Wechsels zwischen eigenem Rechenzentrum, der geteilten Infrastruktur eines IT-Dienstleisters und Cloud Service Providern (CSP) eine gleichbleibende und verlässliche Software-Architektur. Dadurch bleibt das Betriebsmodell über sämtliche Instanzen hinweg konsistent, was die Verwaltung vereinfacht, und die IT-Souveränität stärkt. So können die Vorteile der Cloud auch im öffentlichen Sektor genutzt werden, ohne Kompromisse bei Sicherheit oder Compliance eingehen zu müssen.

Fachbegriffe und Definitionen

Funktion	Vorteil
Betriebsausschluss	Konzept zur Verhinderung von Betreiberzugriff auf sensible Daten.
Cilium	Open-Source-Software für Netzwerk- und Sicherheitsrichtlinien bei containerisierten Anwendungen.
Cisco UCS	Unified Computing System von Cisco mit integriertem Netzwerkmanagement.
Cloud On-Ramp	Technologie, die Daten während der Verarbeitung verschlüsselt und schützt.
Cloud Service Provider (CSP)	Anbieter von Cloud-Diensten wie Rechenleistung, Speicher und Anwendungen.
Cloud-nativ	Softwarearchitektur, speziell für den Betrieb in Cloud-Umgebungen entwickelt.
Confidential Computing	Technologie, die Daten während der Verarbeitung verschlüsselt und schützt.
Confidential Virtual Machine (CVM)	Virtuelle Maschine, die Daten während der Verarbeitung isoliert und verschlüsselt.
Container	Leichte Softwarepakete, die Anwendungen und alle Abhängigkeiten enthalten.
DSGVO (Datenschutz-Grundverordnung)	Europäische Verordnung zum Schutz personenbezogener Daten.
eBPF	Linux-Kernel-Erweiterung für effiziente Netzwerk- und Sicherheitsüberwachung.
Ende-zu-Ende-Verschlüsselung	Verschlüsselung, bei der Daten von der Quelle bis zum Ziel geschützt bleiben.
Kubernetes	Open-Source-Plattform zur Automatisierung der Verwaltung containerisierter Anwendungen.

Funktion	Vorteil
Multi-Cloud	Nutzung mehrerer Cloud-Dienste oder -Anbieter gleichzeitig.
On-Prem	IT-Infrastruktur, die in eigenen Rechenzentren vor Ort betrieben wird.
Public Cloud	Extern betriebene und öffentlich zugängliche Cloud-Computing-Plattform.
SD-WAN (Software-Defined Wide Area Network)	Softwaregesteuerte Technologie zur Optimierung von Netzwerken zwischen Standorten.
Trusted Execution Environment (TEE)	Isolierte, sichere Umgebung in Prozessoren zum Schutz von Daten und Code.
Unified IO Ports	Netzwerkports, die mehrere Protokolle (z. B. LAN, SAN) über einen Anschluss unterstützen.
WireGuard	Moderne VPN-Technologie zur Verschlüsselung von Netzwerkverkehr.

Hauptgeschäftsstelle Nord- und Südamerika
Cisco Systems, Inc.
San Jose, CA

Hauptgeschäftsstelle Asien-Pazifik-Raum
Cisco Systems (USA) Pte. Ltd.
Singapur

Hauptgeschäftsstelle Europa
Cisco Systems International BV Amsterdam
Niederlande

Cisco verfügt über mehr als 200 Niederlassungen weltweit. Die Adressen mit Telefon- und Faxnummern finden Sie auf der Cisco Website unter https://www.cisco.com/go/offices.

Gedruckt in USA

C78-520522-12