EuroCloud DEUTSCHLAND | eco

CONFIDENTIAL COMPUTING:

Sicher und Souverän in der Cloud

Inhalt

1. Einleitung 5

2. Was ist Confidential Computing? 5
2.1. Begriffsdefinition 5
2.2. Exkurs: Homomorphe Kryptografie zur Verschlüsselung von Data in Use 6
2.3. Hauptmerkmale von Confidential Computing 6
2.3.1. Verschlüsselung als CPU-Feature 6
2.3.2. Enklaven 7
2.3.4. Workload Attestation 7

3. Vorteile von Confidential Computing 9
3.1. Operative Vorteile 9
3.1.1. Einhaltung von Datenschutzvorgaben 9
3.1.2. Reduzierter Reporting-Aufwand 9
3.1.3. Schutz von Intellectual Property 10
3.1.4. Unterstützung bei Lift-and-Shift-Migrationen 10
3.2 Schutz gegen Angriffsvektoren 10
3.2.1. Angriffe auf virtuelle Maschinen (VM Attacks) 10
3.2.2. Malware und Rootkits 10
3.2.3. Angriffe auf Arbeitsspeicher (Memory Attacks) 10
3.2.4. Cold Boot Attacks 10
3.2.5. Insider-Bedrohungen 10
3.2.6. Seitenkanalangriffe (Side-Channel Attacks): 10
3.2.7. Man-in-the-Middle-Angriffe 10

4. Risiken und Herausforderungen 11
4.1. Vendor Lock-in 11
4.2. Potenzielle Schwachstellen 11

5. Rechtsrahmen für Confidential Computing 12
5.1. CRA und die CE-Kennzeichnung für IT-Produkte 12
5.2. EUCS und Souveränität 12
5.3. Confidential Computing bei der Umsetzung von Regularien 12

6. Confidential Computing bei der Hyperscaler-Nutzung 13

7. Anwendungsfelder und Beispiele für Use Cases 14
7.1. Confidential Appliances 14
7.2. Cloud Plattform für Human Resources 14
7.3. Internet of Things (IoT) als SaaS-Anwendung 14
7.4. Sichere Speicherung von Transaktionsdaten im Handel 14
7.5. Ende-zu-Ende-verschlüsselte Kommunikation 14
7.6. Flexible Security-Umgebungen 14
7.7 Sichere Datenverarbeitung in der Gesundheitsbranche 14

8. Wie lässt sich Confidential Computing praktisch umsetzen? 15
8.1. Handlungsempfehlungen für Anwenderunternehmen 15
8.1.1. Kritische Prozesse und Daten identifizieren 15
8.1.2. Schlüsselmanagement in die Unternehmenskontrolle bringen 15
8.1.3. Erste Pilotanwendungen benennen 15
8.1.4. Geeignete Technologien und Dienstleister auswählen 15
8.1.5. Betriebsmodelle und Tools absichern 15
8.1.6. Deployment- und Migrationsoptionen evaluieren 15
8.2. Handlungsempfehlungen für SaaS-Anbieter 16
8.3. Handlungsempfehlungen für Service Provider 16

9. Fazit und Ausblick 17

Autoren des Textes: 17

Vorbemerkung

Confidential Computing ist ein junger technologischer Ansatz. Er dient dazu, sensible Daten auch während der Verarbeitung in einer Cloud- oder Hosting-Umgebung zu schützen. Der vorliegende Text, der sich diesem Konzept widmet, wurde durch eine Arbeitsgruppe unter dem Dach des EuroCloud Deutschland_eco e. V. erstellt. Eine Liste der Autoren findet sich am Ende des Dokuments.

1. Einleitung

Cloud Computing ist in Unternehmen angekommen. Die Mehrzahl der Organisationen nutzt heute Services von einem oder mehreren Cloud-Anbietern, seien es internationale Hyperscaler oder regional agierende Provider. Die Unternehmen wollen von den Vorteilen profitieren, die das Bereitstellungsmodell in puncto Agilität, Verfügbarkeit, Flexibilität und Skalierbarkeit bietet. Durch die Cloud sind jedoch neue Herausforderungen für ihre Sicherheit und ihre Souveränität entstanden. Denn Daten werden außerhalb der lokalen IT und damit jenseits des Perimeters verarbeitet. Zugleich bedeutet Cloud Computing einen Verlust an Kontrolle. Schließlich werden Workloads von Unternehmen auf einer Infrastruktur ausgeführt, die durch einen Dritten (intern wie extern) verwaltet und gesteuert wird und auf die sie selbst keinen direkten Zugriff haben.

Als Reaktion auf diese Herausforderungen hat die IT-Branche neue Sicherheitskonzepte entwickelt. So wurden beispielsweise unter dem Begriff „Zero Trust" spezifische Mechanismen entwickelt, die den Zugriff auf Anwendungen und Daten nach dem Prinzip der minimalen Rechte regeln. Ein anderes Konzept, das geeignet ist, die Sicherheit bei der Cloud-Nutzung zu erhöhen, ist „Confidential Computing". Dabei geht es im Wesentlichen darum, innerhalb der IT-Infrastruktur vertrauliche Ausführungsumgebungen für Workloads zu schaffen, auf die die Provider nicht zugreifen können. Isolierung und Verschlüsselung schützen die Daten der Anwender vor nicht autorisierten Zugriffen ebenso wie vor Cyberbedrohungen.

Somit zielt Confidential Computing darauf ab, Organisationen das Vertrauen zu geben, dass ihre sensiblen Daten auch während der Verarbeitung in der Cloud sicher sind. Dieses Whitepaper gibt dem Leser einen Überblick über Confidential Computing. Dazu werden die wesentlichen technologischen Merkmale vorgestellt und die grundlegende Funktionsweise des Konzepts erläutert. Außerdem werden die Vorteile aufgezeigt, die das Konzept bei der Verarbeitung sensibler Daten bietet. Davon profitieren insbesondere Unternehmen aus regulierten Branchen, in denen hohe Anforderungen an die IT-Sicherheit gelten. Confidential Computing kann ihnen helfen, die einschlägigen Regularien einzuhalten. Risiken und Schwächen des Konzepts sollen dabei nicht ausgeblendet werden. Abschließend werden exemplarisch einige Use Cases skizziert

2. Was ist Confidential Computing?

Confidential Computing bezeichnet eine Technologie, die sicherstellen soll, dass sich Daten während ihrer Verarbeitung in einer geschützten Umgebung befinden. Dies geschieht im Wesentlichen durch Verschlüsselung. Bei der Nutzung von Cloud-Plattformen werden Daten normalerweise dann verschlüsselt, wenn sie gespeichert, also im Ruhezustand sind und wenn sie zwischen den Clients der Nutzer und den Servern der Cloud-Anbieter übertragen werden. Jedoch sind Daten in der Regel während der Verarbeitung entschlüsselt, also dann, wenn sie von Anwendungen oder Diensten in der Cloud bearbeitet werden. Daten in diesem kritischen Stadium, in dem sie anfällig für Angriffe oder Fehler in der Systemverwaltung sein können, zu schützen, ist Sinn und Zweck von Confidential Computing. Das Konzept zielt daher darauf ab, dass Daten selbst während der Ausführung von Anwendungen in einer vertraulichen Umgebung bleiben.[1]

2.1. Begriffsdefinition

In Cloud- und Hosting-Umgebungen stehen Unternehmen vor der Herausforderung, sensible Daten sowohl während der Speicherung und Übertragung als auch während der Verarbeitung zu schützen. Somit spielen drei Zustände von Daten eine Rolle: Data at Rest, Data in Transit (auch Data in Motion) und Data in Use. Auch wenn die Verschlüsselung von Daten in den ersten beiden Zuständen bereits weit verbreitet ist und technologisch etwa durch Festplatten- beziehungsweise Transportverschlüsselung umgesetzt wird, ist der Schutz sensibler Daten während ihrer Verarbeitung, also von Data in Use, noch nicht weitreichend implementiert. Genau darauf zielt Confidential Computing ab. Sind Daten in allen drei Zuständen verschlüsselt, spricht man auch von 3D-Verschlüsselung.

In einer allgemeinen Definition kann man Confidential Computing als Konzept bezeichnen, das geeignet ist, die Vertraulichkeit von Daten während ihrer Verarbeitung in nicht vertrauenswürdigen Umgebungen sicherzustellen. Bei einer nicht vertrauenswürdigen Umgebung handelt es sich in diesem Zusammenhang um jedwede IT-Umgebung, auf die Dritte zu Verwaltungs- und Steuerungszwecken Zugriff erhalten. Im Wesentlichen ermöglicht Confidential Computing die sichere Ausführung von Anwendungen und damit die sichere Verarbeitung von Daten, ohne dass der Betreiber der Umgebung, z. B. ein Hosting oder Cloud Provider, auf Anwendungen oder Daten zugreifen kann.

Zu Confidential Computing gehören Technologien der 3D-Verschlüsselung samt notwendiger Begleitprozesse und Tools, die es ermöglichen, sensible Anwendungen in einem geschützten Systembereich auszuführen. Im Allgemeinen spricht man von einer vertrauenswürdigen Ausführungsumgebung, auf Englisch „Trusted Execution Environment" (TEE). Bei Confidential Computing werden solche vertrauenswürdigen Ausführungsumgebungen als sogenannte Enklaven realisiert. Wesentliche technologische Voraussetzungen dafür sind logische Isolierung und Verschlüsselung auf der Ebene der Central Processing Unit (CPU).

1 siehe auch: https://next.enclaive.cloud/s/MPpzyDJbfkBBsFc

2.2. Exkurs: Homomorphe Kryptografie zur Verschlüsselung von Data in Use

Confidential Computing ist ein relativ junges Konzept. Bevor es in den vergangenen Jahren aufkam und sich erste marktfähige Lösungen entwickelt haben, gab es bereits theoretische Ansätze zur Verschlüsselung von Daten bei der Verarbeitung. Dazu zählt die homomorphe Kryptografie. Dieser Ansatz hat jedoch seine Einschränkungen.

Homomorphe Kryptografie ermöglicht es, Berechnungen an verschlüsselten Daten auszuführen, ohne diese zu entschlüsseln. Werden Daten im Rahmen von Cloud-Computing-Modellen durch einen Drittanbieter gespeichert und verarbeitet, eignet sich die homomorphe Kryptografie somit theoretisch als Lösung, die die Privatheit der Daten gewährleistet. Denn im Klartext sind sie nur für den Eigentümer sichtbar. Die Technologie verursacht jedoch einen starken Computing-Overhead: Sie erfordert eine 100 bis 1.000 Mal höhere Rechenleistung, als sie für die Verarbeitung unverschlüsselter Workloads benötigt wird. Deshalb ist dieser Ansatz derzeit (noch) nicht marktfähig.

2.3. Hauptmerkmale von Confidential Computing

Confidential Computing beruht im Kern darauf, vertrauliche Ausführungsumgebungen in Form von Enklaven bereitzustellen. Ermöglicht werden sie durch die hardwarebasierte Verschlüsselung, die Chiphersteller wie AMD, IBM und Intel seit einigen Jahren in ihren Prozessoren unterstützen. Dadurch lassen sich geschützte Bereiche innerhalb einer CPU isolieren, um Anwendungen darin sicher auszuführen.

Darüber hinaus bietet Confidential Computing weitere Sicherheitsfunktionen. So werden die Zugriffe auf eine Enklave, die darin vorgenommenen Operationen und die Veränderungen an den Daten protokolliert. Ein essenzielles Merkmal ist dabei die Möglichkeit, die Integrität und Authentizität von Daten, die in einer Enklave verarbeitet werden, zu überprüfen. Die sogenannte Attestierung („Attestation") stellt mittels kryptografischer Verfahren sicher, dass ein Workload nicht manipuliert oder beeinträchtigt wurde. Dadurch wird das Vertrauen in die Sicherheit einer Ausführungsumgebung gestärkt.

2.3.1. Verschlüsselung als CPU-Feature

Die Hersteller Intel und AMD implementierten in ihren Prozessoren seit 2015 beziehungsweise seit 2017 die Verschlüsselung auf Hardwarebasis. Sinn und Zweck ist es, Workloads in virtuellen Umgebungen vor externen Bedrohungen zu schützen, wie etwa dem Auslesen von Daten aus dem Arbeitsspeicher über den Hypervisor. Wichtige etablierte Ansätze zum Schutz von Verfügbarkeit, Vertraulichkeit und Resilienz und Integrität werden ergänzt, nicht aber abgelöst.

Aktuelle Chipsätze der Anbieter werden standardmäßig mit den Technologien Intel Software Guard Extensions (SGX), Intel Trust Domain Extensions (TDX) beziehungsweise AMD Secure Encrypted Virtualization (SEV) ausgeliefert.

Der Hersteller NVidia hat Ende 2023 mit der GPU-Reihe H100 ein erstes System mit einer Technologie herausgebracht, die ähnlich wie AMD SEV und Intel TDX funktioniert. Für ARM-Prozessoren wird nach einer Ankündigung des Halbleiterspezialisten damit gerechnet, dass Chips mit vergleichbaren Sicherheitsfunktionen zu Beginn des Jahres 2025 auf den Markt kommen werden. Auch das System/390 von IBM unterstützt Confidential Computing.

Somit sind Confidential-Computing-Features inzwischen für fast alle im Markt relevanten Prozessor-Architekturen verfügbar.

Konkret sieht die technologische Unterstützung von Confidential Computing auf CPU-Ebene aktuell (Herbst 2024) wie in der folgenden Tabelle aus:

Technology (verlinkt)	CPU	Codename
AMD Secure Encrypted Virtualization (SEV)	Untervorbehalt: EPYC 2 (SEV ES) EPYC 3 (SEV SNP) or later	Rome Milan
Intel Trusted Domain Extension (TDX)	Xeon Series 5 or related	Saphire EmeraldRapids
ARM Confidential Compute Architecture (CCA)	ARM Cortex A9	Falcon
NVIDIA Confidential Computing	NVIDIA H100 GPU	Hopper
IBM Secure Execution for Linux (SEL)	IBM z15 or later IBM LinuxONE III	

2.3.2. Enklaven

Eine Enklave ist, wie bereits skizziert, eine isolierte Umgebung innerhalb eines Prozessors. Operationen können sicher darin ablaufen, sodass die zu verarbeitenden Daten geschützt sind. Ein wesentliches Merkmal ist dabei die Isolation: Enklaven sind konsequent von den anderen Teilen des Systems getrennt, die wiederum nur über bestimmte sichere Schnittstellen mit ihnen kommunizieren können. Zudem werden starke kryptografische Technologien verwendet, um die Daten innerhalb der Enklave zu verschlüsseln. Isolation und Verschlüsselung stellen sicher, dass Daten in einer solchen Ausführungsumgebung vor nicht autorisierten Zugriffen geschützt sind.

Auf diese Weise dienen Enklaven dem Zweck, sensible Daten in Cloud- und Hosting-Szenarien vor potenziellen Bedrohungen wie Diebstahl oder Kompromittierung durch Malware[2] zu schützen. Die Daten bleiben sicher, selbst wenn ein Angreifer in das Gesamtsystem eindringt und die benachbarten Systembereiche kompromittiert werden.

Attacken auf virtualisierte Systeme finden typischerweise über Sicherheitslücken im Hypervisor oder im Host Operating System statt. Angreifer erhalten so die Möglichkeit, auf Bereiche des Arbeitsspeichers (RAM) zuzugreifen. Theoretisch kann die logische Trennung der RAM-Bereiche, die verschiedenen virtualisierten Instanzen zugeordnet sind, auch aufgrund einer Schwachstelle der CPU durchbrochen werden. Beispiele dafür sind die Sicherheitslücken „Meltdown" und „Spectre", die 2017/2018 bekannt wurden. Sie ermöglichten es potenziellen Angreifern, sensible Daten aus dem Arbeitsspeicher zu stehlen.

Enklaven wirken solchen Szenarien weitgehend entgegen, indem sie alle virtualisierten Speicherbereiche mit jeweils eigenem Schlüsselmaterial verschlüsseln. Sollte eine Attacke über die CPU oder die Verwaltungsebene (Hypervisor, Host Operating System) auf virtualisierte Instanzen erfolgen, erhält der Angreifer allenfalls Einblick in deren verschlüsselte Daten. Damit kann er aber nichts anfangen, solange ihm der Schlüssel für den betreffenden Speicherbereich nicht bekannt ist.[3]

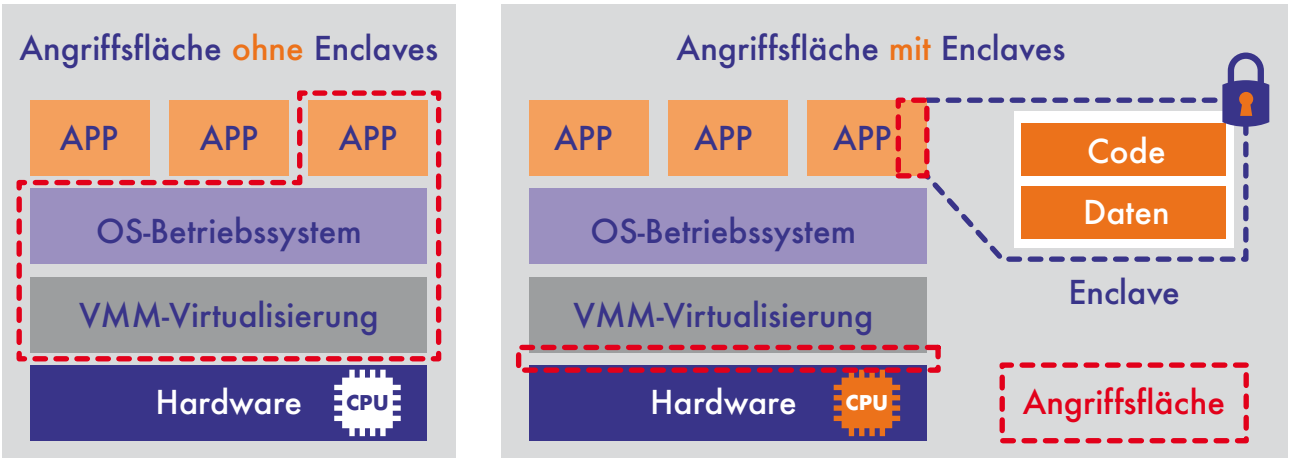
2.3.4. Workload Attestation

Attestierung ist, wie oben erwähnt, ein weiteres wesentliches Merkmal von Confidential Computing. Sie dient dazu, die Integrität und Authentizität von Workloads, die in einer vertrauenswürdigen Umgebung (TEE) ausgeführt werden, revisionssicher zu überprüfen. Durch Attestation lässt sich verifizieren, dass der betreffende Workload nicht manipuliert, beeinträchtigt oder kompromittiert wurde. Der Anwender kann somit darauf vertrauen, dass eine Enklave, die er zur Verarbeitung seiner Daten nutzt, den erwarteten Schutz bietet und keine der bekannten Schwachstellen aufweist. Attestation ist ein komplexes Verfahren. Vereinfacht formuliert, zielt es darauf ab, den einwandfreien Sicherheitszustand einer Ausführungsumgebung überprüfbar zu machen.

Um zu ermitteln, ob eine Enklave tatsächlich den erwarteten hohen Sicherheitsstandard bietet, werden kryptografische Verfahren eingesetzt. Bei der Workload-Attestierung misst die Enklave zu Beginn der Ausführung einer Rechenoperation die Ausgangskonfiguration der Umgebung sowie den Code der Anwendung und generiert daraus einen eindeutigen Hash. Dieser Messwert wird

2 Allerdings muss sichergestellt sein, dass die zu verarbeitenden Daten nicht zuvor kompromittiert wurden. Theoretisch kann Malware innerhalb einer Enklave laufen, wenn sie übersehen und bei der Attestation mit eingemessen wurde. Umso wichtiger ist eine lückenlose Attestierung.

3 Forschungsexperimente haben gezeigt, dass es theoretisch möglich ist, diesen Schlüssel bei direktem Zugang zum System zu extrahieren (Seitenkanalangriffe).



Confidential Computing ermöglicht es, Anwendungscode und Daten innerhalb einer Enklave verschlüsselt zu verarbeiten. Dadurch reduziert sich die Angriffsfläche deutlich. Alle dafür notwendigen Sicherheitsfunktionen sind in der CPU implementiert.

zusammen mit weiteren relevanten Informationen zur Identität der Enklave und ihren Sicherheitseigenschaften in einem Bericht, dem Attestation Report, erfasst.

Bei Enklaven in der Cloud wird die Überprüfung ihrer Identität und ihres Sicherheitszustands üblicherweise remote vorgenommen. Schließlich haben Cloud-Anwender keinen direkten Zugang zur physischen Infrastruktur, auf der die Enklaven laufen. Bei der Remote Attestation kommt eine weitere Instanz ins Spiel, der Attestation Service. Als vertrauenswürdiger Dritter überprüft dieser Bescheinigungsdienst den Attestation Report. Er wertet den Bericht aus, validiert die Messung, beurteilt die Integrität des Workloads und bestätigt im positiven Fall den sicheren Zustand der Enklave durch ein Zertifikat.

Die Überprüfung durch den Attestation Service erfolgt in der Regel auf Basis von Standardrichtlinien. Anwender haben zudem die Möglichkeit, das Attestation-Zertifikat ihrerseits anhand benutzerdefinierter Richtlinien zu überprüfen. Auf diese Weise können sie sicherzustellen, dass die Enklave ihren individuellen Sicherheitsanforderungen genügt. In den Richtlinien können definierte Messungen, der Einsatz bestimmter Softwareversionen oder die Einhaltung spezifischer Sicherheitsstandards festgelegt werden.

Essenziell ist bei der Remote Attestation, dass die Kommunikation zwischen der Enklave, dem Bescheinigungsdienst und dem externen Anwender durchgängig geschützt ist, um die Vertraulichkeit und Integrität der übertragenen Daten zu wahren. Dazu werden Technologien wie Verschlüsselung und sichere Kanäle eingesetzt.

Bescheinigungsdienste können von unterschiedlichen Arten von Unternehmen bereitgestellt werden. Zum einen sind es Cloud Provider selbst, die solche Services anbieten. Bei den Hyperscalern gehören sie bereits zum Portfolio. Zum anderen kommen Anbieter von Security-Software oder IT-Dienstleister als Betreiber von Attestation Services in Frage. Darüber hinaus können aber auch große Unternehmen mit hohen Sicherheitsanforderungen intern einen eigenen Bescheinigungsdienst aufbauen und bereitstellen. Um das Prinzip konsistent umzusetzen, gehören der Betreiber der zu prüfenden Umgebung und die verifizierende Stelle idealerweise nicht der gleichen Organisation an.

Grundsätzlich stellt die Workload Attestation ein solides Verfahren dar, das eine sichere Interaktion zwischen Anwendern und Enklaven ermöglicht. Indem sie die Integrität und Authentizität von Daten, die in vertraulichen Ausführungsumgebungen verarbeitet werden, revisionssicher verifiziert, stärkt die Attestierung das Vertrauen in die Nutzung von Enklaven und damit letztlich das Vertrauen in die Nutzung der Cloud.

3. Vorteile von Confidential Computing

Aus der Funktionsweise und den wesentlichen Merkmalen von Confidential Computing ergeben sich die Vorteile des Konzepts. Mit Hilfe isolierter Enklaven, deren Inhalte verschlüsselt sind und deren Sicherheitszustand regelmäßig überprüft wird, können Unternehmen ihre sensiblen Daten auch bei der Verarbeitung in der Cloud effektiv schützen. Zum einen erhöhen sie damit ihre Sicherheit gegenüber Cyberangriffen. Zum anderen hilft ihnen die Nutzung vertraulicher Ausführungsumgebungen dabei, rechtliche Anforderungen und interne Richtlinien zu erfüllen.

Die Verschlüsselung der Daten erfordert zwar Rechenleistung. Gemessen am Sicherheitsgewinn und an den Vorteilen in puncto Compliance ist die zusätzliche CPU-Last jedoch vergleichsweise gering. Bei aktuellen Implementierungen von Enklaven liegt der Overhead in der Regel bei zwei bis fünf Prozent der Leistung, die die Workloads ohne Confidential Computing benötigen würden.

Es liegt auf der Hand, dass insbesondere Organisationen, die sich in einem regulierten Sektor (z. B. Finance, Healthcare oder Public) bewegen und die dennoch die Cloud nutzen wollen, von Confidential Computing profitieren. Trotz strenger regulatorischer Vorgaben können sie Daten richtlinienkonform auf Cloud-Plattformen verarbeiten.

Prinzipiell eignet sich das Konzept aber für Unternehmen aus allen Branchen. Zudem bietet es nicht nur Vorteile für Organisationen, die IT anwenden, sondern auch für IT-Anbieter wie etwa Softwarehersteller oder Managed Service Provider (MSP), die ihren Kunden sichere SaaS-Anwendungen beziehungsweise sichere Infrastrukturdienste bereitstellen wollen. In der Praxis gibt es Anwendungsbereiche in nahezu allen Industrien und vielfältige Anwendungsszenarien (Beispiele in Kapitel 7).

Die Vorteile von Confidential Computing sollen in den beiden folgenden Unterkapiteln eingehender betrachtet werden, differenziert nach operativen und sicherheitsspezifischen Vorteilen.

3.1. Operative Vorteile

Confidential Computing ist ein technologischer Ansatz, der Unternehmen dabei helfen kann, Maßnahmen zum Security und Compliance Management umzusetzen. Schließlich sorgen wesentliche Prinzipien des Konzepts wie die Bereitstellung vertraulicher Ausführungsumgebungen und die durchgängige Verschlüsselung (3D-Verschlüsselung) dafür, dass Anwendungen und Daten vor unautorisierten Zugriffen geschützt sind. Hinzu kommen weitere Sicherheitsfunktionen wie Zugriffskontrollen und Authentifizierungsmechanismen, die Protokollierung von Zugriffen und Operationen sowie die Workload-Attestierung, die eine konsequente Überwachung und Dokumentation von sicherheitsrelevanten Prozessen ermöglichen.

Diese Merkmale unterstützen Unternehmen dabei, Regularien einzuhalten, Intellectual Property zu schützen sowie Prüf- und Berichtspflichten zu erfüllen. Confidential Computing kann darüber hinaus aber auch hilfreich sein, wenn Workloads von On-Premises in die Cloud migriert werden sollen.

3.1.1. Einhaltung von Datenschutzvorgaben

Confidential Computing macht es für Anwender einfacher, rechtliche Vorgaben zum Datenschutz einzuhalten. Weil Enklaven strikt von der darunterliegenden Infrastruktur getrennt sind, lassen sich administrative Zugriffe auf deren Inhalte ausschließen. Unternehmen können daher sicherstellen, wenn sie personenbezogene Daten in der Cloud verarbeiten, dass sie compliant mit Rechtsakten wie der Datenschutz-Grundverordnung (DSGVO) sind. Denn der Cloud Provider hat, selbst wenn ihn Rechtsakte wie der US CLOUD Act dazu verpflichten sollten (siehe auch Kapitel 6), keinen Zugang zu den verschlüsselten Daten in der Enklave.[4]

Dieser Vorteil bewährt sich nicht nur beim Cloud Computing, sondern immer dann, wenn Unternehmen mit Dritten zusammenarbeiten und ihnen dabei remote Zugang zu ihren Systemen eröffnen. Denn Confidential Computing erlaubt es ihnen, die Zugriffe der Partner lückenlos zu kontrollieren. So unterstützt das Konzept etwa Multi-Party Computation (MPC), ein Verfahren, bei dem mehrere Parteien beispielsweise gemeinsam Datensätze auswerten, ohne dass sie sensible Informationen preisgeben.

3.1.2. Reduzierter Reporting-Aufwand

Weil sämtliche Zugriffe auf Enklaven, darin ausgeführte Operationen und Veränderungen an den Daten protokolliert werden, unterstützt Confidential Computing das Reporting von Unternehmen. Auf diese Weise können unterschiedliche Berichte automatisiert erzeugt werden. Innerhalb von Enklaven lässt sich zudem sicherstellen, dass die Protokolle nicht manipuliert werden, und per Attestation lässt sich ihre Integrität belegen.

So erzeugte Berichte können unterschiedlichen Zwecken dienen. Sie können beispielsweise nachweisen, dass personenbezogene Daten ordnungsgemäß verarbeitet und Datenschutzbestimmungen eingehalten wurden (Compliance Reporting). Oder sie erfassen ungewöhnliche Aktivitäten von Nutzern und zeigen potenzielle Sicherheitsrisiken auf (Security Reporting). Darüber hinaus lassen sich detaillierte Trails für Audits erstellen. Confidential Computing ermöglicht somit eine automatisierte Dokumentation technischer Maßnahmen und reduziert den manuellen Aufwand beim Reporting.

4 siehe auch: https://next.enclaive.cloud/s/Y65T2tZEo8eoWKr)

3.1.3. Schutz von Intellectual Property

Durch den Einsatz von Confidential Computing können Unternehmen sowohl Kunden als auch Partnern den Zugriff auf eigene Anwendungen erlauben, ohne Zugriffe auf ihren Source Code befürchten zu müssen. Zudem können sie durch die Verarbeitung von Daten in einer vertraulichen Umgebung, in der sie wie in einem Tresor geschützt sind, auch heikle digitale Innovationen schnell und unkompliziert in der Cloud erproben. Dabei gehen sie weder das Risiko eines Datenverlusts noch das eines Compliance-Verstoßes ein.

3.1.4. Unterstützung bei Lift-and-Shift-Migrationen

Werden Anwendungen von On-Premises in die Cloud übertragen, ohne ihre Architektur oder ihren Code anzupassen, spricht man von „Lift and Shift". Da sich Cloud-Infrastrukturen von lokalen Infrastrukturen unterscheiden, kann diese Art der Migration zu Problemen führen, etwa zu Leistungseinbußen oder Ausfällen. Confidential Computing umgeht diese Problematik. Denn der Anwender erhält mit einer Enklave eine dedizierte Umgebung in der Cloud, die er mit den gleichen Merkmalen einer On-Premises-Umgegung konfigurieren kann. Dorthin lassen sich Anwendungen ohne nennenswerte Anpassungen migrieren.

3.2 Schutz gegen Angriffsvektoren

Neben operativen Vorteilen stärkt der Einsatz von Confidential Computing auch die Resilienz gegenüber Cyberbedrohungen. Denn das Konzept kann Sicherheitsteams helfen, eine Reihe von Angriffsvektoren auszuschließen oder zumindest so zu entschärfen, dass es Angreifern deutlich schwerer gemacht wird, ihr Ziel zu erreichen. Im Folgenden werden beispielhaft einige dieser Vektoren skizziert.

3.2.1. Angriffe auf virtuelle Maschinen (VM Attacks)

In der Cloud können Angreifer theoretisch auf Daten in virtuellen Maschinen (VMs) zugreifen, indem sie sich Schwachstellen in Hypervisoren oder in anderen VMs zunutze machen. Innerhalb vertraulicher Ausführungsumgebungen sind Anwendungen und Daten isoliert und deshalb vor solchen Attacken geschützt, selbst dann, wenn der Hypervisor oder VMs auf dem gleichen Host erfolgreich angegriffen werden.

3.2.2. Malware und Rootkits

Durch das gleiche Prinzip wird auch schädlicher Code jeglicher Art abgewehrt. So wie Enklaven vor unautorisierten Zugriffen sicher sind, bleiben die darin verarbeiteten Daten selbst dann geschützt, wenn der Hypervisor oder das Betriebssystem von Malware kompromittiert ist.

3.2.3. Angriffe auf Arbeitsspeicher (Memory Attacks)

Confidential Computing schützt Anwender vor Datenverlusten durch Angriffe auf den Arbeitsspeicher. Denn Workloads werden in einer isolierten Ausführungsumgebung verarbeitet und Daten gelangen ausschließlich in verschlüsselter Form in den Speicher. Angreifer haben somit keine Möglichkeit, Daten im Klartext aus dem Memory-Bereich auszulesen.

3.2.4. Cold Boot Attacks

Cold Boot Attacks zielen ebenfalls darauf ab, Daten aus dem Arbeitsspeicher auszulesen. Dazu starten Angreifer ein System schnell neu und extrahieren dabei den RAM-Inhalt. Confidential Computing vereitelt dieses Angriffsmuster durch die Verschlüsselung der Daten im Speicher.

3.2.5. Insider-Bedrohungen

Für die IT-Sicherheit von Unternehmen stellen Personen aus der eigenen Organisation oder dem unmittelbaren Umfeld, die ihre Zugangsdaten und ihr internes Wissen missbrauchen, um Schaden anzurichten, eine besondere Herausforderung dar. Confidential Computing wirkt solchen Insider-Bedrohungen entgegen, weil administrative Zugriffe auf vertrauliche Ausführungsumgebungen ausgeschlossen sind. Zu den Daten, die darin verarbeitet werden, haben selbst privilegierte Benutzer wie Systemadministratoren oder Mitarbeiter von Dienstleistern (z. B. von Cloud Providern) keinen Zugang.

3.2.6. Seitenkanalangriffe (Side-Channel Attacks):

Confidential Computing schützt vor Seitenkanalangriffen auf kryptografische Systeme. Bei diesem Angriffsvektor versuchen Hacker, Rückschlüsse auf geheime Schlüssel zu ziehen, indem sie Nebeninformationen wie Stromverbrauch, elektromagnetische Strahlung oder das Zeitverhalten analysieren. Enklaven sind heute so ausgelegt, dass sie solche Rückschlüsse in den meisten Fällen nicht zulassen.

3.2.7. Man-in-the-Middle-Angriffe

Ein Man-in-the-Middle-Angriff ist eine Attacke, bei der sich ein Angreifer unbemerkt in die Kommunikation zwischen zwei Parteien einschaltet und Daten abfängt oder manipuliert. Werden Workloads in einer Enklave ausgeführt, sind die Daten während der Verarbeitung vor Bedrohungen geschützt. Durch die sichere Verteilung kryptografischer Schlüssel kann Confidential Computing aber auch dazu beitragen, die Kommunikation zwischen Nutzern und der Enklave durchgängig zu verschlüsseln und die Daten somit auch beim Transport zu schützen.

4. Risiken und Herausforderungen

Mit den bereits erwähnten Sicherheitslücken „Meltdown" und „Spectre" wurde offenkundig, dass es potenzielle Angriffsvektoren auf die Sicherheitsmechanismen gängiger Prozessoren gibt. Wenn Hacker diese Schwachstellen ausnutzen, sind sie theoretisch in der Lage, Daten aus Speicherbereichen abzurufen oder zu manipulieren, auf die sie eigentlich keinen Zugriff haben sollten.

CPU-Hersteller bieten seither immer wieder Firmware-Patches an, die bekannt gewordene Sicherheitslücken schließen sollen. Im ungünstigen Fall ist für den Anwender aber der Wechsel auf eine neuere Version des Prozessors notwendig, sollten die Probleme nicht durch eine aktualisierte Firmware zu beheben sein. Wichtig ist ein konsequentes Schwachstellen- und Patch-Management im Betrieb von Serversystemen. Dass Hackergruppen solche Sicherheitslücken früher entdecken, als sie Hardware-Herstellern bekannt werden, lässt sich jedoch nicht ausschließen.

4.1. Vendor Lock-in

Confidential Computing nutzt Micro-Instruktionen, die in Prozessoren verwendet werden, um Daten zu verschlüsseln. Damit bleibt die Hardware der Chiphersteller die technische Basis, der Anwender vertrauen müssen. Die führenden Halbleiterspezialisten Intel, AMD, ARM, IBM und Nvidia bieten mit ihren Server-Prozessoren derzeit die Möglichkeit, Anwendungen in vertrauenswürdigen Umgebungen auszuführen. Einzig die RISC-V-Architektur ist noch nicht für Confidential Computing ausgelegt. Aktuell wird in Projekten in Europa und China daran gearbeitet, die Prozessortechnologie in Richtung Confidential Computing zu erweitern. Alle Hersteller konzentrieren sich inzwischen ausschließlich auf Serversysteme, nachdem Intel anfänglich versucht hatte, das Konzept auch auf den Desktop-PC zu bringen.

Da die Basistechnologie für Confidential Computing in Prozessoren integriert ist, sind Anwender davon abhängig, wie die Chiphersteller ihre Produkte weiterentwickeln. Unter Umständen können bestimmte Funktionen abgekündigt werden. Außerdem sind die Verfahren, die in den CPUs verwendet werden, Stand heute nicht neutral durch Dritte auditierbar. Die Frage der Digitalen Souveränität verlagert sich somit im IT-Stack weiter nach unten auf die Ebene der Halbleiter. Diese Abhängigkeiten sind nicht unbedingt kritisch. Unternehmen sollten sich dessen aber bewusst sein.

Wie häufig in der IT-Industrie ähneln sich die Lösungsansätze der verschiedenen Hersteller und weichen in Details der Umsetzung voneinander ab. Abhängigkeiten entstehen für Anwender derzeit vor allem dadurch, dass Confidential Computing durch Hyperscaler und regionale Cloud Provider unterschiedlich implementiert wird. So hat AWS unter dem Label „Nitro" eine eigene Technologie entwickelt, die auf proprietärer Hardware (Steckkarten) basiert. Unternehmen können dem Vendor Lock-in entgegenwirken, indem sie Middleware einsetzen, sogenannte Multi-Cloud Confidential Computing Broker (MCCCB), die diese Unterschiede nivellieren. Das bedeutet aber auch, dass der Lock-in tendenziell eher auf der Ebene von Infrastructure as a Service (IaaS) und Platform as a Service (PaaS) liegt als auf der Ebene der CPU.

4.2. Potenzielle Schwachstellen

In den vergangenen Jahren wurde immer wieder über Angriffe auf Confidential-Computing-Technologien berichtet. 2023 legte Google eine tiefgehende Sicherheitsanalyse von Intel TDX vor. Dabei wurden 81 mögliche Angriffsvektoren erfasst, was zu zehn bestätigten Sicherheitslücken und fünf Änderungen der Tiefenverteidigung („Defense in depth") durch Intel führte. Der wichtigste Fund war ein Bug im Intel Authenticated Code Module (ACM), das für die Initialisierung von TDX zuständig ist. Der Fehler versetzte Angreifer in die Lage, Programme im privilegierten Modus auszuführen und vermeintlich geschützte VMs zu kompromittieren.

Ebenfalls 2023 entdeckten Forscher des CISPA Helmholtz-Zentrums für Informationssicherheit in Saarbrücken und der TU Graz die Schwachstelle „CacheWarpe" in AMD SEV. Dadurch konnten sich Angreifer über den Zwischenspeicher uneingeschränkten Zugang zu Enklaven verschaffen. AMD hat die Lücke durch ein Microcode-Update geschlossen. Weitere Erkenntnisse lieferten 2024 die „Ahoi Attacks", mit denen Forscher der ETH Zürich mögliche Angriffe auf SEV- und TDX-Umgebungen zeigten. Dabei werden nicht-vertrauenswürdige Hypervisoren genutzt, um vertrauenswürdige VMs zu kompromittieren. Die Angriffe können durch Sicherheitspatches im Linux-Kernel verhindert werden.

Um Schwachstellen zu beheben und die Sicherheit ihrer Enklaven weiter zu verbessern, haben die Hersteller über die Jahre viele Microcode-Updates und neue Versionen ihrer Prozessoren bereitgestellt. Weitere Angriffe der beschriebenen Art scheinen jedoch realistisch, insbesondere deshalb, weil die Architektur von VMs bisher auf der Basis vertrauenswürdiger Hypervisoren entwickelt wurde. Für die Sicherheit der Maschinen reicht das allerdings nicht aus. Darüber hinaus gilt es, die Betriebssysteme in vertrauenswürdigen VMs zu härten und besser zu schützen.

Bei der Identifizierung und Bewertung von Schwachstellen sind Unternehmen auf Experten angewiesen. Vollständige Analysen, welche potenziellen Angriffe für eine Applikation relevant sind und welche Sicherheitsmaßnahmen getroffen werden müssen, gibt es von den Herstellern nicht. Für TDX hat Intel ein "Security Guidance"-Dokument veröffentlicht, das ausführlich über Angriffsvektoren und entsprechende Gegenmaßnahmen informiert. Ähnliche Dokumentationen fehlen bislang für andere Confidential-Computing-Technologien.

Ein noch zu erforschendes Thema ist die sichere Nutzung vertrauenswürdiger Hardware aus Enklaven heraus. So wäre es wünschenswert, wenn darin ausgeführte Applikationen auch sicher auf Netzwerk- oder Grafikkarten zugreifen könnten. Architekturkonzepte gibt es dazu bereits, wie etwa AMD SEV-TIO und Intel TDX Connect TEE-IO, aber noch keine Umsetzungen. Ebenso ist noch unklar, wie die erweiterte Umgebung von entfernten Parteien per Attestation verifiziert werden kann.

5. Rechtsrahmen für Confidential Computing

Die Ausführung von Anwendungen und die Verarbeitung von Daten in vertrauenswürdigen Ausführungsumgebungen erfordert nicht nur technischen Integritätsschutz. Vielmehr unterliegt Confidential Computing auch gesetzlichen, regulatorischen und vertraglichen Anforderungen. Kennzeichen und Testate können Anwendern dabei Orientierung bieten und das Vertrauen in die Technologie fördern.

5.1. CRA und die CE-Kennzeichnung für IT-Produkte

Das CE-Kennzeichen des Normierungsinstituts CENELEC gibt an, dass ein Produkt die grundlegenden Anforderungen europäischer Richtlinien erfüllt („Conformité Européenne").

Mit dem Cyber Resilience Act (CRA) der EU, der in der zweiten Jahreshälfte 2024 in Kraft tritt und Hersteller digitaler Produkte zur Implementierung von Security-by-Design verpflichtet, werden sich auch die CENELEC-Anforderungen erhöhen. Ob für das CE-Kennzeichen eine Eigendeklaration des Herstellers genügt oder ob zuvor ein Audit durch unabhängige Dritte erfolgen muss, orientiert sich an drei Kritikalitätsstufen. Bei Confidential Computing wird eine Erklärung des Herstellers allein aber in keinem Fall ausreichen .

5.2. EUCS und Souveränität

Beim European Cybersecurity Certification Scheme for Cloud Services (EUCS) handelt es sich um ein Rahmenwerk, das die Zertifizierung von Cloud-Diensten im Hinblick auf Cybersicherheit regelt. Ziel ist, innerhalb der EU einheitliche und hohe Sicherheitsstandards für Cloud-Anbieter zu schaffen. Das EUCS ist noch nicht abschließend verhandelt, und der Termin dafür steht noch nicht fest. Ob und welche Souveränitäts-Erfordernisse in der endgültigen Fassung enthalten sein werden, ist deshalb noch offen. Es scheint sich allerdings abzuzeichnen, dass es national in einigen Ländern schärfere Regelungen zur Souveränität geben wird, auch wenn im EUCS darauf verzichtet werden sollte.

Souveränität lässt sich dabei als Kontrolle verstehen: physische Kontrolle über die Infrastruktur (Rechenzentren, Server, Datenleitungen, Mobilfunkantennen etc.), aber auch Kontrolle über die Daten, über ihren Speicher- und Verarbeitungsort sowie die Kontrolle über die Zugriffsberechtigungen und den Lebenszyklus der Daten. Bei diesen Dimensionen von Kontrolle kann Confidential Computing den erhöhten Schutzbedarf erfüllen.

Mit Enklaven stehen Anwendern dedizierte Umgebungen bereit, die von der Infrastruktur isoliert sind. Administrative Zugriffe darauf sind ausgeschlossen, sodass selbst der Betreiber der Infrastruktur, wie etwa ein Cloud Provider, an der unautorisierten Einsicht in die Daten gehindert wird, ebenso wie an ihrer unautorisierten Nutzung und Weitergabe. Auf diese Weise kann Confidential Computing den Anspruch von Unternehmen auf Souveränität einlösen, selbst wenn sie keine Kontrolle über die Infrastruktur haben. Das gilt unabhängig vom Ort der Verarbeitung, da die Daten bei richtiger Implementierung in jeder Dimension geschützt sind.

5.3. Confidential Computing bei der Umsetzung von Regularien

Relevant ist Confidential Computing im Kontext aktueller Regularien des Datenwirtschaftsrechts. Schließlich ist das Konzept geeignet, sowohl die Sicherheit und Privatsphäre von Daten als auch ihre Integrität zu gewährleisten. Zu diesen Regularien zählen insbesondere die Datenschutz-Grundverordnung (DSGVO), die zweite Auflage der Network and Information Systems Directive (NIS2) und der Digital Operational Resilience Act (DORA), eine spezifische Verordnung für den Finanzsektor.

Die DSGVO stellt strenge Anforderungen an den Schutz personenbezogener Daten. Confidential Computing kann Unternehmen dabei unterstützen, die Verordnung einzuhalten, denn die Technologie stellt die Vertraulichkeit und Integrität der Daten sicher, beispielsweise bei der Nutzung der Cloud. Weil die Daten auch bei der Verarbeitung verschlüsselt bleiben, wird das Risiko von Datenschutzverletzungen minimiert, was ein zentrales Anliegen der DSGVO ist.

Bei der NIS2-Richtlinie, die auf die erhöhte Sicherheit von Netzen und IT-Systemen abzielt, können betroffene Unternehmen ebenfalls von Confidential Computing profitieren. Denn das Konzept kann dazu beitragen, die Resilienz kritischer Infrastrukturen gegenüber Cyberangriffen zu erhöhen, indem es bei der Datenverarbeitung eine zusätzliche Schutzschicht bietet.

Ebenso kann Confidential Computing die Finanzindustrie unterstützen, die Anforderungen von DORA zu erfüllen. Durch die Verordnung sollen Banken und Versicherungen besser auf Cyberangriffe vorbereitet und die Widerstandsfähigkeit des Finanzsystems erhöht werden. Konkret fordert DORA in Artikel 6 „Verschlüsselung und kryptografische Kontrollen" sowie „Vorschriften für die Verschlüsselung von Daten im Ruhezustand, bei der Übermittlung und gegebenenfalls bei der Nutzung, wobei die Ergebnisse der genehmigten Datenklassifizierung zu berücksichtigen sind [...] Ist eine Verschlüsselung von Daten bei der Nutzung nicht möglich, so verarbeiten die Finanzunternehmen Daten bei der Nutzung in einer getrennten und geschützten Umgebung oder ergreifen andere gleichwertige Maßnahmen [...]"

Für die mit Blick auf DORA als „relevant" klassifizierten Daten sind Confidential Computing und Enklaven somit eine essenzielle Voraussetzung dafür, dass sie in der Cloud verarbeitet werden dürfen. Als relevant gelten Daten, die für den Betrieb eines Finanzinstituts wesentlich sind und deren Verlust oder Kompromittierung zu erheblichen Störungen führen würde. Ohne Verschlüsselung bei der Nutzung müssten solche Daten in dedizierten Systemen verarbeitet werden, um dem hohen Schutzbedarf zu genügen.

Festzuhalten ist, dass Confidential Computing einen signifikanten Beitrag dazu leisten kann, die Umsetzung technischer Maßnahmen, die der Compliance mit den genannten Regularien dienen, deutlich zu vereinfachen. Gleiches gilt für die Einhaltung von Normen, seien es allgemeine Sicherheitsstandards wie ISO 27001ff oder spezifische wie ISAX für den Automobilsektor.

6. Confidential Computing bei der Hyperscaler-Nutzung

Wenn Unternehmen ihre IT oder Teile davon auf der Plattform eines nordamerikanischen Hyperscalers betreiben, kann Confidential Computing zwei wesentliche Zwecke erfüllen. So bietet den Anwendern zum einen die Sicherheit, dass der Hyperscaler nicht auf ihre Daten im Klartext zugreifen kann. Damit wird auch das Risiko für eine mögliche Datenherausgabe durch den Cloud Provider auf der Basis von Regulierungen wie dem CLOUD Act minimiert. Was der Hyperscaler nicht sieht, kann er auch nicht herausgeben.

Confidential Computing schützt die Daten von Cloud-Anwendern zum anderen auch vor dem Zugriff durch andere Kunden auf der gleichen Plattform. Denn in der Public Cloud teilen sich viele Nutzer, denen Ressourcen flexibel und bedarfsgerecht zugewiesen werden, ein und dieselbe physische Infrastruktur („Shared Infrastructure"). Das bedeutet, dass eine physische Hardware potenziell von mehreren Kunden gleichzeitig genutzt wird. Auch wenn die Accounts logisch voneinander getrennt sind, bleibt ein Restrisiko. Confidential Computing gewährleistet, dass die Daten eines Kunden zu keinem Zeitpunkt für andere Kunden einzusehen, zu kopieren oder anderweitig zu verarbeiten sind.

Die Hyperscaler übernehmen zweifellos eine Vorreiterrolle, wenn es um die Adoption von Confidential Computing geht. Das Konzept hilft ihnen und ihren Kunden, den Sicherheits- und Datenschutzanforderungen in Europa zu genügen. Allerdings befinden sich die Angebote der Hyperscaler noch im Aufbau. Aktuell steht Confidential Computing bei ihnen noch nicht europaweit in allen Regionen zur Verfügung. So bietet Microsoft entsprechende Optionen vor allem in Irland und den Niederlanden an. Seit 2024 gibt es bei dem Cloud Provider auch hierzulande Enklaven, zunächst aber nur auf Basis von AMD SEV. Bei AWS ist zwar das eigene Nitro-System europaweit verfügbar. Confidential Computing auf Basis von AMD SEV stellt der Provider bislang jedoch nur in Irland bereit. Frankfurt steht auf der Roadmap. Bei Google sind vertrau-liche Umgebungen in Frankfurt verfügbar, allerdings nur auf Basis von AMD SEV, noch nicht auf Basis von Intel TDX.

Erste regionale Cloud Service Provider haben sich des Themas ebenfalls angenommen und beginnen damit, sich über spezifische PaaS-Angebote zu differenzieren. Beispielhaft können derzeit Adacor Hosting, Open Telekom Cloud (OTC), OVHcloud, STACKIT (Schwarz Gruppe) und vshosting genannt werden.

Die folgende Tabelle gibt einen Überblick über die Angebote der Hyperscaler[5], die unterstützten Basistechnologien und das Anwendungsspektrum:

Hyperscaler	Unterstützte Technologie	Anwendung	Bemerkung
Microsoft Azure	Intel SGX Intel TDX AMD SEV-SNP NVIDIA H100*	Virtuelle Maschinen Managed Kubernetes (AKS) Confidential AI	*Confidential AI ist in Private Preview
Google Cloud Platform	AMD SEV-SNP Intel TDX NVIDIA H100*	Virtuelle Maschinen Managed Kubernetes (GKS) Confidential AI	*Confidential AI ist in Private Preview
AWS	AMD SEV-SNP Nitro*	Virtuelle Maschinen Managed Kubernetes (EKS)	*Nitro ist ein AWS-eigenes Konzept der Enklavierung.
IBM	Intel SGX IBM SEL	Virtuelle Maschinen* Container Runtime*	*Teil der IBM Hyper Protect Platform
Oracle Cloud Infrastructure	AMD SEV AMD TSME	Virtuelle Maschinen Bare-Metal-Maschinen	
Alibaba	Intel SGX	Containerisierte Workloads	

5 siehe auch: https://docs.enclaive.cloud/virtual-hsm/documentation/supported-cloud-configurations

7. Anwendungsfelder und Beispiele für Use Cases

Confidential Computing eignet sich für Verarbeiter von besonders schützenswerten Personendaten, wie sie unter anderem in der DSGVO definiert sind. Dazu zählen Informationen über die ethnische und kulturelle Herkunft, politische, religiöse und philosophische Überzeugungen, Gesundheit, Sexualität und Gewerkschaftszugehörigkeit.

Ein typischer Anwendungsfall sind Gesundheitsdaten, die nur dann zum Vorteil der Patienten genutzt werden können, wenn auch autorisierte Dritte auf diese Daten zugreifen und sie aggregieren oder nach Bedarf mit weiteren Akteuren austauschen können. Mit Confidential Computing steht die Notwendigkeit, Daten zu nutzen, nicht im Widerspruch zum gesetzlich definierten Anspruch, diese Daten besonders zu schützen.

Da es sich bei Confidential Computing um ein grundlegendes technologisches Konzept handelt, finden sich Anwendungsszenarien in allen Industrien und bei Unternehmen jeder Größe. Wie beschrieben, liegt der Nutzen der Technologie darin, relevante Unternehmenswerte und -prozesse zu schützen sowie die Anforderungen nationaler und internationaler Regularien und Normen zu erfüllen.

Im Folgenden finden sich einige Beispiele.

7.1. Confidential Appliances

Ein Software-Unternehmen stellt seinen Kunden dedizierte Analyse-Umgebungen in Form besonders gesicherter Appliances bereit. Confidential Computing schließt dabei aus, dass die Nutzer auf den Code und die Logik der Applikation zugreifen können. So wird die Intellectual Property des Herstellers geschützt, auch wenn die Appliances bei den Kunden außerhalb seiner Kontrolle laufen.

7.2. Cloud Plattform für Human Resources

Ein Software-Hersteller hat eine globale, Cloud-basierte Plattform aufgebaut, über die Industriespezialisten unternehmensübergreifend zusammenarbeiten und dazu projektspezifische Teams bilden. Auf der Plattform, die bei einem Hyperscaler betrieben wird, sind alle wesentlichen Personaldaten von Experten, teilweise sogar Gesundheitsdaten, gespeichert. Confidential Computing ermöglicht es, sämtliche Personaldaten wie in einem Tresor aufzubewahren. Kunden des Plattformanbieters dürfen die sensiblen Informationen nur auf Basis streng geregelter Zugriffsrechte abrufen.

7.3. Internet of Things (IoT) als SaaS-Anwendung

Ein Hersteller von Analytics-Software für IoT-Szenarien hat sein Geschäftsmodell vom klassischen Lizenzverkauf auf Software as a Service (SaaS) umgestellt. Dabei hat Confidential Computing den Transformationsprozess unterstützt. Wie sich zeigte, förderte die Bereitstellung der Anwendung in einer vertraulichen Umgebung die Bereitschaft der Kunden, die Software in der Cloud zu konsumieren, anstatt sie lokal im Unternehmen zu installieren. Dadurch konnte der Anbieter die Heterogenität seiner installierten Basis in einem überschaubaren Zeitraum reduzieren.

7.4. Sichere Speicherung von Transaktionsdaten im Handel

Einzelhändler sind zunehmend gefordert, Transaktionsdaten zu speichern. Dabei gilt es nicht nur, jeden Kassenbon digital abzulegen und zu signieren. Durch die Saisonalität des Geschäftes variiert auch die benötigte Speicherkapazität stark, was die Cloud zum idealen und wirtschaftlichen Speicherort macht. Ein Handelsunternehmen löste die Herausforderung, indem es seine bestehende Anwendung redundant in zwei Clouds migriert hat. Confidential Computing erlaubt es dem Anwender, die Lösung compliant und resilient zu betreiben. Mit einem Virtual Hardware Security Module (vHSM) verwaltet das Unternehmen seine Schlüssel und Secrets selbst. Dadurch bleiben alle Kunden- und Zahlungsdaten sicher unter seiner Kontrolle, was in der ursprünglichen Umgebung nicht gegeben war.

7.5. Ende-zu-Ende-verschlüsselte Kommunikation

Ein Anbieter einer Kommunikations-Anwendung kam zu der Erkenntnis, dass er sein Kundenversprechen einer Ende-zu-Ende-Verschlüsselung auf einer virtuellen Appliance nicht halten kann. Die Datenströme werden zu Analysezwecken aufgebrochen und entschlüsselt, ehe die Datenpakete erneut verschlüsselt und weitergereicht werden. Aus diesem Grund hat der Hersteller die zentrale Komponente seiner Anwendung in eine Confidential-Computing-Umgebung migriert. Dadurch löst er nicht nur sein Wertversprechen nachprüfbar ein, sondern bietet seinen Kunden auch zusätzliche Flexibilität bei der Installation und Absicherung der Lösung.

7.6. Flexible Security-Umgebungen

Ein Security-Hersteller, zu dessen Portfolio bislang traditionelle Gateways und Appliances gehörten, hat seine Software innerhalb von zwei Wochen in eine Confidential-Computing-Umgebung übertragen. Diese Umgebung kann er nun flexibel für Kunden in der Cloud ihrer Wahl oder in ihrem eigenen Rechenzentrum ausrollen. Dadurch haben sich für den Anbieter neue Geschäftsmodelle ergeben, wie etwa die situative Bereitstellung sicherer virtueller Systemumgebungen.

7.7 Sichere Datenverarbeitung in der Gesundheitsbranche

Die Gesundheitsbranche zählt zu den Vorreitern beim praktischen Einsatz von Confidential Computing. So wird beispielsweise bei der Umsetzung der elektronische Patientenakte eine Lösung auf Basis von Intel SGX eingesetzt: Eine TEE setzt dabei die von der nationalen Agentur gematik geforderte vertrauenswürdige Ausführungsumgebung um und schützt auf diese Weise sensible Patientendaten während der Verarbeitung, und das auch vor Zugriffen der Betreiber. Die gematik trägt die Gesamtverantwortung für die Telematikinfrastruktur im deutschen Gesundheitswesen.

8. Wie lässt sich Confidential Computing praktisch umsetzen?

In der Praxis bietet die Einführung von Confidential Computing (CC) vielfältige Möglichkeiten, kritische Prozesse und sensible Daten zu schützen. Unabhängig davon, für welchen Ansatz ein Unternehmen wählt, gilt es darauf zu achten, dass nur minimale Anpassungen am Code von Anwendungen sowie an Tools und Prozessen vorgenommen werden müssen. Ein solches Vorgehen macht es für Unternehmen einfacher, die Vorteile von Confidential Computing schnell zu erproben. In einem ersten Schritt können beispielsweise Innovations-, Daten- oder AI-Teams innerhalb kurzer Zeit eine Technologie validieren. Natürlich ist es notwendig, im zweiten Schritt das Infrastrukturteam einzubinden, weil Betriebsaspekte für die gelungene Einführung wichtig sind. In der Erprobung sind sie aber noch nicht erfolgskritisch.

8.1. Handlungsempfehlungen für Anwenderunternehmen

Die Einführung von Confidential Computing kann in Unternehmen sehr unterschiedlich verlaufen, abhängig von der individuellen Infrastruktur- und Applikationslandschaft, den bestehenden Datenschutzmaßnahmen oder den vorhandenen Kenntnissen. Die folgenden Handlungsempfehlungen sollen als generischer Leitfaden dienen.

8.1.1. Kritische Prozesse und Daten identifizieren

Die Identifizierung kritischer Prozesse und Daten ist der erste Schritt zur erfolgreichen Einführung von Confidential Computing. Unternehmen sollten dabei einen ganzheitlichen Blick auf ihre Geschäftsabläufe werfen. Welche Prozesse sind für den Unternehmenserfolg besonders relevant? Welche Daten sind für die Ausführung dieser Prozesse unerlässlich und welche Konsequenzen hätte ein Datenverlust oder eine unbefugte Nutzung? Darüber hinaus müssen die gesetzlichen und regulatorischen Anforderungen, wie beispielsweise die DSGVO, berücksichtigt werden.

8.1.2. Schlüsselmanagement in die Unternehmenskontrolle bringen

Die Grundlage jedes kryptografischen Systems ist das Schlüsselmanagement. In der Regel sind sich Unternehmen, die Confidential Computing einführen wollen, der Bedeutung des Datenschutzes bewusst und verschlüsseln daher sensible Daten. Dabei ist das Schlüsselmanagement allerdings nicht selten an Dienstleister ausgelagert oder es kommen Key Management Services von Cloud-Anbietern zum Einsatz. Bei der Einführung von Confidential Computing empfiehlt es sich, sämtliche für das Schlüsselmanagement erforderlichen Technologien unter eigene Kontrolle zu bringen. Dazu zählen insbesondere Hardware Security Modules (HSMs), die dem sicheren Management kryptografischer Schlüssel dienen. Durch den Einsatz eigener physischer oder virtueller HSMs (vHSMs) erlangen Unternehmen die vollständige Kontrolle über alle Schlüssel und Secrets, die sie für ihre Anwendungen benötigen, und zwar unabhängig davon, ob diese Anwendungen lokal (On-Premises), in der Cloud oder in einer hybriden Umgebung ausgeführt werden.

8.1.3. Erste Pilotanwendungen benennen

Bei der Einführung von Confidential Computing empfiehlt es sich, mit Pilotprojekten zu starten. Dabei sollten einige wenige, repräsentative Anwendungen ausgewählt werden, um das Konzept in einer Multi-Cloud-Umgebung zu testen. Idealerweise setzt man dazu einen Multi-Cloud Confidential Computing Broker (MCCCB) ein. Diese Pilotprojekte dienen als Lernphase, um die spezifischen Anforderungen der Anwendung an die vertrauliche Ausführungsumgebung zu verstehen und potenzielle Herausforderungen frühzeitig zu identifizieren. Auf Basis dieser Erkenntnisse können dann konkrete Anwendungsfälle entwickelt werden, die die Vorteile von Confidential Computing voll ausschöpfen.

8.1.4. Geeignete Technologien und Dienstleister auswählen

Auf dem Markt sind unterschiedliche Produkte und Services für Confidential Computing verfügbar. Bei der Auswahl stellen sich verschiedene Fragen, etwa nach der Reife einer Lösung, nach Referenzen oder nach der Kompatibilität. Lässt sich die Technologie einfach in die vorhandene IT-Landschaft integrieren und welche Cloud-Plattformen unterstützt sie. Grundsätzlich müssen Anwender für sich entscheiden, ob sie eine Lösung selbst entwickeln oder ob sie ein weitgehend fertiges Produkt einführen wollen, das sie nur noch an ihre spezifischen Anforderungen anpassen müssen. Im einen wie im anderen Fall sollten sich Unternehmen zudem mit der Frage auseinandersetzen, inwieweit sie das Projekt mit eigenen personellen Ressourcen umsetzen können beziehungsweise inwieweit sie dafür Unterstützung durch externe Dienstleister benötigen.

8.1.5. Betriebsmodelle und Tools absichern

Die Einführung von Confidential Computing erfordert eine Anpassung der bestehenden Betriebsprozesse und -tools. Neben der Implementierung neuer Technologien zur Schlüsselverwaltung und der Konfiguration sicherer Ausführungsumgebungen ist eine kontinuierliche Überwachung und Wartung unerlässlich. Durch ein Monitoring der Systeme können potenzielle Sicherheitsrisiken frühzeitig erkannt und behoben werden. Zudem sollten Software und Hardware stets auf dem neuesten Stand gehalten werden, um bekannte Sicherheitslücken zu schließen und die Resilienz der Systeme zu erhöhen.

8.1.6. Deployment- und Migrationsoptionen evaluieren

Die Einführung von Confidential Computing erfordert eine sorgfältige Planung der Migrationsstrategie. Um Risiken zu minimieren und die Auswirkungen auf den laufenden Betrieb zu begrenzen, empfiehlt sich eine schrittweise Vorgehensweise. Ausgehend von Pilotprojekten können Unternehmen ihr Erfahrungswissen vergrößern und ihre Confidential-Computing-Szenarien kontinuierlich verbessern. Dabei ist eine enge Zusammenarbeit zwischen IT-Abteilung und Fachbereichen sinnvoll. Durch gezielte Schulungen können die Mitarbeiter für die neue Technologie sensibilisiert und

dazu befähigt werden, ihre Vorteile auszuschöpfen. Eine langfristige Strategie sichert die nachhaltige Nutzung von Confidential Computing und ermöglicht eine kontinuierliche Anpassung an sich ändernde Anforderungen.

8.2. Handlungsempfehlungen für SaaS-Anbieter

Cloud Computing hat Software-Anbietern die Möglichkeit eröffnet, Anwendungen als Service bereitzustellen. Ihre Kunden wiederum befreit das SaaS-Modell von der Notwendigkeit, Server-Infrastruktur zu beschaffen, und bietet ihnen flexible Nutzungsoptionen. Indem Provider ihre SaaS-Anwendungen in Enklaven betreiben, erhöhen sie die Sicherheit bei der Verarbeitung der Daten, weil diese vor unbefugten Zugriffen durch Dritte geschützt sind. Dadurch stärken sie das Vertrauen in ihr Angebot.

Dank der Verfügbarkeit von Multi-Cloud Confidential Computing Brokern (MCCCB) und Open-Source-Werkzeugen haben SaaS-Anbieter die Möglichkeit, das Konzept innerhalb weniger Tage zu erproben. Auf diese Weise können sie evaluieren, wie ihre Anwendungen in vertraulichen Ausführungsumgebungen funktionieren und ob sich Confidential Computing für sie als Business Case rechnet. Für die einschlägigen Technologien gelten die im Markt üblichen OEM-Modelle auf Subskriptionsbasis.

8.3. Handlungsempfehlungen für Service Provider

Potenzial birgt Confidential Computing auch für Service Provider, die damit die Sicherheit ihrer Infrastrukturdienste erhöhen können. Ihnen empfiehlt sich ein Vorgehen in drei Phasen[6]. Dabei sollten sie im ersten Schritt die Grundlagen aufbauen, das heißt, die Server-Hardware identifizieren (oder bei Bedarf neu beschaffen), die Confidential Computing unterstützt, klare Richtlinien für Zugangskontrolle, Schlüsselverwaltung und Protokollierung festlegen und ihre Teams in der neuen Technologie schulen.

Die zweite Phase ist dem Aufbau der Confidential-Computing-Umgebung gewidmet. In dieser Phase sollten Provider ein Virtualisierungskonzept entwickeln, mit dem sich vertrauliche VMs und idealerweise auch vertrauliche Container managen lassen. Außerdem sollten sie die Umgebung intensiv auf ihre Sicherheit hin testen. In der Phase der Service-Bereitstellung geht es darum, vertrauliche Cloud-Dienste anzubieten, die den Bedarf einzelner Branchen adressieren, ein Partnerökosystem aufzubauen, spezifische Zertifikate zu erwerben und die Vorteile von Confidential Computing aktiv zu vermarkten.

An dieser Stelle würden detaillierte Empfehlungen sowohl für SaaS-Anbieter als auch für Service Provider allerdings den Rahmen des vorliegenden Whitepapers sprengen, das im Wesentlichen die grundlegende Funktionsweise und die Vorteile von Confidential Computing behandelt. Solche Handlungsempfehlungen könnten Gegenstand eines weiteren, stärker praxisorientierten Dokuments sein.

6 siehe auch: https://next.enclaive.cloud/s/rssJ5c54RJfLCp5j

9. Fazit und Ausblick

Confidential Computing ist kein grundlegend neues Konzept. Mit den heute verfügbaren Technologien und dank der Unterstützung durch Cloud Provider und Managed Infrastructure Provider ist es aber nicht mehr nur eine theoretische Möglichkeit, sondern lässt sich praktisch realisieren. Tatsächlich hat sich die Umsetzbarkeit inzwischen derart vereinfacht, dass Anwender und Software-Anbieter die Möglichkeiten des Konzepts auch ohne tiefgreifendes kryptografisches Wissen nutzen können.

Durch die Kombination von hardwarebasierten Sicherheitsmechanismen, eigenständigem Schlüsselmanagement und der Möglichkeit, den Sicherheitszustand einer genutzten Umgebung zu validieren, bietet Confidential Computing eine robuste Lösung für den Schutz von Daten vor unbefugtem Zugriff. Unternehmen sind mit Hilfe dieser Technologie in der Lage, ihre sensiblen Daten auch in der Cloud sicher zu verarbeiten und damit die Plattformen der Hyperscaler richtlinienkonform zu nutzen.

Zusammen mit einem konsequenten Zero-Trust-Modell stehen Unternehmen damit zwei starke Ansätze zur Verfügung, die ihnen dabei helfen, generische Schutzziele wie Vertraulichkeit und Integrität zu gewährleisten und sich dabei stetig zu verbessern. Besonders in Branchen wie dem Finanzwesen oder dem Gesundheitswesen, in denen der Schutz sensibler Daten von höchster Bedeutung ist, eröffnet Confidential Computing neue Möglichkeiten für innovative Geschäftsmodelle und stärkt das Vertrauen von Kunden und Geschäftspartnern.

Allerdings ist die Einführung von Confidential Computing mit Herausforderungen verbunden. Neben technischen Aspekten wie Performance und Kosten müssen auch organisatorische Aspekte wie die Anpassung von Prozessen und Schulungen berücksichtigt werden. Durch eine sorgfältige Planung und eine kontinuierliche Überwachung können diese Herausforderungen jedoch bewältigt werden.

Die Zukunft von Confidential Computing ist vielversprechend. Mit der weiteren Entwicklung von Hardware und Software sowie der Integration in andere Technologien werden sich neue Einsatzmöglichkeiten eröffnen. Unternehmen, die frühzeitig auf das Konzept setzen, können sich einen Wettbewerbsvorteil verschaffen und ihre Geschäftsmodelle zukunftssicher gestalten.

Autoren des Textes:

Achim Astel
noris network AG

Anna Fischer
secunet Security Networks AG

Prof. Dr. Sebastian Gajek
Hochschule Flensburg

Nicolas Maeding
IBM Deutschland
Research & Development GmbH

Prof. Dr. Norbert Pohlmann
Institut für Internet-Sicherheit –
if(is) an der Westfälischen Hochschule

Andreas Walbrodt
enclaive GmbH

EuroCloud
DEUTSCHLAND | eco

EuroCloud Deutschland_eco e.V.
Lichtstraße 43h
50825 Köln

Tel.: 0221 / 70 00 48 – 0
Fax: 0221 / 70 00 48 – 111

E-Mail: info@eurocloud.de
Web: https://www.eurocloud.de/