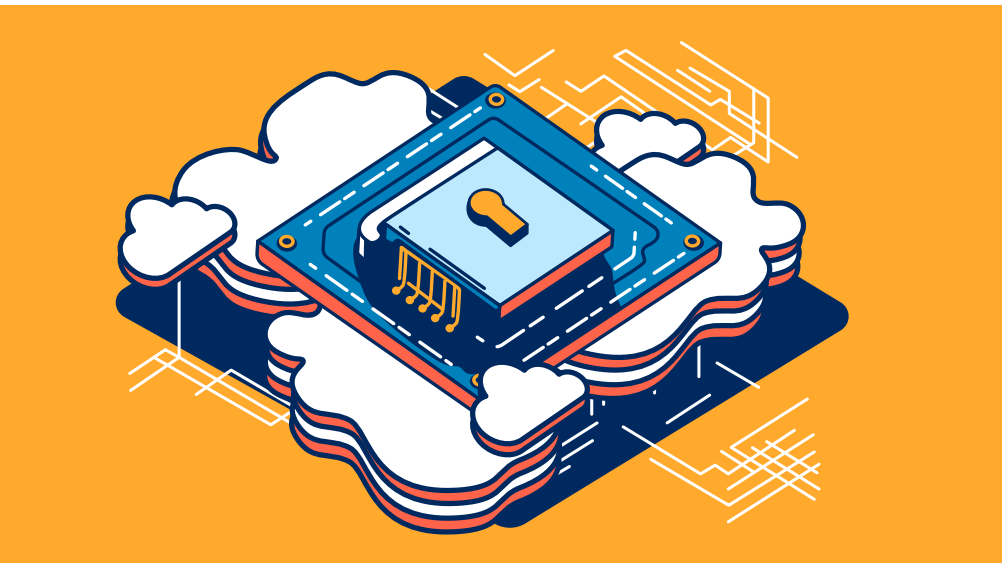


Confidential VMs mit Intel Trust Domain Extensions

Vertrauenswürdigkeit ist ein immer wichtigerer Aspekt moderner IT. Intel hat die vierte Generation seiner Xeon-Enterprise-Prozessoren um die Trust Domain Extensions (TDX) erweitert. Damit lassen sich komplette VMs in einer vertrauenswürdigen Umgebung ausführen.

Von Dr. Sebastian Gajek und Prof. Dr. Norbert Pohlmann

Das Vertrauen von Unternehmen in Cloud-Anwendungen ist heute noch eher gering, da Angst davor besteht, dass Unbefugte auf vertrauliche Daten in der Cloud zugreifen könnten. Als Lösung dafür nutzt Confidential Computing eine hardwaregestützte, vertrauenswürdige Ausführungsumgebung. Jegliche darin ausgeführte Software und die zugehörigen Daten sind vor Zugriffen von anderer Software oder Hardware geschützt.

Public Cloud mit dem Vertrauen eines On-Premises-Ansatzes

Durch die Verlagerung der IT in die Public Cloud können Unternehmen Kosten sparen und dennoch die IT-Sicherheit und den Datenschutz gewährleisten. Confidential Computing (CC) ermöglicht einen durchgängigen Schutz sensibler Daten während ihres gesamten Lebenszyklus – vom Verlassen des Firmengeländes bis zum Eintritt in die Cloud-Infrastruktur –, indem man nur noch den Prozessoren und deren Anbietern vertrauen muss. Das bedeutet, dass selbst Cyberangreifer, Dienstleister und Cloud-Administratoren, die die Infrastruktur vollständig kontrollieren, keinen Zugriff auf unverschlüsselte Daten erhalten können.

Somit können Nutzer ihre Workload auf einer fremden Cloud-Infrastruktur schützen, was erhebliche Erleichterung in der Security-Compliance bringt und Anwendungen in der Cloud ermöglicht, die bislang nicht denkbar waren oder nur in einer On-Premises- oder hybriden Umgebung realisiert wurden. Aber auch für Datacenter-Betreiber ist die Confidential-Computing-Technologie gedacht. Sie verbessert schlagartig die Resilienz gegen Cyberangriffe ihrer Workloads, ohne zusätzliche Kosten zu erzeugen.

Intel hatte schon vor Jahren seine Software Guard Extensions (SGX) vorgestellt, mit denen sich einzelne Applikationen in einer vertrauenswürdigen Ausführungsumgebung ausführen und schützen lassen. Mit Einführung der vierten Xeon-Enterprise-Generation hat der Chiphersteller sein Computing-Portfolio um Intel Trust Domain Extensions (TDX) erweitert. Sie führen komplette virtuelle Maschinen in einer vertrauenswürdigen Umgebung aus. Dies ermöglicht eine neue Virtualisierungsgeneration, die verspricht, auf der Basis der CPU-internen Sicherheitsfunktionen jegliche in der VM ausgeführte oder verarbeitete Software und Daten zu schützen.

Erreicht wird dies durch eine Verschlüsselung der zugehörigen Daten im Arbeitsspeicher und Zugriffskontrollen innerhalb der CPU (siehe Kasten „TDX-Architektur und -Fähigkeiten“). Hyperscaler wie Alibaba, Azure, IBM und Google arbeiten intensiv an der Bereitstellung der Basistechnologie in ihrer Cloud, um dem langjährigen Wunsch nach harter Isolation zwischen Infrastruktur und Applikations- und Geschäftslogik, Datensouveränität sowie Compliance mit Datenschutz nachzukommen und damit die Vorteile der öffentlichen Cloud mit dem gewohnten Vertrauen eines On-Premises-Ansatzes zu kombinieren.

Intel TDX ist eine technologische Evolution

TDX führt den Secure-Arbitration Mode (SEAM) ein, um vertrauliche VMs, die in der TDX-Terminologie Trust Domains (TDs) heißen, kryptografisch zu isolieren. TDX baut auf einer Reihe vorhandener

iX-TRACT

- Die Anforderungen von Privacy Shield und Datensouveränität sind dank Confidential Computing technisch umsetzbar.
- Es liefert hardwaregestützt eine vertrauenswürdige Ausführungsumgebung für Cloud-Anwendungen.
- Über die von Intel in der vierten Xeon-Enterprise-CPU-Generation eingeführte Trust Domain Extension können komplette VMs in einer vertrauenswürdigen Umgebung laufen.
- Mit einem mehrstufigen Remote-Attestation-Verfahren lässt sich der kryptografische Schutz einer Trust Domain von dritter Seite sicher verifizieren.

Glossar

CC – Confidential Computing: Computing-Paradigma ähnlich zu Trusted Computing mit der Erweiterung von Runtime Memory Encryption und Fokus auf Cloud-Sicherheit.

CET – Control Flow Enforcement Technology: Intel-Technik zum Schutz der Ausführung eines Programms durch Überprüfung der Integrität des Programmflusses über einen Shadow Stack.

DCAP – Data Center Attestation Primitives: Intels Framework zur Attestierung von Trusted Domains.

HSM – Hardware Security Module: kryptografischer Coprozessor mit kryptografischen Algorithmen und sicherem Speicher durch spezielle Hardwareschutzmaßnahmen.

KMS – Key Management Service: Dienst zum Generieren, Austauschen und Speichern von Schlüsseln. Im Kontext der Cloud der Vertrauensanker für die Umsetzung sicherer Applikationen.

MKTME – Multi-Key Total Memory Encryption: Intels Spezifikation zur sicheren Erzeugung von Schlüsseln für Trusted Domains.

PCCS – Provisioning Certificate Caching Service: Service innerhalb des DCAP-Frameworks, speichert die Zertifikatskette zum Verifizieren der Root of Trust des DCAP-Frameworks.

PCE – Provisioning Certificate Enclave: Enklave innerhalb des DCAP-Frameworks. Fungiert wie eine lokale Certificate Authority und zertifiziert das Schlüsselpaar der QE, das eine Quote signiert.

QE – Quoting Enclave: Enklave innerhalb des DCAP-Frameworks; signiert den Attestierungsreport.

SEAM – Secure-Arbitration Mode: Intels mit TDX eingeführter Virtualisierungsmodus, um einen VM-Prozess in einem verschlüsselten Speicherbereich auszuführen.

SGX – Software Guard Extensions: Securityerweiterung der Intel-CPU-Architektur, um Applikationen zu kapseln und Prozesse kryptografisch voneinander zu trennen.

TD – Trust Domain: eine zur Laufzeit verschlüsselte und authentifizierbare virtuelle Maschine.

TDX – Trust Domain Extensions: Securityerweiterung der Intel-CPU-Architektur, um virtuelle Maschinen zu kapseln und Hardwareressourcen kryptografisch zu isolieren.

TEE – Trusted Execution Environment: Sicherheitskonzept zum Ausführen von Programmen in einer sicheren, vertrauenswürdigen Umgebung, in der Regel auf Basis von Hardware wie einem HSM.

TLB – Translation Lookaside Buffer: Zwischenspeicher, um die Zustände einer TD zu managen und im Falle von Context Switches zu retten oder zu löschen.

VT – Virtualization Technology: Technik zur softwareseitigen Isolation von Hardwareressourcen. Im Cloud-Computing eine bewährte Methode, physische Ressourcen auf mehrere Nutzer zu verteilen.

Techniken auf, darunter Virtualization Technology (VT), Multi-Key Total Memory Encryption (MKTME) und Trusted Execution Technology (TXT). TDX stützt sich auch auf Software Guard Extensions (SGX) und Data Center Attestation Primitives (DCAP) für die Verifizierung der TD.

Dem Host nicht vertrauen

Das Zero-Trust-Bedrohungsmodell geht davon aus, dass privilegierte Software wie Hypervisoren, Host-Betriebssysteme oder Firmware nicht vertrauenswürdig sind oder zumindest angreifbar sein können. Auch geht es davon aus, dass ein Angreifer Zugang zum Hauptspeicher oder zu anderen Geräten hat. TDX zielt darauf ab, die Vertraulichkeit und Integrität des CPU-Status und des Speichers für TDs zu schützen. Zudem ermöglicht es den TD-Besitzern, die Authentizität der TD per Ferndiagnostik (auch als Remote Attestation bezeichnet) zu überprüfen.

TDs haben neben dem Aspekt der Geheimhaltung der Workload auch einen pragmatischen Effekt. Sie schützen vor vielen Angriffen, die in einer verteilten, virtualisierten Umgebung wie der Cloud passieren. Dazu zählen Attacken wie Rowhammer, Meltdown oder ROP-Attacken (Return-oriented Programming), die eine VM kontaminieren, um in benachbarte VMs einzubrechen. Aber die Laufzeitverschlüsselung schützt auch vor physischen Angriffen wie Cold Boot oder DRAM Probing. Darüber hinaus untersuchen Forscher derzeit die Resilienz gegen Seitenkanalangriffe.

Wie wird eine TD zur Laufzeit isoliert und verschlüsselt?

Secure-Arbitration Mode (SEAM) ist eine Erweiterung der VMX-Architektur und bietet zwei neue Ausführungsmodi: SEAM VMX root mode und SEAM VMX non-root mode. Ein mit TDX erweiterter Hypervisor arbeitet im traditionellen VMX-Root-Modus und verwendet die Anweisung `SEAMCALL`, um hostseitige Schnittstellenfunktionen (Funktionsnamen beginnen mit `TDH`) des TDX Module aufzurufen. Bei Ausführung des `SEAMCALL`-Befehls wechselt der logische Prozessor vom Modus VMX root in den SEAM-Modus root und beginnt mit der Ausführung von Code innerhalb des TDX Module. Sobald dies seine Aufgabe erfüllt hat, kehrt es durch Ausführen des Befehls `SEAMRET` zum Hypervisor im VMX-root-Modus zurück.

TDs hingegen laufen im Modus SEAM VMX non-root. Sie können entweder durch ein `TD EXIT` oder durch die Anweisung `TD CALL` in das TDX Module wechseln. In beiden Fällen wechselt der logische Prozessor vom SEAM-Modus VMX non-noot in den SEAM-Modus VMX root und beginnt die Ausführung im Kontext des TDX Module. Die Namen der gastseitigen Schnittstellenfunktionen, die `TD CALL`s verarbeiten, beginnen mit `TDG`.

Das TDX Module bietet zwei Gruppen von Schnittstellenfunktionen: hostseitige für einen TDX-erweiterten Hypervisor und gastseitige für TDs. Es wird vom Hypervisor in den SEAM RANGE geladen, einen Teil des Systemspeichers, der über UEFI/BIOS wie auch schon bei Intel SGX reserviert wird, und dort ausgeführt. Eine Memory Encryption Engine verschlüsselt die Prozessorinstruktionen in der SEAM RANGE. In der aktuellen TDX-Version ist das AES-XTS. MKTME stellt sicher, dass jede TD mit einem eigenen Schlüssel verschlüsselt wird, der zur Bootzeit generiert wird und nicht per Software aus der CPU extrahierbar ist. Der P-SEAM Loader, der sich ebenfalls im SEAM RANGE befindet,

TDX-Architektur und -Fähigkeiten

Intels TDX setzt sich aus zwei Schlüsselkomponenten zusammen:

- TDX-fähigen Prozessoren, die architektonische Funktionen wie hardwaregestützte Virtualisierung, Speicherverschlüsselung/Integritätsschutz und die Fähigkeit zur Zertifizierung von TEE-Plattformen bieten;
- einem TDX Module, einem von Intel signierten und CPU-zertifizierten Softwaremodul.

Das TDX Module nutzt die Funktionen der TDX-fähigen Prozessoren, um das Erstellen, Ausführen und Beenden von Trust Domains (TDs) zu erleichtern und gleichzeitig die Sicherheitsgarantien durchzusetzen. Damit soll ein TDX-System drei Fähigkeiten realisieren.

Vertraulichkeit des Speichers: Werden die Daten vom Prozessor in den Hauptspeicher verlagert, verschlüsselt die CPU sie mit einem TDX-spezifischen Schlüssel. Der ist nur ihr bekannt, wird bei jedem Systemstart neu generiert und jede TD hat einen eigenen Schlüssel. Die CPU wirkt als Vertrauensanker und speichert den Key sicher in einem per Hardware geschützten Bereich. Auf diese Weise „verschlüsselt" der Prozessor auch das Programm im Speicher. Die Verschlüsselung erfolgt in der Granularität der Cache-Zeilen, sodass Peripheriegeräte den privaten Speicher der TD nie unbemerkt lesen oder manipulieren können. Beim Laden der Daten aus dem Hauptspeicher entschlüsselt der Prozessor die Daten und prüft zudem die Integrität. Dadurch werden Manipulationen an den Daten erkannt.

Vertraulichkeit des CPU-Status: Laufen mehrere TDs gleichzeitig (auf unterschiedlichen Kernen), dann stellt der Prozessor durch Zugriffskontrolle sicher, dass eine TD jeweils nur auf die eigenen Daten zugreifen kann. Sobald ein Kern die Verarbeitung einer TD pausiert, sichert der Prozessor die CPU-Zustände, indem er sie in den Metadaten der TD speichert, die im Hauptspeicher durch den Schlüssel der TD geschützt sind. Während der Kontextwechsel löscht oder isoliert TDX die TD-spezifischen Zustände aus internen Prozessorregistern und Puffern, wie TLB-Einträgen (Translation Lookaside Buffers) oder Verzweigungsvorhersagepuffern (Branch Prediction Buffers), um den Schutz der TD-Informationen zu gewährleisten.

Ausführungsintegrität: TDX schützt die Integrität der TD-Ausführung vor Störungen durch den Host und stellt sicher, dass die TD ihre Berechnungen nach einer Unterbrechung bei der erwarteten Anweisung innerhalb der erwarteten Zustände wieder aufnimmt. Dabei kann es böswillige Änderungen der virtuellen CPU-Zustände sowie das Einfügen, Ändern oder Entfernen von Anweisungen im privaten Speicher erkennen, bietet jedoch keine zusätzlichen Garantien für die Integrität des Kontrollflusses. Es liegt in der Verantwortung des TD-Eigentümers, bestehende kompilationsbasierte oder hardwaregestützte Verfahren zur Durchsetzung der Kontrollflussintegrität, wie die Control Flow Enforcement Technology (CET), zu verwenden.

kann das TDX Module installieren und aktualisieren.

Verifikation per Remote Attestation

Neben dem kryptografischen Schutz einer TD verifiziert Intel TDX sie auch per Remote Attestation. Hierbei kann eine dritte Partei einen Beweis (eine sogenannte Quote) erhalten, mit dem sich folgende Dinge attestieren lassen: Die in der TD ausgeführte Software (inklusive Firmware, eventuell Bootloader, Betriebssystem und Anwendungen) ist wie gewünscht und unverändert, die TD wird von TDX geschützt und die Maschine ist auf aktuellem Patch-Stand.

Wie schon bei SGX stellt Intel das DCAP-Framework als Referenzimplementierung für Remote Attestation bereit, die über eine PKI die CPU durch Intel zertifizieren lässt. Zusätzlich stellt Intel weitere Dienste bereit: die Quoting Enclave (QE) zum Generieren der Quote, die Provisioning Certificate Enclave (PCE) zum Zertifizieren des Attestierungsschlüssels der QE und den Provisioning Certificate Caching Service (PCCS) zum Offline-Speichern der für die Verifizierung der Zertifikatskette erforderlichen Schlüssel und Identitäten. Den Code dieser Dienste hat Intel veröffentlicht, sodass sie sich ebenfalls verifizieren lassen. Auch ist es dem Nutzer überlassen, die Dienste alternativ selbst bereitzustellen und somit auch ein eigenes Remote-Attestation-Protokoll zu implementieren. Einen Standard für das Protokoll gibt es noch nicht, eine Working Group des Confidential Compute Consortium arbeitet aber daran.

Wie läuft eine Attestierung ab?

Der Challenger sendet eine Attestierungsanforderung mit einer Nonce an den Attestation Agent (Schritt 1). Die Nonce sorgt für die Aktualität der Anfrage und verhindert Replay-Angriffe. Der Agent ruft einen TD-Bericht vom TDX Module ab, der die Nonce als `REPORTDATA` enthält (Schritt 2), und fordert anschließend die Quoting Enklave (QE) auf, den TD-Bericht mit ihrem Attestierungsschlüssel zu signieren (Schritt 3). Die QE verifiziert mittels lokaler Attestierung, dass der TD-Bericht auf der Plattform generiert wurde, bevor sie ihn mit ihrem Attestierungsschlüssel signiert. Der Attestierungsagent sendet dann das Angebot an die Gegenpartei zurück (Schritt 4).

Die Gegenpartei benötigt das PCK-Zertifikat der Plattform, um die Offerte zu verifizieren. Sie kann daher das PCK-Zertifikat von einem PCCS herunterladen (Schritt 5a) oder direkt vom Intel PCS abrufen (Schritt 5b). Der Challenger fährt dann mit der Validierung der Quote fort (Schritt 7). Er prüft die Nonce und verifiziert die Integrität der Signaturkette von einer Intel CA über das PCK-Zertifikat bis zur signierten Quote. Der Challenger überprüft auch, ob Schlüssel in der Kette widerrufen wurden und ob die TCB (beispielsweise QE, PCE) aktuell ist. Schließlich prüft der Challenger, ob die Messungen der TD in der Quote mit einer Reihe von Referenzwerten übereinstimmen. Bei erfolgreicher Validierung kann die entfernte Partei darauf vertrauen, dass das TD auf einer TDX-Plattform ordnungsgemäß instanziiert wurde.

Exemplarische Use Cases für den TDX-Einsatz

Mit Intels TDX werden VMs vertraulich. Damit existiert jetzt eine Technologie, mit der man Applikationen in einem Tresor ausführen kann – egal, ob in einer privaten, hybriden oder öffentlichen Cloud. Insbesondere datenhungrige Applikationen profitieren in Umgebungen davon, wo es bislang schwierig war, die Daten zu verarbeiten.

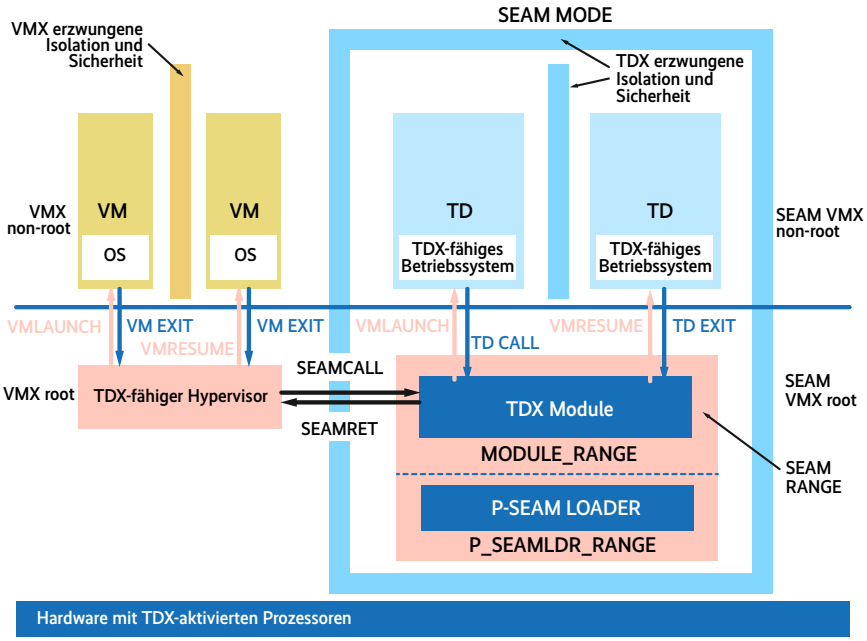
Data-in-Use-verschlüsselte Datenbanken

Datenbanken sind häufig das Herzstück einer Applikation und bedürfen Schutz,

weil sie in der Regel sensitive Daten verarbeiten und speichern. So sind Sicherheitskonzepte wie Data-in-Transit- und Data-at-Rest-Verschlüsselung aus Datenbanken nicht mehr wegzudenken. Data-in-Transit-Verschlüsselung bezeichnet die gesicherte Kommunikation mit der Datenbank. Häufig wird sie per TLS abgesichert und die Datenbank über einen Key Management Service (KMS) mit dem Zertifikat oder Admin-Passwort provisioniert. Zum Absichern der Datenbank werden die Daten auf dem persistenten Volumen verschlüsselt gespeichert. Gängig in Datenbanken ist Data-at-Rest-Verschlüsselung, also die Verschlüsselung von Daten in einem persistenten Speicher. In virtualisierten Umgebungen lassen sich hierfür Disk-Verschlüsselungsverfahren wie LUKS einsetzen. Auch hier ist ein Key Management notwendig, insbesondere eines, mit dem sich Schlüssel rotieren lassen.

Sobald die Datenbank die Daten verarbeitet, liegen die Daten unverschlüsselt im Hauptspeicher, was in einer Cloud-Umgebung unerwünscht ist. Ein einfacher Memory-Dump reicht aus, um Zugriff auf die Daten zu erhalten. In GitHub finden sich Tutorials, die zeigen, wie einfach die Datenbankeinträge über einen Memory Dump auszulesen sind (siehe ix.de/zrny).

Läuft hingegen die Datenbank in einer TD, so gibt es drei Vorteile für Admins: Die Daten sind auch während der Verarbeitung verschlüsselt, das komplizierte Rotieren der Schlüssel entfällt, weil der Decryption Key des Disc Image nicht wie bei Data-at-Rest-Verschlüsselung im



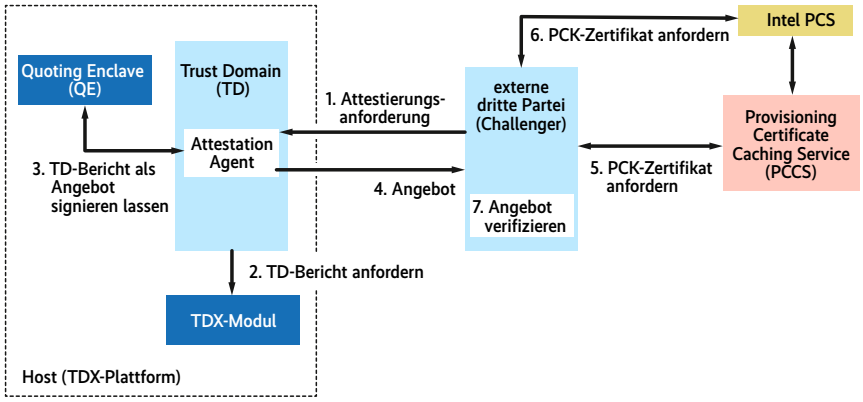
Intels TDX-Architektur setzt sich aus zwei Schlüsselkomponenten zusammen, die im Zusammenspiel mit den in früheren CPU-Generationen eingeführten VMX-Erweiterungen einen sicher gekapselten Betrieb von VMs erlauben (Abb. 1).

Klartext im Speicher steht, und es sind keine Modifikationen an der Applikation oder am DevOps-Prozesses nötig. Data-in-Use-Verschlüsselung war ein bislang offenes Problem, das sich mit CC-Technologien erstmals lösen lässt. Das Datum wird nicht mehr für das Prozessieren der Datenbank entschlüsselt, sondern es bleibt im Speicher geheim. In Kombination mit Data-at-Rest- und -in-Transit-Verschlüsselung ist die Applikation in einem Tresor geschützt vor Dritten.

Confidential HSM

Hardware Security Modules (HSM) dienen zum Härten des Schlüsselmanagements. In Hardware realisierte Schlüsselgeneratoren, -register und kryptografische Algorithmen verhindern eine softwareseitige Extraktion und Manipulation. Teure HSMs lassen sich nun durch softwarebasierte HSMs in einer TD austauschen, sogenannte Confidential HSMs. TDX deckt mit seinen Hardwarefähigkeiten auch den Funktionsumfang eines HSM ab – mit dem Vorteil, dass die Kryptografie „soft“ austauschbar ist.

So lassen sich mit einem TDX-fähigen Prozessor Millionen von Schlüsseln in einer TD verwalten. Hier kommt eine Binding-Eigenschaft zum Einsatz, die die TD an den Prozessor bindet. Auf Basis der Messung der TD und Verifikation der Integrität der Plattform leitet der Prozessor einen Binding-Key ab, mit dem persistent



In einem mehrstufigen Remote-Attestation-Verfahren lässt sich der kryptografische Schutz einer TD von dritter Seite verifizieren (Abb. 2).

gespeicherte Keys ent- und verschlüsselt werden. So lassen sich kostengünstig proprietäre, nicht standardisierte oder quantensichere Algorithmen integrieren. Auch sind komplexere Anwendungen für Passwort-, PKI- und Identitätsmanagement in einer isolierten TD umsetzbar: stets unter der Maxime, dass Geheimnisse wie kryptografische Schlüssel, Passwörter und Zugangs-Policies vor unerwünschten Dritten verborgen bleiben.

Confidential Nextcloud

Nextcloud ist eine Kollaborationsplattform, die in den letzten Monaten als deutsche Open-Source-Alternative zu Microsoft-365-Produkten wie File Storage, Online Collaboration, Chat Messaging oder Videotelefonie gehandelt wurde. Ausgangspunkt war die Kritik an der DSGVO-Verträglichkeit von MS-365-Produkten in Schulen und anderen öffentlichen Institutionen, als deutlich wurde, dass die Daten nicht auf nationalen Servern gespeichert werden. Nextcloud ermöglicht das Hosting im eigenen Rechenzentrum. Damit können die Daten auf nationalen Servern hinterlegt werden. Das birgt aber einen Adminstrations-Overhead und die Verantwortung, die Daten vor Diebstahl und Missbrauch zu schützen. Um die IT-Abteilung zu entlasten, wäre eine SaaS-basierte Lösung wünschenswert.

Nun besteht wieder das Dilemma, dass eine dritte Partei Zugriff auf die Daten hat. Confidential Computing mit Intels TDX ist hierfür eine charmante Lösung. Führt der SaaS-Anbieter jeden einzelnen Nextcloud-Container in einer TD aus, so sieht der Drittanbieter zu keinem Zeitpunkt die Daten, kann aber die Verfügbarkeit des Dienstes sicherstellen, Updates einspielen und auch Maßnahmen gegen Cyberattacken einleiten. Aufgaben, die das IT-Team abgeben kann, um sich nur um die Zugangskontrolle zu kümmern. Einige Anbieter – AWS, Azure, Google Cloud, OVH und OTC – stellen die Confidential Nextcloud zur Verfügung und setzen die oben genannten Vorteile um, indem sie per CC die Vorteile einer SaaS-Applikation mit dem Vertrauen einer On-Premises-Lösung kombinieren.

Was noch kommt: Intel TDX 1.5 und 2.0

Intel hat TDX im Januar 2023 vorgestellt und aktuell gibt es die Version 1.0 bei den ersten Cloud-Service-Providern im (Private) Preview. Dabei handelt es sich um Intels erste Technik zum Schutz virtueller Maschinen, womit man mit der bereits verfügbaren Konkurrenztechnologie AMD Secure Encrypted Virtualization (SEV) gleichzieht. Auch hat Intel bereits angekündigt, weitere Funktionen hinzuzufügen:

Nested Virtualisierung: Intel TDX 1.0 beherrscht keine verschachtelte Virtualisierung. Das bedeutet, innerhalb einer TD dürfen keine VMs ausgeführt werden. Der Versuch, VMX-Anweisungen innerhalb eines TD zu nutzen, kann zu Undefined-Instruction-Ausnahmen führen. Der Entwurf der TD-Partitionierungsarchitektur deutet darauf hin, dass TDX 1.5 künftig verschachtelte Virtualisierung unterstützen wird.

I/O-Schutz: Peripheriegeräte oder Beschleuniger befinden sich außerhalb der Vertrauensgrenzen von TDs und dürfen nicht auf den privaten Speicher der TD zugreifen. Für virtualisiertes I/O kann eine TD explizit Speicher für die Datenübertragung freigeben. TDX bietet jedoch keinen Vertraulichkeits- und Integritätsschutz für die Daten in gemeinsam genutzten Speicherbereichen. Es liegt in der Verantwortung der TD-Besitzer, geeignete Schutzmechanismen zu implementieren, wie die Verwendung sicherer Kommunikationskanäle wie Transport Layer Security (TLS) für Daten, die die Vertrauensgrenze der TD verlassen. In Zukunft soll TDX 2.0 eine vertrauenswürdige I/O-Virtualisierung enthalten.

Fazit

Spätestens sobald sich Unternehmen entscheiden, ihre Daten in der Cloud zu verarbeiten, sollten sie die IT-Sicherheit und Vertrauenswürdigkeit von Daten und Code bei der Verarbeitung berücksichtigen. Eine IT-Sicherheitsarchitektur mit Confidential Computing schützt Daten und Anwendungscode über Sicherheitsfunktionen in der CPU in einem Trusted Execution Environment und überprüft per Attestation dessen Vertrauenswürdigkeit. Das stellt sicher, dass nur gewünschte Daten genutzt werden, und das nur von berechtigten Anwendern, dass der richtige Code im TEE ausgeführt wird und niemand von außen kommt an die Daten heran. Daher hilft Confidential Computing, die IT-Sicherheit und Vertrauenswürdigkeit von Cloud-Anwendungen deutlich zu erhöhen und den Datenschutzanforderungen zu genügen. (avr@ix.de)

Quellen

[1] Inés Atug; Streng nach Vorschrift; Maßnahmen zur sicheren Nutzung von Public Clouds; iX 1/2021, S. 88

[2] Weitere Hintergrundinformationen und -artikel: ix.de/zrny

DR. SEBASTIAN GAJEK

ist Professor an der Hochschule Flensburg für IT-Sicherheit und CTO bei der Berliner enclaive GmbH, die Confidential-Cloud-Computing-Technologie auf Open-Source-Basis entwickelt, und forscht seit 2012 im Bereich Confidential Computing.

PROF. DR. NORBERT POHLMANN

ist Professor für Informationssicherheit und Leiter des Instituts für Internet-Sicherheit – if(is), Vorstandsvorsitzender des Bundesverbands IT-Sicherheit TeleTrusT sowie Mitglied im Vorstand des Internetverbands eco.