AKAMAI-LÖSUNGSÜBERBLICK

Confidential Computing: Daten in Verwendung schützen

Trotz der stetigen Steigerung von Reichweite, Umfang und Komplexität heutiger Bedrohungen gelingt es den Sicherheitsteams im Allgemeinen, sich dieser Herausforderung zu stellen – insbesondere bei der Verschlüsselung von Daten während der Übertragung und der Beschränkung des Zugriffs bei der Speicherung. Es wird jedoch immer deutlicher, dass Teams auch Daten schützen müssen, während sie aktiv bearbeitet, gelesen oder verarbeitet werden, was allgemein als *Daten in Verwendung* bezeichnet wird.

Diese Lücke beim Schutz der Daten in Verwendung wird angesichts der Entwicklung der Datenverarbeitung und der zunehmenden Verbreitung von KI immer wichtiger. Die Verbreitung von Hybrid- und Multicloud-Computing hat die Möglichkeiten erweitert, mit denen Unternehmen Daten sammeln und speichern. Unternehmen, die KI nutzen möchten, bewegen riesige Datensätze – oft ihre wertvollsten und sensibelsten Daten – in Verwendung an Orte, wo sie unverschlüsselt und ungeschützt sind.

Diese Risiken wecken das Interesse an Confidential Computing, einem Sicherheitsansatz, der sicherstellt, dass alle sensiblen Daten, die von Anwendungen, Prozessen oder Diensten verwendet werden, verschlüsselt und geschützt bleiben.

APIs erhöhen die Komplexität

APIs verbreiten sich immer mehr, weil sie in zwei Bereichen, in die Unternehmen immer mehr Ressourcen investieren, wichtige Funktionen erfüllen: Cloudumgebungen und -services sowie KI-Modelle. In der Cloud sind APIs unerlässlich, um Technologien die Kommunikation und den Austausch von Daten zu ermöglichen. Im KI-Bereich verwenden große Sprachmodelle (LLMs) APIs für den Zugriff auf und die Kombination von Daten, um komplexe Aufgaben wie Sprachverständnis und Textgenerierung durchzuführen.

Leider erhalten APIs nicht die gleiche Aufmerksamkeit von Sicherheitsteams wie Anwendungen und Infrastruktur. Angreifer nutzen diese Sicherheitslücke aus, und 84 % der Unternehmen wurden in den letzten 12 Monaten Opfer von API-Sicherheitsvorfällen.[1] Um die sensiblen Daten zu schützen, mit der jede ihrer Cloud- und KI-bezogenen APIs in Kontakt kommt, benötigen Unternehmen umfassende API-Sicherheitsfunktionen, die in ihren vertraulichen Computing-Umgebungen ausgeführt werden.

Alle drei Türen verriegeln

Trotz der Sicherung Ihrer Daten bei der Übertragung und Speicherung kann immer noch eine Tür – die der Daten in Verwendung – weit offen bleiben und Unternehmen einem Risiko aussetzen.

Beim Confidential Computing werden diese Daten in einer Umgebung verarbeitet, die auf Hardwareebene als vertrauenswürdig gilt. Mit APIs können Unternehmen ihre eigenen Instanzen für privates maschinelles Lernen bereitstellen, die speziell für die Sicherung des API-Traffics entwickelt wurden, anstatt einen API-Service einer öffentlichen Cloud zu nutzen, wodurch die Angriffsfläche drastisch reduziert wird. Die Ausführung einer API-Sicherheitslösung in einer Confidential Computing-Umgebung schafft eine zusätzliche Sicherheitsebene. Selbst wenn ein Teil des Systems gefährdet ist, bleiben die Daten innerhalb der geschützten Umgebung sicher. Die Ausführung der API-Analyse für diese Daten in einer vertrauenswürdigen Umgebung ist sicherer und beseitigt die Risiken, die in herkömmlichen Umgebungen bestehen.

Diese Kombination aus KI, API-Sicherheit und Confidential Computing hilft dabei, nicht autorisierte Entitäten – wie Hypervisor, Eigentümer der Host-Betreibersysteminfrastruktur oder Personen mit physischem Zugriff – daran zu hindern, Code oder Daten während der

Geschäftliche Vorteile

Verbesserte Datensicherheit
Beschränkung des Zugriffs auf genutzte Daten mit starken Kontrollen, Reduzierung der Angriffsfläche und Schutz sensibler API-gesteuerter Prozesse vor unbefugtem Zugriff

Schutz für APIs
Tiefgreifende Analyse des API-Verkehrs bei gleichzeitiger Verschlüsselung sensibler Daten, um das Risiko einer Aufdeckung während der Überwachung zu verringern

Stärkere Compliance
Einhaltung der ständig aktualisierten und strengen globalen Datenschutzvorschriften, um die Einhaltung von Branchen- und behördlichen Standards zu gewährleisten

1. Akamai, API-Sicherheitsstudie, 2024.

Ausführung anzuzeigen oder zu ändern. Sie schützt so sowohl vor internen Bedrohungen (z. B. bösartigen Systemadministratoren oder Workloads, die auf einer nicht vertrauenswürdigen Infrastruktur laufen) als auch vor externen Bedrohungen (z. B. Angreifern, die Schwachstellen nutzen).

Vorteile

Mit der zunehmenden Verbreitung von API-Bedrohungen und der Tatsache, dass Daten in Verwendung ein attraktives Ziel darstellen, werden Angreifer nicht lange auf sich warten lassen. Zukunftsorientierte Unternehmen beginnen aus einer Reihe von Gründen, Confidential Computing einzusetzen:

- Beschränkung des Zugriffs auf Daten in Verwendung durch strenge Kontrollen
- Sichere Analyse der wachsenden Anzahl von APIs
- Erfüllung neuer und strenger weltweiter Datenschutz-Compliance-Anforderungen mit den Kontrollen, die Confidential Computing verfügbar macht

Vertrauliches Computing hat den größten Vorteil für stark regulierte Unternehmen, sei es ein Finanzdienstleistungsunternehmen, das Online-Transaktionen schützen möchte, oder ein Life-Sciences-Unternehmen, das Patientendaten schützt. Dieser Ansatz kann auch einem unabhängigen Softwareanbieter helfen, ein KI-Modell zu schützen, das an Kunden an mehreren Standorten verteilt wird – von der Edge bis zur Cloud. In der Tat sollte jede IT-Organisation, die Echtzeit-Analysen mit ihren wichtigen Daten durchführt, über Confidential Computing nachdenken.

Wie wir und unsere Partner Sie unterstützen können

Für effektives Confidential Computing ist eine Reihe integrierter Lösungen erforderlich, die eng zusammenarbeiten, um eine umfassende Kontrolle und umfassenden Schutz zu gewährleisten. Akamai bietet gemeinsam mit unseren Partnern Intel und IBM Sicherheit für Daten in Verwendung, und zwar von der Hardware über die Cloud bis hin zu APIs.

Zunächst bieten Intel® Trust Domain Extensions (TDX) vertrauenswürdige Ausführungsumgebungen, die:

- vor Angriffen von außen schützen, die von Bedrohungsakteuren und/oder nicht böswilligen Einheiten stammen, die keinen Zugriff haben sollten,
- die Sicherheit für die Software verbessern, die die Technologie steuert, die für die Erstellung virtueller Ressourcen in der Cloud verwendet wird, z. B. Netzwerke, Server und Speicher,
- für Personen, die diese verteilten Systeme verwalten, eine dringend benötigte Sicherheitsebene hinzufügt, um das Risiko von unbeabsichtigten Fehlern und potenziellen Fällen von-böswilliger Aktivität von innen zu verringern.

Zudem können Unternehmen mit Intel Tiber™ Trust Authority-Verifizierung und Tokens den Zugriff auf unverschlüsselte Daten in Verwendung beschränken und kontrollieren.

Die Lösung Akamai API Security ermöglicht die Bestandsaufnahme aller im Unternehmen verwendeten APIs, die dann überwacht und erkennt, wie diese APIs verwendet werden. Sie erkennt und verhindert automatisch schädliche API-Anfragen durch Analyse von Trafficmustern und -verhalten und blockiert Bedrohungen an der Netzwerk-Edge effektiv und ohne manuelles Eingreifen. Dies ermöglicht Echtzeitschutz vor API-Angriffen wie Datenlecks, unbefugtem Zugriff und Logikmissbrauch.

Die Remote-Engines für maschinelles Lernen von Akamai bieten in Kombination mit Intel Xeon®-Prozessoren auf virtuellen Cloud-Servern von IBM – die wiederum mit Intel TDX abgesichert und mit Intel Tiber Trust Authority zertifiziert sind – eine private, hyperskalierbare Umgebung, die darauf ausgelegt ist, jegliche Bedrohung von außen zu verhindern, wenn die Daten in der Endphase der Nutzung unverschlüsselt sind, sei es durch KI-gestützte Bot-Angriffe oder menschliche Angreifer.

Es ist an der Zeit, Ihre Daten in Verwendung zu schützen

Unternehmen benötigen eine hochgradig vertrauenswürdige Umgebung, um ihre wertvollsten Unternehmensdaten zu schützen – nicht nur, wenn sie gespeichert oder abgerufen werden, sondern auch, wenn sie tatsächlich verwendet werden. Daher wenden sie sich an Akamai und unsere Partner, um umfassende Sicherheit zu erhalten. Gemeinsam sorgen diese vertrauenswürdigen Computing-Unternehmen dafür, dass die Sicherheit während des gesamten Datenlebenszyklus gewährleistet ist.

Erfahren Sie mehr darüber, wie unsere Partnerschaft für Confidential Computing zum Schutz Ihrer vertraulichen Daten beitragen kann.
Erfahren Sie mehr über die Lösung Akamai API Security.