Entschließung

der Konferenz der unabhängigen Datenschutzaufsichtsbehörden

des Bundes und der Länder vom 16. Juni 2025

Confidential Cloud Computing

Der Begriff „Confidential Computing“ bezeichnet nicht eine einzelne Technologie, sondern wird von verschiedenen Anbietern unterschiedlich belegt. So wird beispielsweise eine Verschlüsselung von Daten im Arbeitsspeicher oder aber auch eine reine Zugriffsbeschränkung auf reservierte Speicherbereiche als Confidential Computing bezeichnet. Unter dem Begriff „Confidential Cloud Computing” werden teilweise Technologien damit beworben, dass Daten sogar vor dem Cloud-Betreiber geheim gehalten werden können. Eine solche allgemeine Aussage trägt jedoch nicht der tatsächlichen Komplexität der eingesetzten Technologie Rechnung. Um solche Werbeversprechen kritisch einzuordnen, werden im Nachfolgenden wichtige zu berücksichtigende Punkte angesprochen.

Angreifermodell

Zuerst sollte festgehalten werden, dass die zugrundeliegenden Technologien ursprünglich insbesondere dem Szenario entstammen, in welchem sich mehrere Nutzende die gleiche Hardware bei einem Cloud-Betreiber teilen. In einer solchen Situation soll sichergestellt werden, dass die eigenen Daten vor den Daten anderer Nutzender geheim gehalten werden können, möglicherweise sogar dann, wenn sich ein anderer Nutzender Administrationsrechte verschafft und auf Teile der Cloud-Betriebsinfrastruktur zugreift.

Wenn jedoch die Daten nicht mehr nur vor anderen Nutzenden, sondern vor dem Cloud-Betreiber geheim gehalten werden sollen, erfordert dies ein komplett anderes und viel stärkeres Angreifermodell. Denn der Betreiber hat physikalischen Zugang zu den Systemen und umfangreiche Möglichkeiten, die Hardware und Software zu manipulieren. Für eine valide Bewertung der Wirksamkeit von Maßnahmen ist ein differenziertes Angreifermodell erforderlich, das auch unterschiedlichen Gruppen von Mitarbeitenden des Betreibers und seiner Auftragnehmer berücksichtigt.

Eine Verbesserung der Sicherheit kann sich dadurch ergeben, dass (z. B. mittels Verschlüsselung) Zugriffsmöglichkeiten innerhalb der Organisation des Betreibers (und ggf. seiner Auftragsverarbeiter) eingeschränkt werden. Auch vor einer missbräuchlichen Nutzung (z. B. Start

geklonter virtueller Maschinen oder Container) oder Manipulation gibt es einen gewissen Schutz.

Solche Maßnahmen gehören aber nicht im engeren Sinne zum „Confidential Computing“: Sie ändern nichts an der Tatsache, dass der Betreiber grundsätzliche Zugriff auf die Daten hat bzw. sich verschaffen kann. Die teilweise anzutreffende Behauptung, dass die Kontrolle über die Datenverarbeitung vollständig auf den Nutzenden übergehe, ist nicht haltbar. So ist es beispielsweise offensichtlich, dass die Kontrolle über die Verfügbarkeit der Datenverarbeitung auch beim Cloud-Betreiber liegt. Auch ist es offensichtlich nicht möglich, jede unrechtmäßige Datenverarbeitung im Cloud-Kontext zu verhindern, beispielsweise eine unrechtmäßige Löschung.

Schlüsselmanagement

Eine besondere Bedeutung kommt dem eingesetzten Schlüsselmanagement zu. Tatsächliche Geheimhaltung vor dem Cloud-Betreiber (als Organisation) ist nur gewährleistet, wenn die Daten zu jedem Zeitpunkt so verschlüsselt sind, dass der Cloud-Betreiber den zur Entschlüsselung notwendigen Schlüssel nicht in Erfahrung bringen oder nutzen kann. Vor dem Hintergrund des oben angesprochenen sehr starken Angreifermodells eines „bösartigen Cloud-Betreibers“ müssen hierbei auch Analysen und Manipulationen von Hardware und Software berücksichtigt werden. Das bedeutet auch, dass der Cloud-Betreiber nachweisen muss, dass er zu keinem Zeitpunkt die Möglichkeit hat, die Verschlüsselung zu manipulieren (z. B. durch Machine-in-the-Middle-Angriffe oder den Austausch eines Nutzenden-Schlüssels durch einen selbst gewählten Schlüssel).

Nicht in allen Fällen ist für die Nutzenden klar überprüfbar, ob Confidential Computing überhaupt eingesetzt wird. Zwar ist es je nach Technologie möglich, dass über auf der Hardware hinterlegte Zertifikate attestiert wird, dass eine Operation in einer vertraulichen Umgebung ausgeführt wird. Um diese Attestierung aber an die Nutzenden durchreichen zu können und somit überprüfbar zu machen, muss die jeweilige Anwendung i.d.R. speziell dafür implementiert werden.

Ein besonderes Augenmerk sollte hier auf die Übergänge zwischen den verschiedenen „Verschlüsselungsdomänen“ gelegt werden, etwa der Übergang von „data-at-rest“ zu „data-in-use“. Wenn bei solchen Übergängen ein Wechsel der eingesetzten Schlüssel vorgenommen wird, und zu diesem Zweck eine kurzzeitige Entschlüsselung der Daten stattfindet, liegen die Daten möglicherweise kurzzeitig in unverschlüsselter Form vor.

Um die Aussagen der Cloud-Betreiber sowie der Hersteller der eingesetzten Hard- und Software (z. B. Hersteller von Chips, Firmware, Virtualisierungssoftware etc.) einordnen zu können, müssen Einsatzszenarien transparent sein. Ebenso müssen die der Sicherheitsanalyse zugrundeliegenden Annahmen offen kommuniziert werden. Eine typische Annahme ist, dass es keine physikalischen Angriffe (z. B. Seitenkanalattacken) gibt. Unter dieser Annahme kann diese Technik einen hohen Mehrwehrt an Sicherheit und Datenschutz bieten. Ist hingegen die Annahme nicht zutreffend (etwa, weil der Cloud-Betreiber einem Dritten physikalischen Zugang zur Hardware ermöglichen oder Schlüssel bzw. Zertifikate auf Hardware herausgeben

oder austauschen muss) oder vertraut man Zusagen von Herstellern oder Betreibern nicht, so hat diese Technik nicht den versprochenen Effekt.

Als Fazit kann „Confidential Cloud Computing“ das allgemeine Sicherheitsniveau erhöhen und typischerweise einen wertvollen Schutz gegen andere Nutzende auf der gleichen Hardware und gegen einzelne Innentäter bieten – letztlich eine weitere Schicht eines „defense-in-depth“-Ansatzes. Der Einsatz sollte daher empfohlen werden, auch wenn nicht alle Datenschutzprobleme so einfach gelöst werden, wie es teilweise beworben wird: Absolute Vertraulichkeit ist nicht möglich und grundsätzlich ist davon auszugehen, dass ein Cloud-Betreiber Zugriffsmöglichkeiten auf die zu schützenden Daten besitzt. Für eindeutig formulierte Angreifermodelle können jedoch konkretere Aussagen getroffen werden. Die Aussagen, mit denen diese Technologie beworben wird, sind daher im Hinblick auf das differenzierte Angreifermodell kritisch zu hinterfragen und die Schlussfolgerungen und die sich aus dem Angebot ergebenden bzw. zusätzlich zu ergreifenden Maßnahmen aus Gründen der Nachweis- und Rechenschaftspflicht nachvollziehbar dokumentieren.