Datenweitergabe nach E-Evidence vs Confidential Computing: Werden ganze Berufsgruppen von der Cloud-Nutzung ausgeschlossen?

16.12.2020 – München: Mit E-Evidence schickt sich ein neues, internationales Regelwerk an, Daten über Landesgrenzen hinweg für Behörden verfügbar zu machen[1]. Fordert beispielsweise die Justizbehörde in Griechenland die Nutzerdaten eines deutschen Kunden an, so soll es zukünftig möglich sein, den deutschen Cloud-Anbieter zur Herausgabe dieser Daten zwingen zu können. Davon betroffen sind alle Informationen, die dem Cloud-Dienstleister über seinen Kunden zur Verfügung stehen: Angefangen von den gespeicherten Inhalten bis hin zu den Metadaten bezüglich des Zeitpunkts der Datenübertragung, IP-Adresse des Absenders sowie den Empfänger der Datenpakete.

Dieser Entwurf mag für eine effektive internationale Strafverfolgung hilfreich sein – doch die Forderung wirft grundsätzliche Fragen zur Datensicherheit von Cloud-Diensten auf.

Cloud-Anbieter können auf Kundendaten zugreifen

Denn technisch ist der Zugriff auf Nutzerdaten – Inhaltsdaten sowie Metadaten – durch den Anbieter prinzipiell möglich! Viele Anbieter von Cloud-Diensten können auf die in der Cloud gespeicherten Daten ihrer Kunden zugreifen. Das bedeutet, dieser Zugriff kann grundsätzlich auch ohne behördliche Anordnung erfolgen. Gerade, wenn Unternehmen mit sensiblen Daten hantieren, ist das eine unangenehme Vorstellung. Wenn der Cloud-Betreiber jederzeit auf die Daten seiner Kunden zugreifen kann – wer kann das dann noch alles?

Die Möglichkeit zur Kenntnisnahme stellt für manche Berufsgruppen (Träger von Berufsgeheimnissen nach §203 StGB, wie z.B. Anwälte und Ärzte) sogar eine Offenbarung von Geheimnissen im Sinne des StGB dar. „So schließt man mit der Forderung nach der Möglichkeit des behördlichen Zugriffs gewisse Berufsgruppen von vornherein von der Nutzung von Cloud-Diensten aus und setzt sie den wirtschaftlichen Nachteilen aus, die sich daraus ergeben“, argumentiert Ulrich Ganz, Director Software Engineering bei der Münchner TÜV SÜD-Tochter uniscon.

Confidential Computing: Technologie vs Anordnung

Unternehmen, die Zugriffe durch Dritte – auch durch den Dienstbetreiber – zuverlässig verhindern wollen, setzen bereits jetzt auf Dienste, die das Prinzip des Confidential Computing umsetzen[2]. Dabei werden sensible Daten nicht nur bei der Speicherung und Übertragung verschlüsselt, sondern bleiben auch während der Verarbeitung geschützt. Ziel des Confidential Computing ist neben einer allgemeinen Verbesserung der Datensicherheit auch, die Vorteile des Cloud Computing auch denjenigen Branchen zugänglich zu machen, die schützenswerte Daten verarbeiten.

Bei uniscons hochsicherer Business-Cloud idgard® wird der Confidential-Computing-Ansatz durch die Sealed-Cloud-Technologie[3] realisiert. Hier schließen eine gründliche Datenverschlüsselung und ein Satz ineinander verzahnter technischer Maßnahmen in speziell abgeschirmten Server-Käfigen jeglichen unbefugten Zugriff zuverlässig aus. Nur der Kunde ist im Besitz des dazugehörigen Schlüssels.

[1] https://www.europarl.europa.eu/news/en/press-room/20201207IPR93219/meps-want-legally-sound-solutions-for-obtaining-e-evidence-in-cross-border-cases
[2] https://www.idgard.de/privacyblog/confidential-computing-und-sealed-cloud
[3] https://de.wikipedia.org/wiki/Sealed_Cloud

Eine Anfrage von Dritten nach Zugriff auf diese Daten ist somit zwecklos, da auch der Betreiber keinen Zugang dazu hat. Diese Technologie erlaubt somit Berufsgruppen die Nutzung von Cloud-Diensten, die sonst davon ausgenommen wären, etwa Ärzte und Kliniken, aber auch Steuerberater, Wirtschaftsprüfer und viele mehr.

Es ist wichtig, dass gesetzgeberische Maßnahmen nicht mehr Schaden anrichten, als sie Nutzen generieren. Eine grenzübergreifende Auslieferung von Daten ist daher mit großer Skepsis zu betrachten und sollte auf keinen Fall überstürzt verabschiedet werden.

Weitere Beiträge rund um die Themen Datenschutz und Datensicherheit finden Sie unter www.privacyblog.de.

uniscon – Ein Unternehmen der TÜV SÜD Gruppe

Die uniscon GmbH ist ein Münchner Anbieter von DSGVO-konformen Cloud- und Datenraum-Lösungen für Unternehmen und einer der führenden Secure-Cloud-Provider in Europa. Die Produkte von uniscon greifen Hand in Hand: uniscons *Sealed Platform®* bietet eine sichere Ausführungsumgebung für Webanwendungen mit hohem Sicherheitsbedarf bzw. hohen Datenschutzanforderungen.

uniscons Business-Cloud *idgard®* sichert die digitale Kommunikation und den Datenaustausch mit Partnern, Kunden und Kollegen auf höchstem Niveau ab und vereinfacht sie darüber hinaus. Mehr als 1.200 Unternehmen vertrauen bereits auf den webbasierten Datenraum- und Filesharing-Dienst, darunter IT- und Kommunikationsanbieter (z.B. T-Systems), Unternehmensberatungen (u.a. PwC, Baker Tilly) sowie diverse Anbieter von Finanzdienstleistungen (z.B. Sparkassen und Volksbanken).

Was uniscons Lösung gemeinsam haben? Sie basieren alle auf der international patentierten *Sealed Cloud Technologie*, welche mit rein technischen Maßnahmen unbefugte Datenzugriffe ausschließt. Die Lösungen werden alle nach dem Grundsatz „Privacy by Design“ entwickelt.

Uniscon wurde 2009 gegründet und ist seit 2018 Teil der Digitalisierungsstrategie von TÜV SÜD. TÜV SÜD ist ein weltweit führendes technisches Dienstleistungsunternehmen mit über 150 Jahren branchenspezifischer Erfahrung und heute mehr als 24.000 Mitarbeitern an etwa 1000 Standorten in 54 Ländern. In diesem starken Verbund kann uniscon die Entwicklung seiner Technologie weiter vorantreiben und ist in der Lage, mit der Sealed Cloud und ihren Produkten internationale Großprojekte in den Bereichen IoT und Industrie 4.0 zuverlässig zu realisieren.

Weitere Informationen zum Unternehmen und den Lösungen: www.idgard.de und www.uniscon.com

Pressekontakt
uniscon GmbH, Wilhelm Würmseer
Ridlerstr. 57
80339 München
E-Mail: press@uniscon.com
Telefon: 089 / 41 615 988 104

Kafka Kommunikation GmbH & Co KG, Markus Reck
Auf der Eierwiese 1
82031 Grünwald
Tel. +49 (0) 89 74747058-0
Fax + 49 (0) 89 74747058-20