Datenaustausch ist nicht gleich Datenaustausch – Wie man das geeignete Werkzeug für die jeweilige Anforderung findet

München, 15.07.2021 – Mit fortschreitender Digitalisierung, die durch die Effekte der Pandemie zusätzliche Beschleunigung erfahren hat, verspüren Unternehmen immer stärkeren Druck, ihre Daten und Arbeitsprozesse in die Cloud zu migrieren. Viele davon, vor allem mittelständische Betriebe, hängen jedoch an ihren traditionellen On-Premise-Konstrukten mit eigenen Servern vor Ort. Sie fürchten um die Sicherheit ihrer Daten und scheuen sich, diese in fremde Hände zu geben.

Neben Mittelständlern sind es vor allem streng regulierte Branchen wie Rechtsvertretung, Consulting oder Finanzwesen, die Bedenken wegen der Integrität und Geheimhaltung ihrer Daten in der Cloud haben[1]. Denn Sie unterliegen besonders strengen Vorschriften. Die Anforderungen an den Datenschutz in diesen Geschäftsfeldern gehen über die der DSGVO weit hinaus. Public-Cloud-Dienste sind einfach und praktisch für den Austausch von Dateien, bietet aber nicht für jede Art von Daten das erforderliche Schutzniveau und können sogar Compliance-Richtlinien verletzen. Müssen Rechtsanwälte, Berater oder Finanzdienstleister also auf die Vorzüge der Cloud verzichten, um sich nicht in Rechtsunsicherheit zu begeben?

Datenräume bieten eine revisionssichere Alternative für sensible Daten

Um das Nutzererlebnis für jedermann so intuitiv wie möglich zu gestalten, sind Web-Dienste (SaaS) in der Regel oft mit dem nötigen Minimum an Sicherheitsbarrieren vorkonfiguriert. Für die private Anwendung sehen die meisten Nutzer dies oftmals als ausreichend an.

Anders stellt sich die Sachlage jedoch bei der Arbeit mit digitalen Dokumenten im beruflichen Kontext dar. Wer besonders schützenswerte Daten – etwa mit Personenbezug oder Firmengeheimnissen – versendet oder verarbeitet, muss gegebenenfalls weitere Anforderungen beachten:

- Gibt es eine interne Klassifizierungsrichtlinie für Daten?
- Liegt ein Personenbezug vor?
- Muss sichergestellt sein, dass Dokumente nur von einem bestimmten Personenkreis empfangen werden können?
- Liegt eine Notwendigkeit für weiteren Verbreitungsschutz vor? Dürfen Dokumente beispielsweise nur gesichtet, aber nicht bearbeitet werden?
- Müssen Zugriffe minutiös und revisionssicher protokolliert werden?

Je nach Bedarfsfall reichen Filesharing-Dienste hier nicht aus. Anders verhält es sich hingegen mit virtuellen Projekt- und Datenräumen. Diese bieten nicht nur nötige Funktionen wie Zugangsbeschränkungen, Verbreitungsschutz und Protokolle, sondern auch das Sicherheitsniveau, das Secure Content Collaboration – also den sicheren Austausch und die gemeinsame Nutzung sensibler Dokumente – möglich macht. Das ist wichtig, um gesetzliche Datenschutz-Vorgaben erfüllen zu können und zusätzlich strengen und oft branchenspezifischen Compliance-Anforderungen zu entsprechen.

Datenschutz dank Confidential Computing

Das notwendige Schutzniveau im virtuellen Datenraum lässt sich am besten mit einem Confidential Computing-Ansatz erreichen[2]. Diese spezielle Technologie ermöglicht es Unternehmen, ihre Daten verschlüsselt zu speichern und zu übertragen sowie sie versiegelt zu verarbeiten. Dafür sorgt eine spezielle Sicherheitsarchitektur mit reduzierten Schnittstellen und mehreren ineinander verzahnten technischen Schutzmaßahmen. Weder Außenstehende noch der Cloud-Betreiber haben Zugriff auf die

[1] https://netzpalaver.de/2021/05/10/sturm-auf-idgard-co-unternehmen-erobern-die-cloud/
[2] https://www.idgard.de/privacyblog/confidential-computing-und-sealed-cloud

so gesicherten Datenräume. Den Schlüssel zu den Daten besitzt einzig und allein der Datenraum-Kunde. Durch die Vorzüge des Confidential Computing lassen sich unberechtigte Zugriffe dritter (einschließlich des Providers) zuverlässig verhindern und somit selbst strengste Datenschutz-Regularien einhalten. Darüber hinaus werden durch diese Technologie auch Metadaten zuverlässig geschützt.

„Vielen Vertretern besonders streng regulierter Branchen, wie etwa Rechtsanwälten oder Finanzdienstleistern, sollte es um mehr gehen als nur darum, die DSGVO-Latte nachweislich nicht zu reißen und mögliche horrende Strafzahlungen zu vermeiden." sagt dazu Jörg Horn, Chief Product Officer der Münchner TÜV SÜD-Tochter uniscon. „Sie wollen ihren Klienten den bestmöglichen Datenschutz bieten, ohne dabei auf die Vorzüge der digitalen Zusammenarbeit verzichten zu müssen."

Fazit:

Filesharing-Dienste aus der Public Cloud und hochsichere Datenräume erfüllen ihre spezifischen Rollen für den jeweiligen Anwendungsfall und werden auch in Zukunft nebeneinander koexistieren. Nutzer – und ganz besonders Unternehmen – sollten vor einer Migration ihrer Daten in die Cloud genau abwägen, welche Lösung für sie die richtige ist. Für den digitalen Austausch von unkritischen Daten können auch weiterhin Public-Cloud-Dienste genutzt werden. Personenbezogene Daten sowie Firmengeheimnisse erhalten den notwendigen Schutz jedoch nur in hochsicheren Datenräumen, die durch Confidential Computing jeglichem unberechtigten Fremdzugriff sowie dem Missbrauch von Privilegien einen Riegel vorschieben.

Wurde Ihnen diese Pressemeldung weitergeleitet? Hier können Sie sich zu unserem Presseverteiler anmelden. Aktuelle Artikel zu den Themen Datenschutz und Datensicherheit finden Sie im privacyblog.

uniscon – A member of TÜV SÜD

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 2017 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