ALTHAMMER & KILL

PRESSEMITTEILUNG

Datenschutz: Umstellung auf Microsoft 365

Die wichtigsten Schritte, um Ihre Daten in der Cloud zu schützen

Hannover, 13. August 2020. Cloud-Computing ist für Unternehmen und Privatkunden eine der relevantesten Zukunftstechnologien. Jederzeitige Verfügbarkeit von überall auf der Welt, dynamische Ressourcenverwaltung und stets aktuelle Software. Für Datenschützer dagegen ist es ein Problemfall. Vor- und Nachteile der Umstellung auf Cloud-Lösungen wie Microsoft 365 müssen erwogen und Risiken minimiert werden, teilte das auf Datenschutz, Informationssicherheit und IT- Compliance spezialisierte Unternehmen Althammer & Kill mit.

Dem Online-Analysten StatCounter zufolge ist Microsoft mit seinen Betriebssystemen mit mehr als 77 Prozent Marktanteil führend in Deutschland. Ältere Betriebssysteme des US-Anbieters werden künftig nach und nach aus der Wartung fallen. Das heißt, der Umzug in die Wolke wird einen großen Teil der privaten Nutzer und Unternehmen in Deutschland betreffen. Die gängigen Microsoft Software-Anwendungen, wie Excel, Outlook und Word werden dann nicht mehr zwingend lokal auf dem Computer des Benutzers betrieben, sondern online (as-a-service-Anwendung). Standardmäßig erfolgt die Programmnutzung nunmehr auf Microsoft-Servern und der Zugriff des Endbenutzers erfolgt lediglich über das Internet. „Bei der Migration von Daten in eine Cloud lauern einige Gefahren. Diese muss man genau bewerten“, sagt Thomas Althammer, Geschäftsführer von Althammer & Kill. „IT-Verantwortliche in Unternehmen, aber auch Verbraucher müssen Vorkehrungen treffen, um die Vertraulichkeit, Verfügbarkeit und Integrität der eigenen Informationen und personenbezogenen Daten zu gewährleisten.“ Denn bei Verstößen haftet am Ende meist derjenige, der die kritischen Daten in der Cloud gespeichert hat.

Wie gelingt die datenschutzkonforme Cloud-Migration?

Der größte Vorteil des Arbeitens in der Cloud birgt auch das größte Risiko: die ständige Verfügbarkeit der Daten von überall auf der Welt.
Es gibt aber technische und organisatorische Möglichkeiten, die einzelnen Verarbeitungsvorgänge auf das Nötigste zu begrenzen:

- Option „Telemetrie- und Diagnosedaten an Microsoft senden“ auf das Nötigste beschränken.
- So weit wie möglich lokal installierte Versionen der Microsoft-Software nutzen.
- SharePoint Online/OneDrive nur nach intensiver Auseinandersetzung mit den datenschutzrechtlichen Vorgaben nutzen. Besonders schützenswerte Daten gesondert behandeln.
- An einigen Arbeitsplätzen datenschutzfreundliche Software, wie Open Office installieren und besonders kritische Informationen nur dort verarbeiten.
- Benutzung von microsofteigenen und verbundenen Diensten (zum Beispiel Cortana oder Übersetzungsvorschläge) zentral ausschalten bzw. Nutzerprofile anpassen.

Zu jedem Zeitpunkt bleibt die Pflicht des Verantwortlichen bestehen, für eine rechtmäßige Verarbeitung von personenbezogenen Daten in Microsoft 365 oder anderen Cloud-Angeboten Sorge zu tragen.

Risiken des Cloud-Computings aus Datenschutzsicht

Beim Cloud-Computing werden im Auftrag des Verantwortlichen eigene Daten auf IT-Systemen externer Dienstleister verarbeitet (zum Beispiel Microsoft sowie weiteren Subunternehmen). Das nennt man Auftragsverarbeitung. Dafür gelten in der Europäischen Union die strengen gesetzlichen Regeln der Datenschutzgrundverordnung (DSGVO Artikel 28 und 32).

Unternehmen müssen den beauftragten Dienstleister hinsichtlich der eingesetzten technisch-organisatorischen Maßnahmen regelmäßig überprüfen.

In der Praxis können unabhängige Sicherheits-Zertifizierungen teilweise als Ersatz für persönliche Kontrollen herangezogen werden, zum Beispiel gemäß ISO 27001.

Ein zusätzliches Problem stellt der Auslandsbezug dar. Denn oft werden beim Cloud-Computing Rechenzentren auf der ganzen Welt verwendet, von denen der Kunde letztendlich nicht einmal den Standort weiß. Auch der Zugriff eines Microsoft-Mitarbeiters im Rahmen des Kunden-Supports stellt einen Auslandsbezug dar (beispielsweise Support durch Subunternehmer aus Indien).

Die datenschutzrechtlichen Voraussetzungen der Auftragsverarbeitung inkl. Auslandsbezug werden durch Microsoft zwar vertraglich zugesichert, der Auftraggeber wird dadurch allerdings nicht von einer schutzbedarfsorientierten Risikoanalyse bezüglich der konkreten Verarbeitung von personenbezogenen Daten (Gesundheitsdaten und andere) in der Cloud befreit.

Europäischer Gerichtshof kippt Datentransfer in die USA

Gängige Grundlagen der Datenübermittlung in die USA waren bisher das EU-US Privacy Shield sowie die EU-Standardvertragsklauseln. Im Juli 2020 hat der Europäische Gerichtshof (EuGH) das EU-US Privacy Shield für ungültig erklärt. Im selben Zuge wurden die EU-Standardvertragsklauseln unter Vorbehalt für weiterhin gültig erklärt. Der strenge europäischer Datenschutz erlaubt die Übermittlung von personenbezogenen Daten in Drittstaaten außerhalb der Europäischen Union nur, wenn dort ein gleichwertiges Schutzniveau sichergestellt ist, wie in der EU. Dies sah der EuGH in den USA als nicht gegeben an. Da aufgrund dessen die Gültigkeit der EU-Standardvertragsklauseln mit US-amerikanischen Unternehmen in Frage gestellt wird, bedarf es einer neuen Vereinbarung zwischen der EU und den USA.
Speicherort der Microsoft-Cloud-Dateien sind unter anderem zwar Server in Deutschland und der EU, allerdings können US-Behörden aufgrund des sogenannten CLOUD Acts darauf gegebenenfalls Zugriff nehmen. Dies ist einer der Gründe, wieso der EuGH ein angemessenes Schutzniveau in den USA nicht anerkannt hat.

Web-Seminar vom 9. bis 10. September 2020

Für Unternehmen (Datenschutzbeauftragte, IT-Verantwortliche und Management) vertieft Althammer & Kill das Thema in einem Web-Seminar, stellt Vor- und Nachteile des Cloud-Computings vor und erläutert, wie Risiken minimiert werden können.

Die dargestellten Herausforderungen des Cloud-Computings betreffen auch andere Anbieter, wurden aber hier am Beispiel von Microsoft als Marktführer in Deutschland aufgezeigt.

Über Althammer & Kill:

Die Althammer & Kill GmbH & Co. KG hat sich als Beratungsunternehmen auf die Themen Datenschutz, Informationssicherheit und IT-Compliance spezialisiert. Zum 30-köpfigen Team gehören Juristen, IT-Berater, zertifizierte Datenschutzbeauftragte und IT-Sicherheitsspezialisten. Das Unternehmen ist von den Standorten Hannover, Düsseldorf und Mannheim aus bundesweit tätig, z. B. in der Funktion als externe Datenschutzbeauftragte oder Informationssicherheitsbeauftragte. Zu den weiteren Angeboten zählen die Bereiche Zertifizierung und die Durchführung von IT-Sicherheitsanalysen/Penetrationstests.

Kontakt:

Susanne Maack
Pressereferentin

Mail: sm@althammer-kill.de
Mobil: 0170 933 17 52

Althammer & Kill GmbH & Co. KG
Roscherstraße 7
30161 Hannover