Die dunkle Seite der Cloud: Datenschutzrisiken beim Einsatz von Microsoft 365?

In der öffentlichen Diskussion werden widersprüchliche Standpunkte hinsichtlich des Datenschutzes bei Microsoft 365 (siehe Infokasten) diskutiert. Während einige Experten die Plattform loben und als sichere Lösung empfehlen, gibt es andere Stimmen, die Risiken für den Datenschutz befürchten. Der vorliegende Artikel informiert über den aktuellen Stand und zeigt grundlegende Anforderungen auf, die bei der Implementierung zu beachten sind.

Cloud Technology: Elevating efficiency and teamwork

In Anbetracht der sich stetig wandelnden Anforderungen der modernen Arbeitswelt müssen sich Unternehmen frühzeitig mit neuen Technologien auseinandersetzen. In diesem Kontext hat sich Microsoft 365 als eine der führenden Lösungen für Unternehmen etabliert, die bestrebt sind, ihren Mitarbeitenden moderne Arbeitsmittel zur Verfügung zu stellen, um Arbeitsabläufe effizient und sicher zu gestalten und die Kollaboration zu optimieren. Dabei bietet Microsoft 365 innovative Technologien (wie etwa die Integration von KI-Funktionen für Office-Anwendungen), die es Unternehmen ermöglichen sollen, den Herausforderungen einer sich schnell verändernden Geschäftswelt standzuhalten und zugleich die Produktivität und Effizienz ihrer Arbeitsprozesse zu steigern.

Durch die Adaption innovativer Technologien können sich jedoch auch neue Gefahrenpotenziale manifestieren. Risiken aus den Bereichen Datenschutz und Informationssicherheit sind daher frühzeitig zu identifizieren, zu bewerten und mittels geeigneter Maßnahmen zu minimieren oder zu beseitigen.

Was die Datenschutzkonferenz kritisiert

Im Rahmen der Risikoermittlung wird man sich vernünftigerweise auch mit den Verlautbarungen der zuständigen Aufsichtsbehörden auseinandersetzen.

Die Datenschutzkonferenz (DSK), das gemeinsame Gremium der Aufsichtsbehörden, hat hierzu im November des vergangenen Jahres einstimmig beschlossen, dass der Nachweis von Verantwortlichen, Microsoft 365 datenschutzkonform zu betreiben, auf der Grundlage des von Microsoft bereitgestellten Data Protection Addendum (DPA) nicht geführt werden kann.

Prüfungsgegenstand waren weder das Unternehmen Microsoft noch dessen Produkte oder Dienstleistungen. Vielmehr wurde lediglich das für die zahlreichen Services zugrundeliegende DPA (der Auftragsverarbeitungsvertrag) begutachtet. Die Beanstandungen betreffen im Einzelnen:

- die unzureichende Festlegung von Arten und Zwecken der verarbeiteten Daten,
- Intransparenz in Bezug auf die Datenverarbeitungen, die Microsoft für eigene Geschäftszwecke vornimmt,
- Ausnahmen bei der Weisungsbindung aufgrund des Cloud Act und FISA 702,
- Sicherheitsmaßnahmen, die nur eine Teilmenge der vertragsgegenständlichen personenbezogenen Daten erfassen,
- Intransparenz und Ausnahmen bei der Löschung und Rückgabe von Daten,
- unzureichende Informationen bei der Einschaltung von Unterauftragnehmern und schließlich
- Datenübermittlungen in Drittstaaten (hier die USA).

Obwohl die genannten Kritikpunkte auf den ersten Blick gültig erscheinen, sollte nicht übersehen werden, dass es sich bei Microsoft 365 um hochkomplexe Dienste und Services eines global agierenden Hyperscale-Anbieters handelt. Es ist anzuerkennen, dass Verträge für komplexe Services nicht den gleichen Detaillierungsgrad aufweisen können wie beispielsweise ein trivialer Auftrag zum Druck von Visitenkarten.

Microsoft bietet ergänzend unzählige Produktinformationen, die zwar nicht Vertragsbestandteil sind, aber für weitreichende Transparenz sorgen. Unter Berücksichtigung dieser Umstände sowie der Tatsache, dass keine perfekten Verträge existieren, kann die Auffassung vertreten werden, dass die meisten der oben genannten Beanstandungen nicht angemessen sind und damit auch die Schlussfolgerung der Datenschutzkonferenz überzogen ist.

Wie Microsoft reagiert

Eine ausführliche Stellungnahme von Microsoft auf den DSK-Beschluss, in der die Kritik zurückgewiesen wurde, ließ nicht lange auf sich warten. Dem Verfasser der Stellungnahme ist es jedoch nicht gelungen, die Zweifel vollständig auszuräumen. Vermutlich wurden aus diesem Grund auch die vertraglichen Grundlagen ein weiteres Mal überarbeitet. Im Januar 2023 wurde eine angepasste Fassung des Data Protection Addendum veröffentlicht. Es handelt sich hierbei bereits um die 7. Anpassung in den zurückliegenden 36 Monaten. Ein Blick in den neuen Vertrag zeigt zwar einige Änderungen im Vergleich zur Vorversion aus September 2022, die von der DSK monierten Klauseln des Vertrags wurden jedoch entweder gar nicht oder nur unwesentlich abgeändert.

Daher ist das gelegentlich vorgebrachte Argument, der DSK-Beschluss sei allein aufgrund des neuen DPA hinfällig, als unhaltbar anzusehen. Bei vernünftiger Betrachtung bleiben die (überzogenen) Beanstandungen im Wesentlichen aktuell.

Quick Info: Microsoft 365

Microsoft 365 ist ein Abonnementdienst, der eine Vielzahl von Anwendungen (z. B. Word, Excel, PowerPoint, Outlook) und Diensten (u. a. OneDrive, SharePoint und Teams) umfasst. Es ist als Software-as-a-Service (SaaS) konzipiert, was bedeutet, dass die Programme, Anwendungen und Daten nicht auf unternehmenseigenen Geräten installiert und verarbeitet werden müssen. Stattdessen werden sie auf weltweit verteilten Microsoft-Servern gehostet, die über das Internet zugänglich sind. Dadurch können Benutzer von verschiedenen Geräten aus auf dieselben Anwendungen und Daten zugreifen, ohne dass sie physisch auf ihrem Computer installiert sein müssen.

Bedenkenlose Datentransfers in die USA bald möglich?

Trotz aller Entwicklungen und Maßnahmen werden im Rahmen der Nutzung von Microsoft 365 auch zukünftig bestimmte personenbezogene Daten in die USA übermittelt werden. Dies gilt selbst für den Fall der vollständigen Implementierung der EU Data Boundary (dazu sogleich).

Dies ist jedoch nur unter der Voraussetzung zulässig, dass das durch die DSGVO gewährleistete Schutzniveau in den USA nicht untergraben wird. Gegenwärtig versucht man dies im Wege der Nutzung sogenannter Standard Contractual Clauses (SCC) zu erreichen. Dabei besteht jedoch die Herausforderung, dass dieses Übermittlungsinstrument nur in Verbindung mit ergänzenden Maßnahmen wirksam ist, mit deren Hilfe die Rechtsschutzlücken im Drittland geschlossen werden können und die Einhaltung des unionsrechtlichen Schutzniveaus gewährleistet werden kann.

Entsprechende Maßnahmen sind nach Ansicht der DSK beim Einsatz von Microsoft 365 jedoch nicht verfügbar. Zwar bestehen hier verschiedene Möglichkeiten der Verschlüsselung, dabei ist jedoch Microsoft entweder selbst im Besitz des Verschlüsselungsschlüssels oder die Verschlüsselung ist (wie beispielsweise bei Nutzung des „Customer Key“) auf „Data at rest“ beschränkt. Viele der in Microsoft 365 enthaltenen Dienste erfordern zudem einen Zugriff von Microsoft auf die unverschlüsselten, nicht pseudonymisierten Daten, beispielsweise wenn die Daten im Browser angezeigt werden müssen. Microsoft hat somit regelmäßig und letztlich schon zur Erfüllung vertraglicher Leistungspflichten die Möglichkeit, Daten im Klartext zu lesen.

Abhilfe soll hier ein neuer Angemessenheitsbeschluss der EU-Kommission schaffen. Dabei handelt es sich um ein weiteres Instrument, welches die Bewertung und Anerkennung des Datenschutzniveaus in Drittstaaten ermöglicht. Durch einen Angemessenheitsbeschluss wird bestätigt, dass ein Nicht-EU-Land einen adäquaten Schutz von personenbezogenen Daten gewährleistet, wodurch Datenübermittlungen ohne ergänzende Schutzmechanismen erfolgen können. Dies trägt zur Vereinfachung und rechtlichen Absicherung des grenzüberschreitenden Datenaustauschs zwischen der EU und den betreffenden Ländern bei.

Angemessenheitsbeschlüsse bestehen für mehrere Länder (u. a. für Kanada, die Schweiz und Südkorea). Für die Übermittlung in die USA existierten in der Vergangenheit ebenfalls bereits Angemessenheitsbeschlüsse. Von 2000 bis 2015 durften Datenübermittlungen auf der Grundlage des Safe-Harbor-Abkommens erfolgen. Nachdem der Europäische Gerichtshof (EuGH) dieses für ungültig erklärte, wurde Mitte 2016 ein Nachfolger, das EU-US Privacy Shield, erlassen. Jedoch wurde auch dieser Angemessenheitsbeschluss vom EuGH für ungültig erklärt. Er begründete dies in seinem Urteil vom 16. Juli 2020 u. a. mit einer unverhältnismäßigen Überwachung durch US-Geheimdienste und einem unzureichenden Rechtschutzfür EU-Bürger gegenüber US-Geheimdiensten.

Im März 2022 gab die EU-Kommission schließlich bekannt, dass man sich mit den USA auf ein neues Abkommen geeinigt habe. Ein halbes Jahr später, am 7. Oktober, wurde diese grundsätzliche Einigung durch eine Verfügung des US-Präsidenten („Executive Order on Enhancing Safeguards for United States Signal Intelligence Activities“) in US-Recht umgesetzt. Sie richtet sich an die Intelligence Community, also an alle 18 US-Geheimdienste, und sieht u. a. die Einführung eines Verhältnismäßigkeitsgrundsatzes sowie weiterer Rechtsbehelfsmechanismen vor (so z. B. die Möglichkeit, Entscheidungen des Civil Liberties Protection Officer vor dem Data Protection Review Court anzufechten).

Der Europäische Datenschutzausschuss (EDSA) begrüßt die Verbesserungen, äußert in seiner Stellungnahme vom 28. Februar 2023 jedoch auch einige Bedenken.

Der neue Angemessenheitsbeschluss, auch als Privacy Framework bezeichnet, dürfte den aktuellen Prognosen zufolge dennoch etwa Mitte des Jahres 2023 wirksam werden. Allerdings erscheint der künftige Gang zum Europäischen Gerichtshof (EuGH) als vorhersehbarer Verlauf.

Für den Fall, dass kein Angemessenheitsbeschluss zustande kommen sollte oder dieser vor dem EuGH erneut für ungültig erklärt wird, will Microsoft mit der sogenannten EU Data Boundary aber bereits Vorsorge treffen. Danach soll bis 2024 sichergestellt werden, dass grundsätzlich alle personenbezogenen Daten in europäischen Rechenzentren verarbeitet werden. Bei der Bewertung der Wirksamkeit dieser Strategie sind jedoch etwaige extraterritorial wirkende Rechtsvorschriften (wie der US-CLOUD-Act) zu berücksichtigen.

Risikobeurteilung und -behandlung

Die Diskussionen rund um den DSK-Beschluss und die Befugnisse US-amerikanischer Geheimdienste sollten jedoch zu keiner Schieflage gegenüber der Einhaltung elementarer datenschutzrechtlicher Anforderungen führen.

So stellt sich beispielsweise schon zu Beginn eines Projekts die Frage nach der Notwendigkeit zur Durchführung einer Datenschutz-Folgenabschätzung (DSFA). Der Blick ins Gesetz und auf die Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist, liefert hierzu jedoch keine eindeutige Antwort. Verantwortliche müssen daher im Vorfeld unternehmensindividuell evaluieren, ob durch die Nutzung von Microsoft 365 die Schwelle eines voraussichtlich hohen Risikos für die Betroffenen überschritten wird. Hierzu ist eine ganzheitliche Bewertung vorzunehmen, bei der verschiedene Aspekte des jeweiligen Einzelfalls berücksichtigt werden müssen, insbesondere die Art, der Umfang, die Umstände und die Zwecke der geplanten Datenverarbeitung. Denkbar ist dabei auch, dass zwar nicht für das Gesamtprodukt, wohl aber für einzelne, besonders problematische Dienste eine Datenschutz-Folgenabschätzung durchgeführt wird.

Die Nutzung vorkonfektionierter Datenschutz-Folgenabschätzungen ist häufig nicht zielführend und in Unternehmen mit erprobtem Prozess zur Erstellung einer DSFA auch nicht erforderlich. Eine DSFA für Microsoft 365 (oder Teile davon) sollte dem Standard-Unternehmensmuster folgen und in die eigene DSFA-Landschaft passen.

Technische und organisatorische Maßnahmen

Die technischen und organisatorischen Maßnahmen, die gemäß DSGVO erforderlich sind, um die Datensicherheit bei der Verarbeitung personenbezogener Daten in Microsoft 365 sicherzustellen, können je nach Größe, Art und Umfang des Unternehmens variieren. Deren Festlegung und Dokumentation ist auch dann erforderlich, wenn keine DSFA durchgeführt wird. Microsoft bietet hierzu zahl-

reiche Optionen, deren Verfügbarkeit jedoch von der gewählten Lizenz abhängt. Exemplarisch kann Folgendes genannt werden:

- Datenverschlüsselung (Microsoft Managed Key, Customer Key, DKE)
- E-Mail-Verschlüsselung (OME, IRM, S/MIME)
- Nutzung der „Customer Lockbox“
- Nutzung von Bordmitteln zur Steuerung und Visualisierung der Sicherheit des Tenants
- Conditional Access und Multi-factor Authentication (MFA)

Das bestehende Löschkonzept muss überarbeitet und im Übrigen auf Microsoft 365 angewendet werden. Dies kann unter Verwendung von Datenklassifizierungswerkzeugen erfolgen.

Überdies bedarf es Festlegungen organisatorischer Art, etwa zum Umgang mit Funktionen, die im Rahmen des operativen Datenschutzes zum Einsatz kommen können, über grundlegende Entscheidungen zur Aktivierung/Deaktivierung kritischer Dienste bzw. Komponenten und zu einem fortlaufenden Monitoring von Updates, Erweiterungen und sonstigen Änderungen.

Weitere Vorgaben für Sicherheitsmaßnahmen werden für gewöhnlich nach einer bekannten Methodik aus dem Informationssicherheitsmanagement abgeleitet und in den entsprechenden Standards und Richtlinien detailliert beschrieben.

Die Prognose: Wechselhafte Wetterlage mit sonnigen Aussichten

Das Datenschutzgewitter scheint abzuflauen und stattdessen heitere Schönwetterwolken am Microsoft-365-Horizont aufzuziehen. In allen relevanten Bereichen sind – wie oben dargelegt – deutliche Fortschritte erkennbar. Die Restrisiken, die im Wesentlichen mit Anhörungen bzw. Maßnahmen seitens der zuständigen Datenschutz-Aufsichtsbehörde verbunden sind, müssen akzeptiert werden.

Eine erfolgreiche Einführung von Microsoft 365 erfordert jedoch eine sorgfältige Planung und Umsetzung. Da Datenschutz- und Compliance-Anforderungen in jeder Umsetzungsphase zu berücksichtigen sind, gilt dies auch für die Einbindung der entsprechenden Fachexperten.

Gerade in kleinen und mittleren Unternehmen wird hierzu in Ermangelung entsprechender Funktionsträger mit Verantwortung für Datenschutz und Informationssicherheit häufig auf die jeweiligen Beauftragten zurückgegriffen. Mit diesen sollte daher vor Beginn des Projekts eine klare Absprache bezüglich der Ressourcenplanung und -verwaltung getroffen werden. Bei Bedarf sollten die Kontingente angepasst werden.

Die datenschutzrechtlichen Fragen bleiben trotz des neuen Angemessenheitsbeschlusses und der EU Data Boundary zahlreich und die Aufgaben zur Einhaltung und Aufrechterhaltung der formalen Rechtmäßigkeit vielfältig. Neben einer gewissenhaften Dokumentation von DSFA und TOM sowie der Prüfung der vertraglichen Rahmenbedingungen (und deren regelmäßiger Aktualisierung) muss schließlich auch eine laufende Überprüfung und Bewertung der technischen Änderungen sichergestellt sein.

Nicht zuletzt müssen auch die Beschäftigten von den neuen Lösungen überzeugt werden und muss die Datenverarbeitung ihnen gegenüber transparent dargestellt werden. Der Betriebsrat ist aufgrund seines Mitbestimmungsrechts einzubinden, wobei etwaige datenschutzrechtliche Bedenken ausgeräumt und entsprechende Festlegungen und Absprachen Eingang in eine Betriebsvereinbarung finden sollten.

Die Einführung und Nutzung von Microsoft 365 kann nur als Gemeinschaftsleistung gelingen, bei der jeder einzelne Beitrag zum Schutz der Daten von Beschäftigten und Kunden sowie zur effizienten Nutzung der Plattform unverzichtbar ist. ▬

Maximilian Schmidt
Beauftragter Informationssicherheit und Datenschutz,
E-Mail: maximilian.schmidt@dz-cp.de