Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundeskanzlei BK

Bereich Digitale Transformation und IKT-Lenkung

Version 1.0

Informationspapier Entscheid CEBA

Informationen zur produktiven Nutzung von Microsoft 365

Projekt Cloud Enabling Büroautomation (CEBA)

Inhaltsverzeichnis

Hinweis: Das vorliegende Dokument fasst Informationen für den Entscheid zur Einführung von Microsoft 365 in der Bundesverwaltung zusammen. Die Informationen bilden den Stand vom 4. November 2022 ab und wurden in bundesinternen Gremien als Grundlage für die Diskussionen verwendet.

1 Ausgangslage

Das Projekt Cloud Enabling Büroautomation prüft, ob und wie «Microsoft 365», die Cloud-Version der Microsoft-Dienste, in der Bundesverwaltung eingeführt wird. Die Entscheidung dazu fällt DTI im Q1/2023 nach Konsultation des Digitalisierungsrat Bund DRB, der Generalsekretärenkonferenz GSK und nach Information des Bundesrates.

Die Firma Microsoft verfolgt die Strategie «Cloud first». Die Weiterentwicklung neuer Office- und Kollaborations-Funktionen erfolgt nur noch in der Public Cloud. Mittel- bis langfristig können viele bestehende oder neue Funktionen nicht mehr aus dem eigenen Rechenzentrum (On-Premises) bereitgestellt werden. Jedoch bleibt es mit Microsoft 365 möglich, Dokumente im eigenen Rechenzentrum zu speichern.

Die aktuelle Roadmap für einige On-Premises-Produkte von Microsoft endet 2025. Gemäss heutigem Stand ist danach der Support für diese Produkte nicht mehr sichergestellt. Deshalb muss die BK als verantwortliche Organisation für den Standarddienst Büroautomation jetzt die Nachfolgelösung Microsoft 365 in Angriff nehmen. Das Projekt CEBA schafft die Voraussetzungen zum Bezug von Microsoft 365 aus der Public Cloud mit dem Ziel, dass

- die Bundesverwaltung weiterhin handlungsfähig bleibt, sobald die Produkte nicht mehr On-Premises (im eigenen Rechenzentrum) angeboten werden können,
- den Mitarbeitenden moderne Anwendungen zur Zusammenarbeit mit internen, aber auch externen Stellen angeboten werden können.

Bei einem positiven Entscheid wird Microsoft 365 eingeführt.

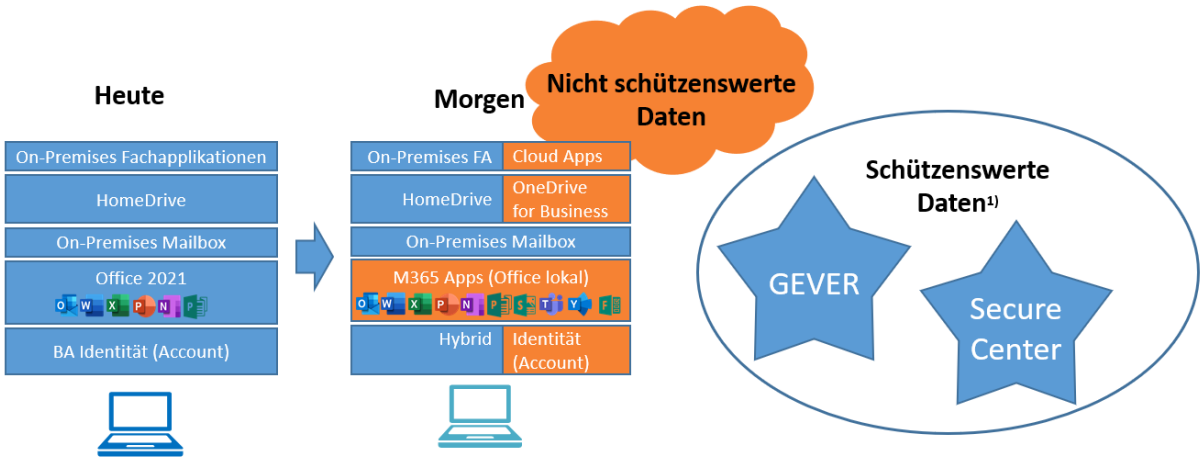
CEBA ist dabei eng abgestimmt mit der «Umsetzung Cloud-Strategie Bundesverwaltung».

Das Projekt CEBA hat in der Phase Initialisierung eine Marktanalyse vorgenommen. Kandidaten für eine neue Generation der Büroautomation waren Microsoft 365 und Google G-Suite. Die beiden Produkte wurden umfassend getestet, auch im Zusammenspiel mit On-Premises-Infrastrukturen. Ebenfalls abgeklärt wurden On-Premises-Alternativen (inkl. Open Source) zu den Microsoft-Produkten. Die Erkenntnis daraus war, dass Microsoft 365 aus zwei Gründen weiterverfolgt werden soll: Erstens sind heute zahlreiche Fachanwendungen der Bundesverwaltung eng mit Microsoft Office Anwendungen verzahnt und damit stark abhängig. Zweitens hat die Benutzerfreundlichkeit von Microsoft 365 im Vergleich überzeugt.

2 Funktionen von Microsoft 365 (M365)

Nachfolgende Microsoft 365 Produkte und Services werden eingeführt:

a. Outlook, Word, Excel, PowerPoint, OneNote. Diese stehen lokal installiert auf dem Arbeitsplatz zur Verfügung, aber auch webbasiert über den Browser. **Werden Dokumente in GEVER oder in den Fachanwendungen erstellt oder von dort geöffnet, geschieht dies auch bei Office365 wie bisher lokal auf dem Arbeitsplatz.** Das ist insbesondere relevant im Umgang mit VERTRAULICH klassifizierten Daten.
b. Microsoft Teams für Collaboration und Web-Conferencing (ohne Anbindung an das öffentliche Telefonnetz). Skype for Business wird weiterhin, im Parallelbetrieb zu Teams in der Cloud, in den Rechenzentren der Bundesverwaltung betrieben. Zurzeit werden im Rahmen der betrieblichen Tätigkeiten – ausserhalb des Projekts CEBA – erste Abklärungen zur nächsten Telefonie-Generation vorgenommen.
c. SharePoint Online & OneDrive for Business als temporäre Ablage für Geschäftsdaten. Grundsätzlich bleibt jedoch GEVER die einzige definitive Ablage für geschäftsrelevante Daten gemäss GEVER-Verordnung Art. 2 und 3.
d. Produktivitäts-Apps wie Planner, Aufgaben, Forms, Yammer und weitere.



1) Schützenswerte Daten sind z.B besonders schützenswerte Personendaten nach DSG, klassifizierte Daten nach ISchV/ISG oder Amtsgeheimnisse

Blau: bestehende Funktionalitäten
Orange: neue Funktionalitäten (teilweise in Cloud)

Was ändert sich damit für den Benutzer:

- Nahtlose Integration zwischen On-Premises und M365-Services.
- Der Benutzer kann die Funktionalitäten von Teams und freigegebene zusätzliche M365-Apps nutzen und hat damit moderne Collaborationstools zur Verfügung, die das effiziente Zusammenarbeiten fördern.
- Der Benutzer nutzt die neusten Funktionen der Office Palette (z.B. Word) mit M365-Apps, die lokal auf seinem Arbeitsplatz installiert sind.
- Es gibt eine zusätzliche persönliche Cloud-Ablage (OneDrive for Business) in M365, die in Teams integriert ist und die Zusammenarbeit mit externen Partnern vereinfachen soll.

Eine weitere Neuerung ist die Möglichkeit, Clients ortsunabhängig aufzusetzen.

Zurzeit nicht eingeführt werden Postfächer (Mail), Kalender und Kontakte in M365 (Exchange Online) sowie die Verbindung von Microsoft Teams mit dem öffentlichen Telefonnetz (PSTN). Die bestehenden Inhalte der Postfächer und Kalender sind nicht klassifiziert und das Risiko besteht, dass kritische Daten in die Public Cloud gelangen. Deshalb werden diese Gefässe grundsätzlich weiterhin On-Premises betrieben.

Mit dem Projekt und der Hybrid-Cloud werden keine bestehenden On-Premises Büroautomation Services unmittelbar abgebaut, da einige Verwaltungen voraussichtlich, aufgrund sensibler Geschäfte, vorerst keine Cloud Services nutzen werden. Mit der Hybrid-Cloud hat die Bundesverwaltung die Flexibilität, schrittweise neue Funktionen von Microsoft 365 zu nutzen.

3 Beschaffung

Mit Microsoft werden seit Jahren Verträge in Form von Enterprise Agreements abgeschlossen. Das Enterprise Agreement (EA) wurde per Anfang 2020 aktualisiert und neu abgeschlossen. Der Zuschlag erfolgte als freihändige Vergabe und wurde auf simap öffentlich publiziert. Die freihändige Vergabe wurde 2020 damit begründet, dass auf Grund der technischen Abhängigkeit keine Alternative zu den Microsoft Produkten besteht. Das EA läuft bis Ende 2022 mit Option zur Verlängerung um zwei Jahre bis Ende 2024.

4 Erkenntnisse aus der Rechtsgrundlagenanalyse

Es bestehen keine rechtlichen Hürden, welche die Bearbeitung von Daten jeglicher Art (ausser GEHEIM) in Microsoft 365 (M365) grundsätzlich verbieten. Unter Prüfung der bestehenden Rechtsgrundlagen und der durchgeführten Risikoanalyse kann eine Verarbeitung von **INTERN klassifizierten Daten** nach Informationsschutzverordnung (ISchV) und **Personendaten** nach Datenschutzgesetz (DSG) ohne zusätzliche Schutzmassnahmen in M365 zugelassen werden.

Für die Bearbeitung von VERTRAULICH klassifizierten Daten (Office Daten), Amtsgeheimnissen sowie besonders schützenswerten Personendaten, werden die Officeanwendungen von M365 weiterhin lokal verwendet und die Daten werden bei Bedarf mit der Software Secure Center (später CHCrypt) bearbeitet und auf On-Premises Ablagen (wie GEVER) gespeichert.

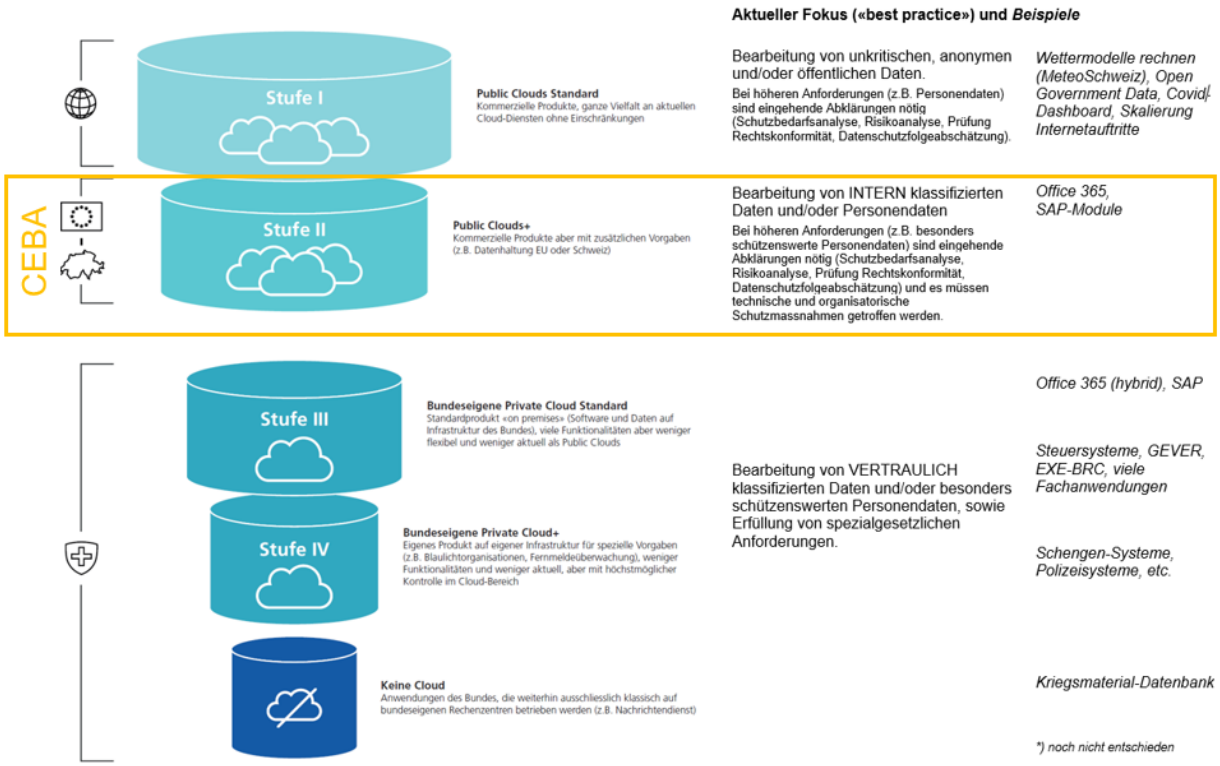
Mit in Verträgen mit Microsoft definierten Massnahmen und Werkzeugen zur Verschlüsselung der Daten, laufenden Überwachung der Vorgänge und von Sicherheitsvorfällen, Compliance Prüfungen und vertraglichen Absicherungen wird ein adäquater Schutz geboten, damit Daten der Stufe INTERN in M365 bearbeitet werden können. Aufgrund der Wichtigkeit dieser Daten empfiehlt CEBA die Bearbeitung von VERTRAULICH klassifizierten Daten nur in der Geschäftsverwaltung des Bundes GEVER oder auf den im eigenen RZ betriebenen Datenablagen. Entsprechend müssen die Benutzer dafür geschult und technisch unterstützt werden (beispielsweise durch Popup-Warnungen oder einer Blockierung, wenn jemand versucht, ein als VERTRAULICH klassifiziertes Dokument in M365 zu speichern).

5 Verfügbarkeit

Microsoft garantiert eine sehr hohe Verfügbarkeit in der Public Cloud (99.9% während 7x24 Std.).

Die Microsoft 365 Benutzerdaten werden täglich in die Bundes-Rechenzentren gesichert. Gesichert werden die Cloud-Datenablagen von SharePoint, OneDrive und Teams. Das Detailkonzept dazu wird in der Phase Realisierung erstellt und umgesetzt.

Das Projekt CEBA hält die Cloud-Strategie des Bundesrates ein und bewegt sich auf der Stufe II der Cloud Stufen in der Bundesverwaltung.



6 Massnahmen zum Business Continuity Management (BCM)

Das BCM-Konzept sieht einen zweistufigen Backup Prozess vor: Die Daten, die neu in der Cloud bewirtschaftet werden, werden regelmässig in einem Cloud Backup gesichert. Diese Sicherung wird danach als Kopie in den Rechenzentren der Bundesverwaltung abgelegt. Bei einer Wiederherstellung in andere Tools als Microsoft 365 gibt es allerdings qualitative Einbussen, insbesondere bei Chatverläufen und Teams Inhalten, da es dafür kein adäquates Tool auf dem Markt gibt.

Das Projekt sieht ausserdem vor, alternative Open Source Produkte in einem Laborbetrieb zu überprüfen. Damit sollen in der Bundesverwaltung Erfahrungen gesammelt werden, wie die bestehenden Abhängigkeiten von Microsoft reduziert werden können. Ausserdem wird so eine zusätzliche BCM-Möglichkeit aufgebaut.

7 Restrisiken

Bei der Verwendung von Microsoft 365 fallen technische, politische und rechtliche Risiken an. Die trotz der getroffenen Massnahmen verbleibenden Restrisiken beim Bezug von Public Cloud Leistungen müssen bekannt sein und von den Verwaltungsstellen getragen werden.

7.1 Technische Risiken und Ausfallrisiko

Die Verfügbarkeit von IKT-Services ist in der Public Cloud sehr hoch. Hingegen sind die Cloud-Dienste bei einem Netz-Ausfall nicht mehr zugänglich. Der Netz-Zugang ist daher kritisch und muss entsprechend redundant und leistungsfähig ausgebaut sein. Das lokal installierte Office-Paket von Microsoft 365 funktioniert weiterhin, auch wenn das Gerät nicht online ist.

Durch den Cloud Anbieter werden mit der Nutzung des Services Rand[1]- und Metadaten generiert und gespeichert. Diese könnten potenziell missbraucht werden, wie z.B. durch Auswerten des Arbeitsverhaltens oder Persönlichkeitsprofils und Weitergabe an interessierte Stellen oder für andere kommerzielle Interessen. Obwohl Microsoft gegenüber relevanten Standards auditiert und zertifiziert ist und die Auditberichte im Microsoft Trustcenter jederzeit eingesehen werden können, kann diese Gefahr nicht ganz ausgeschlossen werden.

Im Rahmen des Microsoft Enterprise Agreement (EA) wurden auch vertragliche Absicherungen für die Bundesverwaltung vereinbart. Trotzdem werden Identitäten und Anmeldeinformationen in Europa und damit in einem anderen Rechtsraum gehalten. Auch muss davon ausgegangen werden, dass das Management respektive die Aktivitäten der Betriebsorganisation des Providers teilweise global erfolgen.

Das unverschlüsselte Ablegen von VERTRAULICHEN Informationen und besonders schützenswerten Personendaten ist auf den Ablagen in Microsoft 365 nicht zulässig. Dies kann technisch nicht vollumfänglich verhindert werden, insbesondere wenn keine oder eine falsche Klassifizierung erfolgt. Das Projekt testet dazu den Einsatz eines «Data Loss Prevention Tools» auf dem Client. Der Endbenutzer muss, trotz der technischen Unterstützung, die Verantwortung für die abgelegten Dateninhalte übernehmen und sich dieser Verantwortung auch bewusst sein.

7.2 Politisches Risiko

Mit dem Grad der «Cloudisierung» von Microsoft 365 Services wächst die Abhängigkeit zu Microsoft. Diese Tatsache führt zu Diskussionen rund um die Aufrechterhaltung der staatlichen digitalen Souveränität. Aktuell wird dies in Zusammenhang mit Beschlüssen von Kantonen und der SUVA auch in der Presse und der Öffentlichkeit breit diskutiert. Das Risiko besteht, dass bei entsprechend hohem Druck der Bundesverwaltung die Nutzung von Public Clouds und damit auch der Einsatz von Microsoft 365 untersagt wird.

Bei Staaten wie Deutschland und Frankreich werden diese Diskussionen ebenfalls geführt, eine Lösung wurde aber noch nicht gefunden. Aktuell versucht man, mit europäischen Anbietern Gegensteuer

[1] Z.B. Fehlerlogs, Logs über Nutzungsverhalten der Anwendungen, Lizenzinformationen

zum US-dominierten Markt zu geben. Microsoft reagiert auch bereits auf den Druck, es wurde angekündigt, die Zusammenarbeit mit lokalen Providern zu suchen. CEBA ist offen für Anpassungen, die allenfalls in den kommenden Monaten und Jahre möglich werden (ein Zuwarten auf diese Entwicklungen würde jedoch bedeuten, dass der Standarddienst Büroautomation aus heutiger Sicht ab 2026 nicht mehr gewährleistet werden kann).

Ferner besteht das Risiko einer widerrechtlichen nachrichtendienstlichen Ausspähung der Daten und Metadaten durch Staaten oder andere Organisationen. Da die Microsoft Services weltweit breit genutzt werden und dadurch unter ständiger Beobachtung stehen, wird dieses Risiko gemäss der Risikoanalyse zum ISDS Konzept jedoch als moderat eingeschätzt und besteht grundsätzlich auch für bestehende On-Premises-Anwendungen.

7.3 Rechtliche Risiken

Der CLOUD (Clarifying Lawful Overseas Use of Data) Act erlaubt US-Strafverfolgungsbehörden, zur Aufklärung oder Verfolgung schwerer Straftaten («serious crimes»), die Herausgabe von Daten bei den Cloudanbietern zu verlangen, die diese in ihrem Besitz oder unter ihrer Kontrolle haben. Dies gilt auch dann, wenn sich die entsprechenden Daten im Ausland befinden, was dem Gesetz einen extraterritorialen Anwendungsbereich verleiht. Gemäss dem CLOUD Act der USA können US-Unternehmen verpflichtet werden, Kundendaten an die amerikanischen Behörden herauszugeben.

Microsoft verpflichtet sich, eine Strafverfolgungsbehörde immer direkt an die Kundin oder den Kunden zu verweisen. Wenn Microsoft gezwungen wird, verarbeitete Daten an Strafverfolgungsbehörden weiterzugeben, benachrichtigt Microsoft die Kunden unverzüglich, sofern die Benachrichtigung nicht gesetzlich verboten ist.

8 Einsatzrichtlinie

Für den Pilotbetrieb von CEBA wurde eine Einsatzrichtlinie definiert, welche die Grundsätze der Bearbeitung der Daten auf der Plattform regelt. Für den produktiven Einsatz von CEBA ist dasselbe Vorgehen geplant. Die Einsatzrichtlinie regelt insbesondere den Umgang mit als VERTRAULICH klassifizierten und besonders schützenswerten Personendaten. Zur Unterstützung werden technische Massnahmen eingeführt (Warnung vor der ungewollten Ablage in der Cloud bei klassifizierten Dateien; siehe Ziff. 4).

9 Kosten und Finanzierung

Die Projektkosten für BK-externen Leistungen werden sich auf rund 26 Mio. CHF belaufen (Vergleich Migration Windows 10 mit dem Programm APS2020 CHF 70 Mio.). Dies umfasst die zentrale Beschaffung und Einführung der Microsoft 365 Services. Diese Kosten trägt das Projekt zentral (Mittel für die Weiterentwicklung der Standarddienste).

Die Departemente und Verwaltungseinheiten werden Einführungsprojekte starten, das Projekt CEBA wird mit dem Einführungskonzept den Ablauf vorgeben. Das Projekt wird für die Schulung der Endanwender Schulungskonzepte und Schulungsinhalte erarbeiten und die Schulungen organisieren. Die Departemente und Verwaltungseinheiten finanzieren ihre Aufwände für die Einführung selbst, wie dies auch bei der letzten Migration (Arbeitsplatzsystem 2020) der Fall war. Das Projekt CEBA wird die Konzepte und den Systembau, die Transition, Schulung, sowie die Hälfte der Kosten für die während den ersten zwei Einführungstagen eingesetzten Floorwalker (Supporter) finanzieren.

Mit der etappenweisen Einführung von Microsoft 365 wird es einen Parallelbetrieb von Services aus der Cloud, wie auch On-Premises Services geben (Hybrid-Cloud-Umgebung, vgl. Kap.2). Für den Parallelbetrieb wird mit Mehrkosten gerechnet.

Bei der Beantragung des Verpflichtungskredits wird auf eine besondere Botschaft – wie bei Schlüsselprojekten sonst üblich – verzichtet, insbesondere weil CEBA nicht aufgrund seiner finanziellen Dimensionen, sondern primär aufgrund seiner strategischen Bedeutung für die Bundesverwaltung als

Schlüsselprojekt festgelegt wurde. Das geplante Gesamtvolumen für das Projekts CEBA ist deutlich kleiner als bei den meisten übrigen Schlüsselprojekten.

10 Konsequenzen bei Verzicht auf Microsoft 365

Beim Verzicht auf Cloudleistungen von Microsoft, ohne adäquate Alternativprodukte, drohen folgende Konsequenzen:

- Erhöhte Sicherheitsrisiken: Für die Microsoft Services werden laufend Sicherheitsfunktionalitäten weiterentwickelt und auf den Systemen implementiert. Mittelfristig werden solche Schutzmechanismen nur noch als Cloud Lösungen bereitgestellt werden.
- Höhere Kosten: Voraussichtlich werden die Kosten für den Support und den Weiterbetrieb von On-Premises Microsoft Produkten zunehmend erhöht.
- Geringe Zukunftsfähigkeit: Die Cloud-Strategie von Microsoft führt dazu, dass Funktionalitäten und Services nur noch für die Cloud Versionen entwickelt werden. Dies birgt das Risiko, dass ab 2026 benötigte Funktionalitäten nicht mehr On-Premises zur Verfügung stehen.
- Einbussen bei der Zusammenarbeit: Mit Teams bietet Microsoft die Nachfolgelösung zu Skype for Business, die noch wesentlich stärker für die organisationsübergreifende Kollaboration ausgelegt ist. Teams ist nur als Cloud Lösung verfügbar.
- Bremsen der Digitalisierung: Hinter Microsoft 365 stehen auch Tools für eine Optimierung der Automatisierung und durchgängiger Prozesse sowie mobiler Zusammenarbeit. Diese sind nur als Cloud Lösung verfügbar.