Eine kritische Einschätzung zur Einführung von Microsoft 365

Für was diese Präsentation?

- Argumentationshilfe für
  - Menschen, die von der Einführung von M365 betroffen sind und diese kritisch sehen
  - Alle anderen, die dieses Thema interessiert

Die hier vorgebrachten Argumente sind solche, die gegegenüber "Entscheidern" vorgebracht werden können.

- Folgende Argumentfelder sind nicht enthalten
  - Freiheit der User/Freie Software
  - Überwachungskapitalismus
  - soziale Argumentation
  - ökologische Argumentation
  - antikapitalistische Argumentation
- Also generell keine Argumentation aus einer ethischen Motivation heraus

Überblick

- Motivation
- Microsoft 365 und Datenschutz
- Microsoft 365 und Vendor Lock-In
- Microsoft 365 und digitale Souveränität
- Einführung Microsoft 365: Organisation
- Fragen

- Wer hat die Einführung von M365 beschlossen?
  - Die IT
  - Die IT-Leitung
  - Die Geschäftsführung
- Wurden betroffene Personen und Abteilungen (Mitarbeiter:innen, IT, Betriebsrat) beteiligt?
- Was soll durch die Einführung von M365 erreicht werden?
  - Kostensenkung
  - Steigerung der Effizienz
  - Nutzung von Synergien, weil andere Abteilungen/Schwesterfirmen schon M365 nutzen

Mögliche Fragen an die Entscheider am Ende dieser Präsentation

Datenschützer sehen Microsoft 365 in Behörden als nicht rechtskonform an

- Datenschutzkonferenz: Es sei “kein datenschutzgerechter Einsatz von Microsoft 365 möglich”
  - fehlende Beschreibung von Art und Zweck der Verarbeitung
  - es geht nicht eindeutig hervor, welche personenbezogenen Daten verarbeitet werden
  - Microsoft unterliegt dem Cloud Act
  - keine ausreichende Darstellung von Maßnahmen zum Schutz von personenbezogenen Daten
  - von Microsoft werden Daten, die zu eigenen Zwecken verarbeitet werden, nicht gelöscht
  - fehlende Transparenz beim Einsatz von Unterauftragnehmern
- Quellen:
  - https://www.datenschutzkonferenz-online.de/media/pr/20201030_protokoll_3_zwischenkonferenz.pdf
  - https://www.dids.de/2020/10/26/entscheidung-der-datenschutzkonferenz-zu-ms-office-365/
  - https://www.heise.de/news/Datenschuetzer-sehen-Microsoft-365-in-Behoerden-als-nicht-rechtskonform-an-4893604.html

Datenschutzbewertungen aus den Bundesländern: Berlin

Berliner Datenschützerin: Rote Ampel für Teams

- Microsoft hat das DPA "Deutsch, Januar 2020" ohne Kennzeichnung nachträglich umfangreich geändert.
- Anbieter behält sich die Verarbeitung von Auftragsdaten im Punkt "Eigentumsverhältnisse" zu eigenen Zwecken vor. Eine Rechtsgrundlage ist nicht ersichtlich
- Microsoft behält sich eine Verarbeitung der Auftragsdaten an jedem Ort vor, an dem Microsoft oder seine Unterauftragsverarbeiter tätig sind, also auch in den USA
- Unklar, welche Unterauftragsverarbeiter konkret wofür eingesetzt werden
- Viele Unklarheiten und Widersprüche im Auftragsverar-beitungsvertrag
- Unzulässige Datenexporte
- DPA Januar 2020 enthält an vielen Stellen Regelungen, die den gesetzlichen Mindestanforderungen widersprechen
- Unzulässige Einschränkungen des Rechts für Kund:innen
- Löschpflicht nach Auftragserledigung wird stark eingeschgränkt
- Unklarer AVV macht es den Verantwortlichen unmöglich, ihrer Rechenschaftspflicht nach DSGVO nachzukommen

https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2021-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf

Datenschutzbewertungen aus den Bundesländern: Baden-Württemberg

Offenbar negative Datenschutz-Folgeabschätzung in BW

Kultusministerin Eisenmann hat eine Datenschutz-Folgenabschätzung zum Einsatz von M365 in Auftrag gegeben. Die Studie wurde nicht veröffentlicht. Der Datenschutzbeauftragte Brink konnte sie einsehen und schrieb anschließend: "Es scheinen derzeit strukturelle Merkmale vorzuliegen, welche die Möglichkeit eines datenschutzkonformen Einsatzes fraglich erscheinen lassen"

https://www.badische-zeitung.de/eisenmann-setzt-auf-microsoft-plattform-fuer-schulen-und-erntet-kritik--189022089.html

PS: Eine Datenschutz-Folgeabschätzung ist immer dann durchzuführen, wenn "aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen" besteht

Problem Cloud Act

- US-Unternehmen sind verpflichtet, US-Behörden auch dann Daten zu übergeben, wenn die Server nicht in den USA stehen
- MS versucht, dies mit Anhängen zu den Standardvertragsklauseln abzumildern, diese sind aber weitgehend wirkungslos "Damit sei, so die gemeinsame Bewertung der beteiligten Datenschutzaufsichtsbehörden, die Transferproblematik in die USA nicht generell gelöst"
- die Klauseln sehen an keiner Stelle eine Information der betroffenen Personen vor wenn Microsoft ihre personenbezogenen Daten an Behörden von Drittländern herausgibt.
- Matthias Bergt, Datenschutz-Referatsleiter in Berlin: "gigantische Masse an Nebelkerzen"

https://www.cr-online.de/blog/2020/11/22/zusatz-zu-standardvertragsklauseln-massenweise-nebelkerzen-von-microsoft-und-manchen-datenschutz-aufsichtsbehoerden/

Teams sammelt Daten

- Eine neue Funktion zur Berechnung von “Produktivitätswerten” verwandelt Microsoft 365 in ein vollwertiges Werkzeug zur Arbeitsplatzüberwachung
- Das Objekt “activityStatistics” stellt die “Zeit dar, die ein Benutzer für verschiedene Arbeitsaktivitäten während und außerhalb der Arbeitszeit für den angegebenen Zeitraum in der Anfrage verbracht hat, von Anrufen über Chats bis hin zu E-Mails und Kalendereinträgen”.
- in Workplace Analytics weist Microsoft jedem Mitarbeiter einen “Influence Score” zu, einen “numerischen Wert, der angibt, wie gut eine Person innerhalb des Unternehmens vernetzt ist”, basierend auf umfangreichen E-Mail-, Kalender-, Anruf- und Chat-Daten.

Datenschützer Wolfie Christl
https://twitter.com/WolfieChristl/status/1331579706349645824

Teams sammelt Daten

Microsoft hat angekündigt (noch nicht umgesetzt), diese Funktionalität abzumildern. Überwacht und gespeichert werden wird das Verhalten weiterhin, kann dann jedoch nur noch in aggregierten Ansichten zu größeren Personengruppen eingesehen werden.

Weiter werden mehr oder minder arbiträre Daten wie die Nutzung von Chatfunktionen herbeigezogen, um die Qualität von Arbeitsergebnissen zu bewerten. Die Akzeptanz technischer Mittel wird mit Erfolg gleichgesetzt.

Es gibt ein MS-Patent auf eine Methode aufgrund von "Veränderung von Verhalten" Nutzer:innen mit "Kollaborationsproblemen" zu identifizieren.

https://netzpolitik.org/2020/microsoft-office-365-ueberwachung-des-verhaltens-angestellter-soll-beschraenkt-werden/

Microsoft Viva

Am 04.02.2021 hat Microsoft die neue Plattform "Microsoft Viva" vorgestellt, die Teil von M365 sein wird. MS Viva besteht aus 4 Teilen:

- Viva Connections: Ein soziales Intranet
- Viva Topics: Eine Wissenssammlung
- Viva Learning: Eine Lern-Plattform
- Viva Insights:

Analyse für das Zeitmanagement. Manager haben Zugriff auf die Zeiteinteilung von Teams. Es lassen sich Analysen über die Verbindungen verschiedener Arbeitsgruppen herstellen. *"Viva Insights unterstützt Einzelpersonen und Unternehmen mit datengestützten Erkenntnissen und Empfehlungen. Viva Insights ermöglicht Führungskräften, Entwicklungen auf der Team- und Organisationsebene zu erkennen"* Ein herunterbrechen der Analyseergebnisse auf einzelne Mitarbeiter:innen soll für Vorgesetzte nicht möglich sein.

Quellen:

- https://www.golem.de/news/microsoft-teams-wird-mit-ms-viva-zum-intranet-2102-153947.html
- https://www.drwindows.de/news/microsoft-enthuellt-microsoft-viva-die-all-in-one-plattform-fuer-den-digitalen-arbeitsplatz
- https://news.microsoft.com/de-de/microsoft-stellt-neue-employee-experience-platform-microsoft-viva-vor/

Fazit Datenschutz

Es ist davon auszugehen, dass alles was über die Microsoft-Online-Werkzeuge getan und verarbeitet wird bei Microsoft gespeichert und durch Microsoft analysiert wird, denn Microsoft behält sich die Verarbeitung von Kundendaten für eigene Zwecke vor Arbeitgeber erhalten - wenigstens zum Teil - Zugriff auf diese Analysen, was auch zu einer Beurteilung von Gruppen oder gar einzelnen Mitarbeitern führen kann. Auch wenn das herunterbrechen der Analsye auf einzelne Mitarbeiter:innen nicht möglich sein soll - die betroffenen Personen selbst können sie einsehen und das Management könnte von Mitarbeiter:innen verlangen, diese Daten weiterzuleiten. Außerdem ist es äußerst unangenehm zu wissen, dass man von der Software, mit der gearbeitet wird, ständig überwacht und analysiert wird.
Die weiterhin offenen Fragen beim Datenschutz - insbesondere, was den Transfer von Daten in die USA angeht -, die unklaren und widersprüchlichen Aussagen in den Verträgen, die unzulässige Einschränkung von Rechten für Nutzer:innen, die die DSGVO vorsieht, machen Microsoft 365 zu keinem Werkzeug, dem man sorglos Daten anvertrauen kann, von der dadurch fehlenden Rechtssicherheit ganz zu schweigen.

Microsoft 365 und Vendor Lock-In

Unter Vendor Lock-in versteht man wenn Kunden derart von den Produkten oder Dienstleistungen eines Anbieters abhängig sind, dass sich der Wechsel zu einem Mitbewerber wirtschaftlich nicht rechnen würde.

Die Gefahr des Vendor Lock-In ist um so höher je mehr Dienste eines Cloud Service Providers in Anspruch genommen werden und je integrierter die Services sind.

Microsoft 365 bietet einen umfassend integrierten Dienst an, eine komplette SaaS-Lösung. **Die Gefahr des Vendor Lock-In ist hier also sehr hoch zu bewerten**

- IT-Strategen raten beim Gang in die Cloud zur Vermeidung des Vendor Lock-In zu einer Strategie, welche beinhaltet
  - die Nutzung mehrerer Cloud-Anbieter parallel
  - die Infrastruktur des Cloud-Anbieters lokal zu duplizieren
  - die Nutzung offener Standards
  - zu Vermeiden proprietäre Elemente der Cloud zu nutzen
  - auf Interoperabilität und Portabilität zu achten
  - die Nutzung von Open-Source Software
  - eine Hybrid-Cloud bzw. Hybrid-IT Strategie
    - Wichtige Daten werden in einer private Cloud bzw. vor Ort im Rechenzentrum vorgehalten
    - weniger wichtiges kommt in die Public Cloud
  - das Planen einer Exit-Strategie vor dem Gang in die Cloud

Siehe auch "Vendor Lock-in in the transistion to a Cloud Computing platform", Menatalla Ashraf Fawzy Kamel, KTH Royal Institute of Technology, Stockholm, 2015

Microsoft 365 und digitale Souveränitat

Digitale Souveränität bedeutet:

- selbstbestimmtes Handeln und Entscheiden von Menschen, Unternehmen und anderen Institutionen im digitalen Raum, wobei sie die Hoheit über ihre eigenen Sicherheits- und Datenschutzinteressen behalten sollen
- die Fähigkeit, die Vertrauenswürdigkeit, Integrität, Verfügbarkeit der Datenübertragung, -speicherung und -verarbeitung durchgängig kontrollieren zu können
- die Selbstbestimmung von Dateneigentümern über die Nutzungsbedingungen für ihre Daten

"Wer öffentliche Clouds und Plattformen nutzt, gibt digitale Souveränität preis. Unverschlüsselt in einer von Dritten betriebenen Cloud oder Plattform gespeicherte oder verarbeitete Daten sind gegenüber dem Betreiber technisch nicht geschützt. Ein Ausfall der Cloud/Plattform oder der notwendigen Kommunikationsdienste führt zu (temporärer) Unverfügbarkeit der Daten/Dienste"

"Digitale Souveränität" - Kompetenzzentrum Öffentliche IT - Fraunhofer-Institut für Offene Kommunikationssysteme

- Ein Microsoft-Account kann jederzeit ohne Begründung gesperrt werden, es wird meist nur auf die Nutzungsbedingungen verwiesen
- Auf Inhalte, die auf den betreffenden Diensten abgelegt sind, kann nicht mehr zugegriffen werden.

Günter Born: https://www.golem.de/news/microsoft-digitale-amnesie-durch-willkuerliche-kontensperrungen-2008-150217-3.html

Bedeutung für die Organisation

- Unweigerliche Bindung an Microsoft
- Die Komplexität für Nutzer wird stark erhöht, ohne Schulung werden viele mit Teams nicht zurecht kommen
- Teams wird der neue Desktop
- Viele Prozesse (z.B. Telefonieren) werden viel mehr Schritte erfordern, es wird un-intuitiver
- Prozesse müssen angepasst werden
- Upgrade und redunante Auslegeung der Internetanbindung
- Kosten?
- Fallstricke sind:
  - Fehlende Nutzerakzeptanz
  - Fehlende Vorbereitung
  - Mangelnde Fortbildung

Quelle: Webinar “Microsoft Teams – die ultimative Plattform für alle?”
https://www.comconsult.com/kostenlos-microsoft-teams/

Fragen

- Wurde eine Datenschutz-Folgeabschätzung nach Art. 35 DSGVO vorgenommen?[1]
- Wird beabsichtigt, die Analyse-Möglichkeiten zu Beurteilung von Teams/Mitarbeiter:innen zu nutzen?
- Wie sollen Mitarbeiter:innen vor der Analyse ihres Verhaltens durch Microsoft geschützt werden?
- Was wurde getan, um Vendor Lock-In zu vermeiden?
- Wurde eine Exit-Strategie geplant?
- Welche Sicherungsmaßnahmen gibt es, um die Verfügbarkeit zu gewährleisten, wenn Microsoft Dienste nicht erreichbar sind oder Konten gesperrt werden?
- Wie sieht die Gesamtstrategie aus? Gibt es einen "Masterplan"?
- Welche Alternativen zur Migration nach M365 wurden in Betracht gezogen?
- Wer wird in welchem Umfang geschult?
- Wie soll der, zumindest kurzfristige, erhöhte personelle Mehraufwand bei der Migration bewältigt werden?

[1]Aufgrund einiger datenschutzrechtlicher Risiken beim Einsatz in Unternehmen muss beim Einsatz von Microsoft 365 in der Regel im Vorfeld eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO (DSFA) durchgeführt werden
https://www.srd-rechtsanwaelte.de/blog/dsfa-microsoft-365/