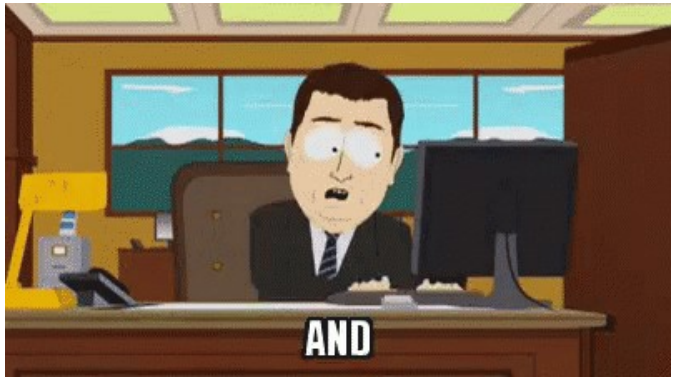
Testfolie

- Testtext nach Klick
- Noch ein Testtext nach Klick

There is no cloud, just other people's computers.



Risiken bei der Nutzung von Cloud-, Videokonferenz- oder Übersetzungsdiensten

Zur Person

- Mathematiker, CAU Kiel
- Seit 2001 hauptberuflich in der IT eines großen internationalen Logistikers, dort nicht-freigestellt (für ver.di) im Betriebsrat
- Ehrenamlich
  - Referent bei mehreren DGB-Gewerkschaften zu netzpolitischen Themen
  - Seit 2008 Datenschutzbeauftragter verschiedener Einrichtungen der EKiR
  - Aktiv im Chaos Computer Club
  - Seit 2013 Veranstalter von Praxisseminaren zur digitalen Selbstverteidigung

Hackerethik

- Der Zugang zu Computern und allem, was einem zeigen kann, wie diese Welt funktioniert, sollte unbegrenzt und vollständig sein.
- Alle Informationen müssen frei sein.
- Mißtraue Autoritäten – fördere Dezentralisierung.
- Beurteile einen Hacker nach dem, was er tut, und nicht nach üblichen Kriterien wie Aussehen, Alter, Herkunft, Spezies, Geschlecht oder gesellschaftliche Stellung.
- Man kann mit einem Computer Kunst und Schönheit schaffen.
- Computer können dein Leben zum Besseren verändern.
- Mülle nicht in den Daten anderer Leute.
- Öffentliche Daten nützen, private Daten schützen.

Cloud?


Cloud
Web 2.0
Multimedia
Big Data
Blockchain
AI
agile
Social media
Resilienz
IoT
Cyber
Security

Endlich in der Cloud

Kein Stress mehr mit

- Updates
- Sicherheitslücken
- Hardwareausfällen
- Serveradministration
- Backup
- dem Umkopieren von Daten
- Physischer Serversicherheit

Und wie kommen wir wieder raus?

- Clouddienste sind, wie alle Abhängigkeiten von Monopolen, wie Aalreusen.
- Am besten arbeiten sie mit den Diensten des eigenen Herstellers zusammen.

A propos

https://www.heise.de/news/Informatiker-Deutschland-tappt-in-der-Microsoft-Cloud-in-die-Datenfalle-10002062.html

Informatiker: Deutschland tappt in der Microsoft-Cloud in die Datenfalle

Immer mehr Behörden wollen in die Microsoft-Cloud, schlägt die Gesellschaft für Informatik Alarm. Deutschland drohe, "im goldenen Microsoft-Käfig" zu landen.

337

(Bild: StockStudio/Shutterstock.com)

01.11.2024, 17:46 Uhr Lesezeit: 3 Min.

Von Stefan Krempl

Aus dem Artikel

- Die GI zitiert ein Interview des britischen Geheimdienstchefs Richard Moore vom MI6 aus dem Jahr 2021. Der Spionageexperte sprach von einer "Datenfalle": "Wenn Sie einem anderen Land erlauben, Zugang zu wirklich kritischen Daten über Ihre Gesellschaft zu erhalten, wird das mit der Zeit Ihre Souveränität aushöhlen."
- Digitale Monopole könnten ihre Preise brutal erhöhen, heißt es weiter. In der Verwaltung sei hier eine weitere Explosion zu erwarten.

Inside IT

https://www.inside-it.ch/behoerden-fuerchten-goldenen-microsoft-kaefig-20241105

Behörden fürchten goldenen Microsoft-Käfig

Von Mark Schröder, 5. November 2024 um 12:26

DATENSCHUTZ DOMINIKA BLONSKI KANTON BUND CLOUD E-GOVERNMENT
MICROSOFT LUZERN ZÜRICH POLITIK & WIRTSCHAFT

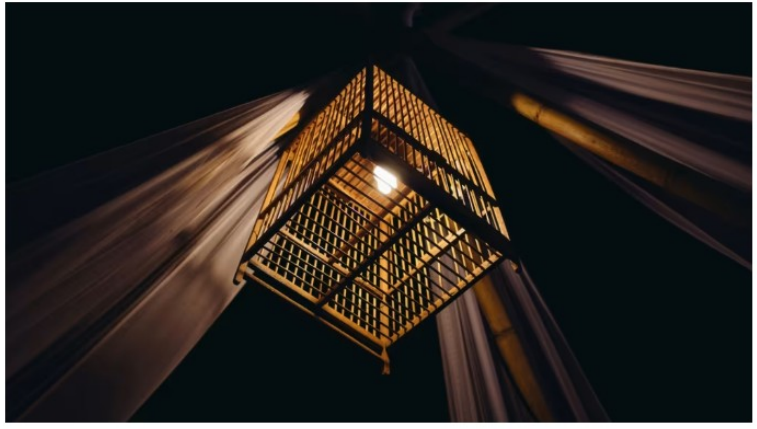


Foto: Samule Sun / Unsplash

Durch deutsche Amtsstuben tönt der Aufschrei: Wir sind gefangen im goldenen Microsoft-Käfig! Denn bei der Büro-Software haben sie oftmals keine Wahl. In der Schweiz ist die Situation vergleichbar.

Aus dem Artikel

Die Frage nach dem geltenden Datenschutzrecht könne lediglich auf dem Papier geklärt werden. Sind die Daten einmal auf Microsoft-Servern gespeichert, hat der Provider die volle Kontrolle. Dann gelten für die Bürgerdaten das deutsche und das US-amerikanische Recht, so die Experten. [...]

Das Versprechen der Datenhaltung innerhalb der Landesgrenzen ist allerdings nur die halbe Wahrheit, betonte zum Beispiel Zürichs Datenschützerin Dominika Blonski im Interview mit inside-it.ch. Nach ihren Worten ist die Nutzung von Software wie Microsoft 365 eine "Auslagerung der Datenbearbeitung". Diese könne nur dann datenschutzkonform sein, wenn je nach Konstellation sichergestellt werden könne, dass der Auftragnehmer keinen Zugriff auf die Daten hat. Das sei zum Beispiel mit Datenverschlüsselung sicherzustellen, schlug sie vor.

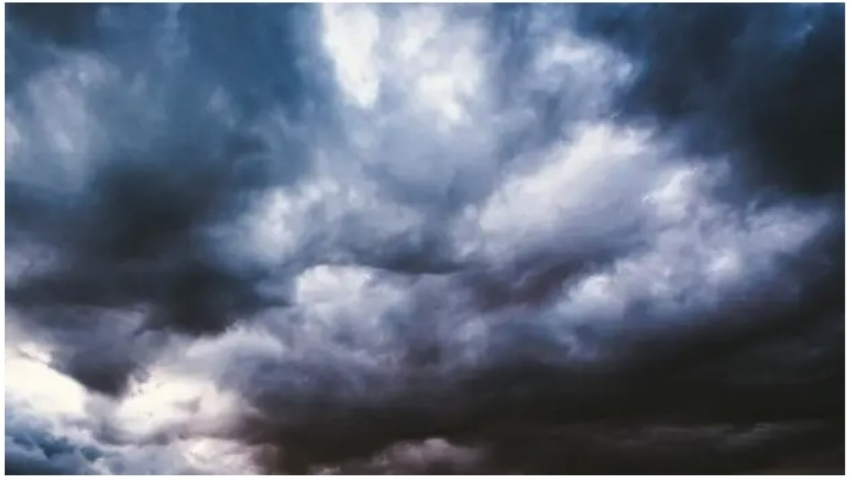
CLOUD Act

https://www.heise.de/news/Im-Widerspruch-CLOUD-Act-gegen-EU-DSGVO-4103247.html

Im Widerspruch: CLOUD Act gegen EU-DSGVO

Mit dem CLOUD Act verschärft die US-Regierung ihre weltweite Kontrolle über Daten. Doch das Gesetzt steht klar im Konflikt mit der EU-DSGVO.

101



12.07.2018, 09:30 Uhr Lesezeit: 1 Min. | iX Magazin

Von Moritz Förster

International Data Corporation

https://www.heise.de/news/IDC-Viele-Unternehmen-wollen-teils-raus-aus-der-Cloud-10001826.html

Kosten meist höher als gedacht: Kunden verabschieden sich (teils) von der Cloud

Zu teuer, zu kompliziert, zu langsam: Die Marktforscher von IDC sehen einen klaren Trend, dass Unternehmen Workloads aus der Cloud zurückholen.

259

(Bild: iX)

01.11.2024, 15:25 Uhr Lesezeit: 3 Min. | iX Magazin

Von Moritz Förster

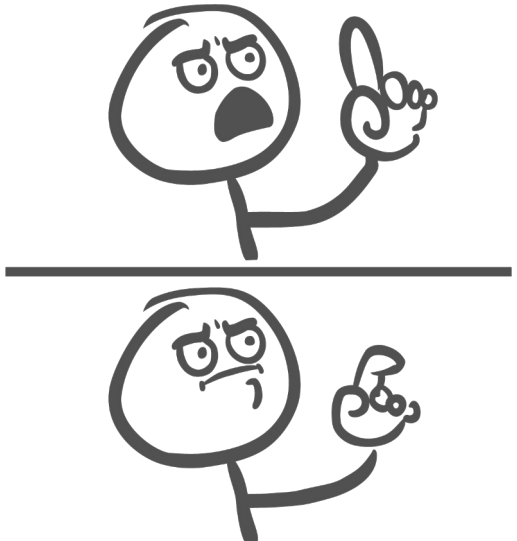
Beispiel: Schulen in der Pandemie

- Entweder: Linuxserver mit Owncloud plus Moodle plus Only Office plus Big Blue Button oder Jitsi plus Element (Matrix)
  - Wo hosten? Wer ist verantwortlich? Gibt es einen AV-Vertrag? Wie funktioniert das Backup?
  - Wer trainiert die Anwenderinnen?
  - Wer pflegt, wer kümmert sich um den Server, wenn die 9a am Montagmorgen um 8 Uhr nicht an ihre Aufgaben kommt?

- Oder: MS365, hier unterschreiben, morgen hat die ganze Schule Vollzugriff auf die gesamte Produktpalette.
  - Nobody ever got fired for bying ~~IBM~~ Microsoft.

Was heißt hier „verschlüsselt“?

- Was Firmen sagen: „Unser Dienst ist verschlüsselt.“
- Was Firmen meinen: „Ihre Daten sind auf dem Weg zu unseren Servern verschlüsselt. Wir selbst können (und werden) sie selbstverständlich lesen.“



Transport- vs Ende-zu-Ende-Verschlüsselung

Client lesbar

verschlüsselt

Server lesbar

Client

verschlüsselt

Server

Wer kann mitlesen?

- Der Cloudanbieter zur
  - „Verbesserung des Benutzungserlebnisses“
  - Erkennung von Urheberrechtsverletzungen und Straftaten
- Bei Firmen: die Geschäftsführung
- Ermittlungsbehörden (nicht nur die eigenen)
- Geheimdienste (nicht nur die eigenen)
- 3\/i1 |-|4X0rZ
- Andere Nutzerinnen, wenn es eine Sicherheitslücke gibt

Übersetzungs- und KI-Dienste

- Um die Qualität der Ausgabe zu verbessern, müssen wir Interna an die KI geben, die unter anderem zum weiteren Training verwendet werden könnten.
- Bei MS Copilot besteht das Problem nicht, weil das Modell austrainiert ist und nicht anhand der Eingaben dazulernt.
- Wer kann auf diese internen Informationen zugreifen?

Manchmal trifft es die Richtigen

»Auf dem Rechner des Angeklagten fanden sich klare Hinweise. So benutzte er – das zeigen die Daten aus seinem Firefox-Browser – mehrfach den Google-Übersetzer, kurz nachdem der Nutzer „Fancy“ [...] im Netz auf Englisch angesprochen worden war. Der entsprechende Satz war eins zu eins in den Übersetzer übertragen worden. Auch Antworten wurden offenbar mit dem Übersetzungsdienst erzeugt.«

Die Grenzen generativer KI

- Die KI kann gut
  - Plakate malen (sofern sie keine Schrift enthalten sollen)
  - Lieder komponieren
  - Prosatexte schreiben
- Die KI kann schlecht
  - Ungewöhnliche Inhalte schaffen
  - Fakten verlässlich wiedergeben
  - Auf schlurige Angaben hin das passende Programm schreiben

Greift die DSGVO bei fabulierender KI?

- Der Fall: „Der Journalist Martin Bernklau ist Opfer des KI-Chats Copilot geworden. Die Künstliche Intelligenz von Microsoft macht aus dem unbescholtenen Tübinger einen Kinderschänder.“ (SWR aktuell vom 16.8.2024 15:15 Uhr)
- Die Probleme:
  - In einem LLM ist kein Datensatz gespeichert, in dem die Falschaussage explizit steht. Sie ergibt sich aus den gespeicherten Gewichtungen und kann zudem bei jeder erneuten Frage anders aussehen.
  - Die Falschaussage lässt sich schwer wegtrainieren. Sie lässt sich allenfalls wegfiltern, ist also weiterhin im System und wird nur nicht ausgegeben.
- Eine KI ist keine Suchmaschine, auch wenn Google das Gegenteil behauptet.

Messenger

- Überraschung: Es gibt noch andere Messenger außer Whatsapp.
- Whatsapp wirft datenschutzrechtliche Fragen auf.
- Die anderen Messenger (z.B. Telegram) aber auch.
- Die meisten Messenger (z.B. Signal, Threema, Wire) hängen an einem zentralen Anbieter.
- Einige(!) Ausnahmen: Element (Matrix), Conversations (XMPP), Briar (Tor), Deltachat (Mail), doch das ändert wenig an den rechtlichen Fragen.

Was heißt hier „sicher“?

- Golem 31.1.2019: Azure löscht aus Versehen Datenbanken von Kunden
- Heise 31.1.2019: Störung in Microsofts Cloud führt zu Datenbankverlusten bei Azure
- Heise 18.12.2021: Google scannt Cloud-Dateien nach rechtswidrigen und schädlichen Inhalten
- Borncity 31.12.2021: Microsoft Kontensperre wegen OneDrive-Inhalte und aktivierter Staatsanwalt
- Heise 16.11.2022: Automatisierte Scans: Microsoft sperrt Kunden unangekündigt für immer aus
- Golem 15.11.2023: Hacker stehlen Signaturschlüssel - Microsoft vertuscht Cloud-Sicherheitslücken
- Heise 15.11.2023: Neues Outlook: Microsoft bezieht Stellung zur Übertragung von Zugangsdaten
- Futurezone 27.11.2023: Google-Drive-Daten verschwinden plötzlich aus Cloud-Speicher
- ERecht24 5.1.2024: „Google scannt hochgeladene Dokumente nach Informationen, Schlüsselwörtern und Bildern […]. Google gibt in Drive gespeicherte, personenbezogene Daten an Partnerunternehmen weiter […].“
- Golem 16.10.2024: Microsoft warnt Kunden vor Datenverlust beim Logging
- Heise 11.4.2024: Microsoft-Code und -Passwörter standen frei im Netz
- Hardwareluxx 14.5.2024: Google löscht unabsichtlich Daten eines Rentenfonds

Rechtliche Fallstricke

- Server oder Firma befinden sich in einem unsicheren Drittstaat.
  - CLOUD Act
  - FISA Act
  - DPF bietet vorerst Rechtssicherheit
- Unklar, in welchem Land sich die Daten physisch befinden
- Fehlender Vertrag zur Datenverarbeitung im Auftrag (Art 28 DSGVO)
- Bei sensiblen Daten: fehlende Datenschutzfolgenabschätzung (Art 35 DSGVO, im Beschäftigungsverhältnis iVm § 26(3) BDSG)

Apropos mitlesen

Die Chatkontrolle wird Ende-zu-Ende-Verschlüsselung faktisch aushebeln, indem sie auf dem sendenden Endgerät Daten vor der Verschlüsselung zur Analyse ausleitet.

Was heißt das fürs Betriebsratsbüro?

§ 79a BetrVG

Bei der Verarbeitung personenbezogener Daten hat der Betriebsrat die Vorschriften über den Datenschutz einzuhalten. Soweit der Betriebsrat zur Erfüllung der in seiner Zuständigkeit liegenden Aufgaben personenbezogene Daten verarbeitet, ist der **Arbeitgeber** der für die Verarbeitung **Verantwortliche** im Sinne der datenschutzrechtlichen Vorschriften. Arbeitgeber und Betriebsrat unterstützen sich gegenseitig bei der Einhaltung der datenschutzrechtlichen Vorschriften. Die oder der Datenschutzbeauftragte ist gegenüber dem Arbeitgeber zur Verschwiegenheit verpflichtet über Informationen, die Rückschlüsse auf den Meinungsbildungsprozess des Betriebsrats zulassen. § 6 Absatz 5 Satz 2, § 38 Absatz 2 des Bundesdatenschutzgesetzes gelten auch im Hinblick auf das Verhältnis der oder des Datenschutzbeauftragten zum Arbeitgeber.

§ 6 (4) BDSG

(4) Die Abberufung der oder des Datenschutzbeauftragten ist nur in entsprechender Anwendung des § 626 des Bürgerlichen Gesetzbuchs zulässig. Die Kündigung des Arbeitsverhältnisses ist unzulässig, es sei denn, dass Tatsachen vorliegen, welche die öffentliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigen. Nach dem Ende der Tätigkeit als Datenschutzbeauftragte oder als Datenschutzbeauftragter ist die Kündigung des Arbeitsverhältnisses innerhalb eines Jahres unzulässig, es sei denn, dass die öffentliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigt ist.

§ 6 (5) Satz 2 BDSG

(5) Betroffene Personen können die Datenschutzbeauftragte oder den Datenschutzbeauftragten zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß der Verordnung (EU) 2016/679, diesem Gesetz sowie anderen Rechtsvorschriften über den Datenschutz im Zusammenhang stehenden Fragen zu Rate ziehen. Die oder der Datenschutzbeauftragte ist zur Verschwiegenheit über die Identität der betroffenen Person sowie über Umstände, die Rückschlüsse auf die betroffene Person zulassen, verpflichtet, soweit sie oder er nicht davon durch die betroffene Person befreit wird.

§ 6 (6) BDSG

(6) Wenn die oder der Datenschutzbeauftragte bei ihrer oder seiner Tätigkeit Kenntnis von Daten erhält, für die der Leitung oder einer bei der öffentlichen Stelle beschäftigten Person aus beruflichen Gründen ein Zeugnisverweigerungsrecht zusteht, steht dieses Recht auch der oder dem Datenschutzbeauftragten und den ihr oder ihm unterstellten Beschäftigten zu. Über die Ausübung dieses Rechts entscheidet die Person, der das Zeugnisverweigerungsrecht aus beruflichen Gründen zusteht, es sei denn, dass diese Entscheidung in absehbarer Zeit nicht herbeigeführt werden kann. Soweit das Zeugnisverweigerungsrecht der oder des Datenschutzbeauftragten reicht, unterliegen ihre oder seine Akten und andere Dokumente einem Beschlagnahmeverbot.

§ 38 BDSG

§ 38 Datenschutzbeauftragte nichtöffentlicher Stellen

(1) Ergänzend zu Artikel 37 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679 benennen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit sie in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Nehmen der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vor, die einer Datenschutz-Folgenabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 unterliegen, oder verarbeiten sie personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung, haben sie unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen.

(2) § 6 Absatz 4, 5 Satz 2 und Absatz 6 finden Anwendung, § 6 Absatz 4 jedoch nur, wenn die Benennung einer oder eines Datenschutzbeauftragten verpflichtend ist.

Was heißt das?

- Sind Betriebsräte verantwortliche Stellen?
  - Nein
- Brauchen Betriebsräte eigene Datenschutzbeauftragte?
  - Nein, die betriebliche Datenschutzbeauftragte reicht aus, aber es ist sinnvoll, eine für Datenschutzfragen Zuständige zu benennen.
- Muss der Betriebsrat ein Verarbeitungsverzeichnis (VVT) führen?
  - Nein, aber er muss die nötigen Informationen dafür liefern, was aufs Gleiche hinausläuft.

Schlussfolgerung der Geschäftsführung

„Wenn wir für die Einhaltung des Datenschutzes verantwortlich sind, dürfen wir dem Betriebsrat auch Anweisungen geben.“

Die Situation

- Der Betriebsrat nutzt die dienstliche Infrastruktur, insbesondere Fileshare, Chat, WWW und Mail.
- Die Geschäftsführung kann jederzeit auf die Datenbestände und Kommunikation des Betriebsrats zugreifen.
- Vorschläge, diesem Mangel abzuhelfen, werden mit Verweis auf die exorbitanten Kosten abgelehnt (immerhin müssen die Indienflüge der Geschäftsführung bezahlt werden).
- Mitbestimmung in der IT geschieht nach Aktenlage
- Datenschutzanfragen werden über Jahre verschleppt und mitunter auch falsch beantwortet – beweist uns erst einmal das Gegenteil.
- Adminoberflächen werden im Rahmen einer Videokonferenz in Windeseile vorgestellt. Eine tiefere Analyse möglicherweise kritischer Funktionen findet aus Zeitgründen nicht statt.

Mögliche Auswege

- Zusätzliche Verschlüsselungsebenen einziehen (EncFS, Veracrypt, Cryptomator)
  - Zusatzaufwand
  - Komforteinbußen
  - Widerstand der Firmen-IT und der Geschäftsführung
- Eigene Infrastruktur betreiben
  - Probleme siehe oben
  - Wer soll das verantwortungsvoll betreiben?

Cookiebanner in Unternehmen

- Informierte Freiwilligkeit ist im Vorgesetzten-Angestellten-Verhältnis nur sehr selten gegeben (§ 26(2) BDSG). Ich kann nicht freiwillig den Datenverarbeitungsvorgängen einer Anwendung zustimmen, zu deren Nutzung ich durch Weisung gezwungen bin.
- „Allem zustimmen oder keine Nutzung“ ist in diesem Kontext ebenfalls fragwürdig.
- Englische Cookiebanner bei deutscher Unternehmenssprache widersprechen dem Transparenzgebot (Art 7(2), Art 12(1) DSGVO).

Cookiebanner in Unternehmen

- Phrasen wie „durch die Nutzung stimmen Sie zu“ sind unwirksam. Schweigendes Einverständnis gibt es im Datenschutz nur unter engen Voraussetzungen.
- Seitenlange Cookiebanner im Fachjargon entsprechen meiner Ansicht nach nicht dem Transparenzgebot (Art 7(2), Art 12(1) DSGVO).
- Dutzende Genehmigungen im „berechtigten Interesse“ (Art 6(1)f DSGVO) zu verstecken ist rechtlich fragwürdig.
- Zum Ablehnen muss wie für die Zustimmung ein einziger Mausklick ausreichen (Art 7(3) DSGVO).

Microsoft 365

- Artikel 28 DSGVO legt die Kriterien für Auftragsverarbeitung fest.
- 2022: Die Datenschutzkonferenz spricht sich ablehnend zu einem Einsatz im öffentlichen Dienst aus.
- 2024: Der LfDI Niedersachsen hält den Einsatz von Teams in der Landesverwaltung für möglich.
- Gute Zusammenfassung bei Dr. Datenschutz:
  Datenschutz & Microsoft 365: DSGVO-konformer Einsatz möglich?

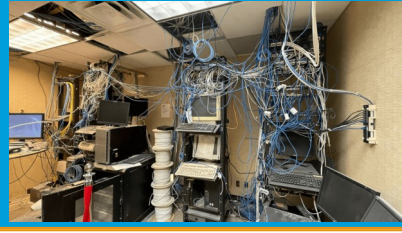
Vorschläge von Dr. Datenschutz

- Betrieb „on premise“ oder zumindest in der EU
- Übertragung der Diagnose- und Telemetriedaten weitgehend unterbinden
- Personenbezogene Telemetriedaten auf der Firewall filtern
- Pseudonyme dienstliche Mailadressen, keine privaten Microsoft-Accounts
- Auf Datensparsamkeit optimierte Browser
- Metadaten durch Terminal-Clients anonymisieren
- Inhaltsverschlüsselung

Weitere Vorschläge von Dr. Datenschutz

- Speicherung der Vertragstexte
- Einbeziehung des Betriebsrats
- Etablierung eines hinreichenden Berechtigungskonzepts
- Sicherstellung der Löschung von Daten im Rahmen der Nutzung von MS 365
- Führung eines Verarbeitungsverzeichnisses gemäß Art. 30 DSGVO
- Bereitstellung von Informationsblättern für Beschäftigte und Kunden gemäß Art. 12, 13 DSGVO

Dann doch lieber selber hosten?



- Cloud und Selbsthosten sind nicht Alternativen, sondern Ergänzungen.
- Es ist immer gut, ein Backup zu haben.
- Nobody wants backup, everybody wants restore.
- Selbsthosten löst die Frage der Datenverarbeitung im Auftrag, wirft aber die Frage auf, ob, wie und vor allem von wem Server in Eigenregie rechtssicher betrieben werden können.
- Selbsthosten eines vertrauensunwürdigen Dienstes ändert vielleicht rechtlich etwas, nicht aber technisch.

Videokonferenzsysteme: Jitsi

- Open Source, kann auf eigener (leistungsfähiger!) Hardware betrieben werden.
- Ende-zu-Ende-verschlüsselt
- Arbeitet nur bei relativ kleinen Konferenzen (ca. 20) noch flüssig.

Videokonferenzen: Big Blue Button

- Open Source, browserbasiert, kann auf eigener (leistungsfähiger!) Hardware betrieben werden.
- Optimiert für Vortragssituationen
- Auch größere Konferenzen noch flüssig (getestet bei 80 bis über 100 Clients)
- Haklige Installation und Pflege
- Nur auf dem Transportweg verschlüsselt
- Mitschnitte können nur serverweit aktiviert oder deaktiviert werden. Alles Andere sind nur Anfangs- und Endmarkierungen bestehender Komplettaufzeichnungen, die irgendwann in der Zukunft vielleicht gelöscht werden. Das kann datenschutzrechtlich bedenklich sein.

Rechtliche Fallstricke bei Online-Besprechungen

- Das nicht-öffentlich gesprochene Wort darf nicht ohne ausdrückliche Einwilligung der Betroffenen nicht aufgezeichnet werden (§ 201 StGB).
- Wo läuft die Grenze zwischen einer nicht-öffentlichen Besprechung und einer großen Veranstaltung, in der die Teilnahme zwingend mit der Aufzeichnung verbunden ist?

Fazit

- Cloud oder Selbsthosten sind kein Entweder-Oder
- Abwägung zwischen Eigen- und Fremdverantwortung, zwischen Kontrolle behalten und abgeben
- Die Vorherrschaft der Quasi-Monopole ist kein Naturgesetz
- Es ist sowohl politisch als auch technisch und wirtschaftlich sinnvoll, mehrere Optionen zu haben – oder sich zu schaffen.

Weitere Informationen

- Auslegungssache 118: Datenschutz-Minenfeld Microsoft 365?
- DSGVO-Linkliste, Unterpunkt MS 365

Dann doch lieber selber hosten?