Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

Microsoft 365 aus Sicht einer Aufsichtsbehörde

Datenschutz und Drittlandübermittlung

Alvar C.H. Freude, Leiter der Abteilung 5 für technisch-organisatorischen Datenschutz und Datensicherheit beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg


Kann Microsoft 365
datenschutzkonform
eingesetzt werden?

Landesbeauftragter für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

Die richtige Antwort ist immer …

Landesbeauftragter für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

Die richtige Antwort ist immer …

Es kommt drauf an!

Landesbeauftragter für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

Wer ist der Verantwortliche?

Landesbeauftragter für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

Wer ist der Verantwortliche?

Der Verantwortliche ist der Verantwortliche im Sinne von Artikel 4 Nr. 7 DS-GVO

Häää?

Artikel 4 Nr. 7 DS-GVO:

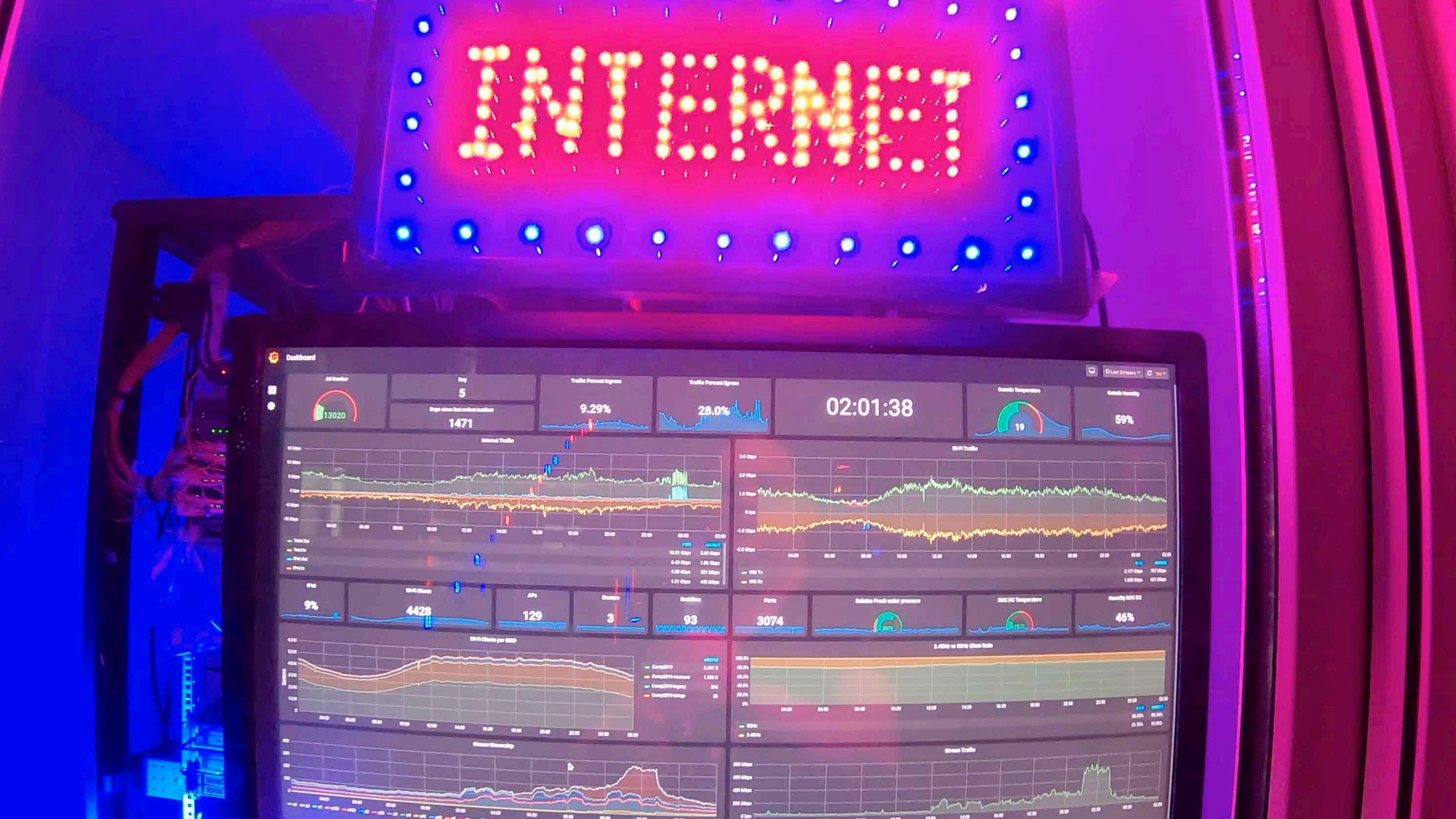
„Verantwortlicher“ [ist] die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet

Artikel 4 Nr. 7 DS-GVO:

„Verantwortlicher“ [ist] die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen **über die Zwecke und Mittel der Verarbeitung** von personenbezogenen Daten **entscheidet**

Verantwortlicher ist z.B.:

- Das Unternehmen oder die Behörde, die eine Software einsetzt
- Der Dienstebetreiber, der betroffenen Personen einen Dienst anbietet


INTERNET
Dashboard
13020
5
1471
9.29%
28.0%
02:01:38
19
59%
9%
4428
129
3
93
3074
46%

u.a. wurde seitens des LfDI geprüft …

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

- ob die in der DSFA des Ministeriums vorgeschlagenen Abhilfemaßnahmen zur Minimierung des Risikos tatsächlich umgesetzt wurden und ausreichend sind;
- welche Verarbeitungen abseits der von den Nutzern gewünschten/angeforderten stattfinden (in Stichproben);
- ob der Funktionsumfang ausreichend ist und den Erwartungen der Lehrkräfte entspricht;
- ob die als deaktiviert geltenden problematischen Verarbeitungen auch deaktiviert sind, z.B. solche, die in den USA verarbeitet werden oder bei denen MS personenbezogene Daten zu eigenen Zwecken verarbeitet wie Übersetzungs- und Diktatfunktion;
- ob durch Verschlüsselung die Möglichkeiten des Zugriffs seitens Microsoft oder von erfolgreichen Angreifern auf Daten eingeschränkt werden konnten.

Ergebnis der Beratung

- LfDI hat wegen zahlreicher Risiken vom Einsatz im Rahmen der digitalen Bildungsplattform abgeraten, u.a. wegen:
- Herausforderungen beim Einsatz bei Schülern
- Teilweise fehlende Rechtsgrundlage, vor allem für die Verarbeitung seitens MS zu eigenen Zwecken
- Fehlende Transparenz (keine vollständige Übersicht über alle Verarbeitungen) (vgl. Rechenschaftspflicht)
- Risiko durch US-Transfers

Ergebnis der Beratung

- LfDI hat wegen zahlreicher Risiken vom Einsatz im Rahmen der digitalen Bildungsplattform abgeraten, u.a. wegen:
- Herausforderungen beim Einsatz bei Schülern
- Teilweise fehlende Rechtsgrundlage, vor allem für die Verarbeitung seitens MS zu eigenen Zwecken
- Fehlende Transparenz (keine vollständige Übersicht über alle Verarbeitungen) (vgl. Rechenschaftspflicht)
- Risiko durch US-Transfers

Umfangreiche technische Analyse:

- Bei Prüfung wurden über 500 verschiedene Microsoft-Server kontaktiert
- z.B. sehr detaillierte Telemetrie- und Diagnosedaten
  - Office.Word.Online.NonUser.RightArrow, Office.Word.Online.UserAction.Typing, Office.Word.Online.UserAction.Backspace, Office.Word.Online.UserAction.Undo, office_excel_online_useraction_copy, …
- Schwer für Verantwortliche, Rechenschaftspflicht aus Art. 5 Abs. 2 DS-GVO einzuhalten

Host (FQDN)	Subdomain	Anzahl Requests	Host in Liste der Verarbeitungen genannt?
login.windows.net	login.windows.net	143	NEIN
fs.microsoft.com	fs.microsoft.com	141	Ja
go.trouter.teams.microsoft.com	teams.microsoft.com	140	Ja
dc.services.visualstudio.com	services.visualstudio.com	140	NEIN
c.s-microsoft.com	c.s-microsoft.com	138	NEIN
c1-officeapps-15.cdn.office.net	cdn.office.net	135	Ja
main.iam.ad.ext.azure.com	ext.azure.com	128	NEIN
augloop.office.com	augloop.office.com	127	NEIN
api.interfaces.records.teams.microsoft.com	teams.microsoft.com	119	NEIN
emea.api.flow.microsoft.com	flow.microsoft.com	119	NEIN
upload.fp.measure.office.com	measure.office.com	110	NEIN
c1-word-view-15.cdn.office.net	cdn.office.net	107	Ja
mysignins.microsoft.com	mysignins.microsoft.com	104	NEIN
c3-powerpoint-15.cdn.office.net	cdn.office.net	97	Ja
eur.delve.office.com	delve.office.com	96	NEIN
loki.delve.office.com	delve.office.com	95	NEIN
francecentral-prod.notifications.teams.microsoft.com	teams.microsoft.com	93	NEIN
static2.sharepointonline.com	static2.sharepointonline.com	91	NEIN
emea.flow.microsoft.com	flow.microsoft.com	91	NEIN
api.myaccount.microsoft.com	myaccount.microsoft.com	90	NEIN

Ereignis-Name bzw. Endpunkt	Anzahl
Office.Docs.SharedComments.SharedCommentsUILazyLoad	176
Office.Word.Online.UserAction.ShowFloatie	175
Office.AugLoop.Client.WebSocketWorker	173
Office.AugLoop.Client.ProcessMessage	170
Office.Word.Online.UserAction.ReportTabSwitch	164
Office.Word.Online.UserAction.TabSwitch	164
Office.Word.Online.UserAction.	137
Office.Insights.SmartLookup.ResponseFromService	128
Office.Word.Online.NonUser.LeftArrow	123
Office.Word.Online.UserAction.KeyboardSelectBlock	116
Office.TellMe.TellMeWAC.Events	116
Office.Word.Online.UserAction.TouchRevertPictureGripSize	115
Office.Word.Online.Health.Kpi.BootPerf	110
Office.AugLoop.Client.TryToConnectAndInitializeSession	108
Office.Word.Online.Health.Kpi.GetCloudPolicySettings	108
Office.AugLoop.Client.SessionInit	108
Office.Word.Online.Health.Kpi.AFHSLicensingSuccessfulRequest	108
Office.Online.SessionStart	107
Office.Online.SessionEnd	105
Office.Word.Online.UserAction.Undo	104
Office.Word.Online.Health.Kpi.WordClpReadPolicy	104
Office.Word.Online.NonUser.RightArrow	97
Office.Docs.SharedComments.ApplyCommentChangesAction	95
Office.Insights.SmartLookup.SendActionToPane	95
Office.Word.Online.UserAction.MenuOpen	95
Office.Word.Online.NonUser.RetrieveAddInCommandsEntitlementsList	94
Office.AugLoop.Client.InitRuntime	90
Office.Docs.SharedComments.ResolveAtMentionCapabilityState	88

Wer hat die Kontrolle?

Ausschnitt:
Seite 21, Abschließende Bemerkungen

Es sind viele, nicht kontrollierbare Datenflüsse zu Microsoft festzustellen. Microsoft hat den Gesamtprozess des KM zwar konstruktiv unterstützt, auf Nachfragen zu kritischen Punkten bzw. Datenflüssen aber **nicht ausreichend Auskunft erteilen und Klarheit schaffen können.** Die Kenntnis über die stattfindenden Verarbeitungen ist nach der DS-GVO aber Voraussetzung dafür, dass der Verantwortliche seinen Pflichten nach Art. 5 Abs. 2 DS-GVO nachkommen kann: Er ist für die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Datenverantwortlich und muss dies auch nachweisen können (Rechenschaftspflicht).

Trotz umfangreicher Bemühungen seitens des LfDI auch im direkten Gespräch mit hochrangigen Vertretern von Microsoft war es nicht möglich, eine vollständige Übersicht über alle Verarbeitungen personenbezogener Daten (auch zu eigenen Zwecken seitens Microsofts) zu erhalten. Wenn es trotz großer Anstrengungen, hohem Personaleinsatz und Zugang zu versierten Microsoft-Technikern im Rahmen des Pilotbetriebs selbst dem Kultusministerium mit intensiver Unterstützung des LfDI nicht gelungen ist, eine hinreichende Klarheit über Datenflüsse, Rechtsgrundlagen und technische Maßnahmen des Anbieters zu erlangen, so **ist es schwer vorstellbar, dass einzelnen Schulen dieses besser gelingt**. Da die Schulen jedoch Verantwortliche für die Verarbeitungen von Schülerdaten sind und insoweit eine Garantenstellung einnehmen, liegt hier ein ungelöstes Datenschutzproblem im Sinne von Artikel 5 Absatz 2 DS-GVO vor.

Kann Microsoft 365 datenschutzkonform eingesetzt werden?

Landesbeauftragter für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

Die richtige Antwort ist immer …

Es kommt drauf an!

Grundlegende Voraussetzungen (Art. 5 Abs. 1 DS-GVO)

a) Rechtmäßigkeit, für betroffene Person nachvollziehbar
b) Nur für festgelegte, eindeutige und legitime Zwecke
c) Angemessen und auf das notwenige Maß beschränkt
d) Richtigkeit
e) Nur so lange wie erforderlich
f) Angemessene Sicherheit

Rechenschaftspflicht (Art. 5 Abs. 2 DS-GVO)

- „Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können“

- Der Verantwortliche!

Hinweise bzgl. E-Mail-Hosting

- Der Anbieter speichert und verarbeitet auch alle E-Mails auf seinen Servern
- Im Klartext
- Kommunikationsdaten!
- Ende zu Ende Verschlüsselung könnte (teilweise) helfen, aber wenig verbreitet

Beschäftigtendatenschutz

- Diverse Herausforderungen bei der Konfiguration
- Mitarbeiterüberwachung?
- Diverse Analysefunktionen
  - z.B. Leistungskontrolle, Produktivität
  - Office Graph, MyAnalytics, Workplace Analytics, Delve
- Jeweils Rechtsgrundlagen?

Analysen und Berichte

Analysen und Berichte helfen Ihnen dabei, unterschiedliche Typen von Berichten zu erstellen, um Erkenntnisse und Informationen über die Teams-Verwendung zu erhalten. Diese Berichte helfen Ihnen beim besseren Verständnis von Verwendungsmustern, sodass Sie bessere geschäftliche Entscheidungen treffen können. Weitere Informationen

Berichte anzeigen | Downloads

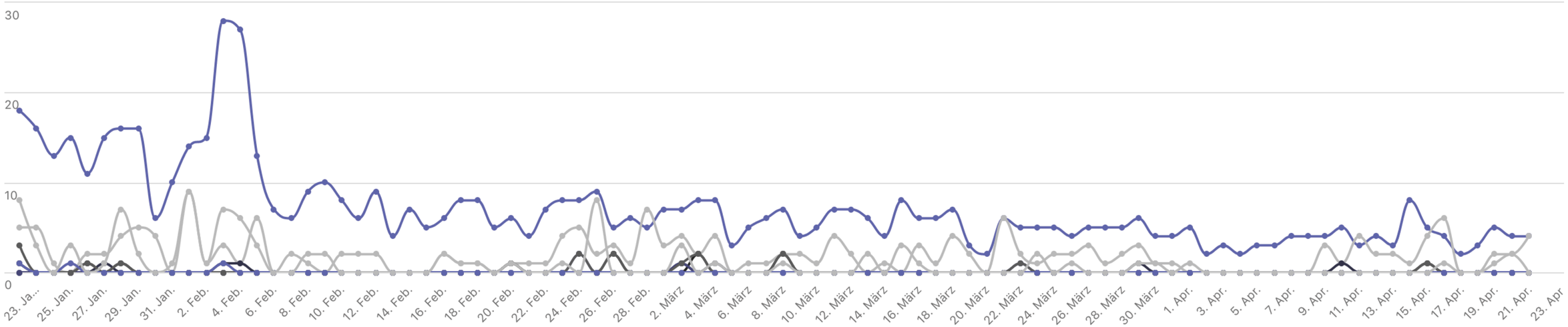
Bericht: Teams-Nutzung

Datumsbereich: Letzte 90 Tage

Bericht a...

Teams-Nutzungsbericht

22. Apr. 2021 20:55:53 UTC | Datumsbereich: **22. Jan. 2021** - **21. Apr. 2021**



112	70	1	11	4	17	3	90
Aktive Benutzer gesamt	Aktive Kanäle	Gäste	Antwortnachrichten	Beitragsnachrichten	Kanalnachrichten	Reaktionen	Besprechungen organisiert

MS Office, lokale Installation

- Einfacher zu kontrollieren, aber Konfiguration nötig!
  - z.B. Deaktivierung und Sperrung von Telemetrie- und Diagnosedaten
- Vorsicht bei einzelnen Komponenten wie Outlook iOS/Android:
  - Daten gehen stets über Microsoft Server, liegen dort im Klartext vor; Passwörter werden bei MS im Klartext gespeichert!

Festgestelltes Verhalten:

Nach Eingabe der erforderlichen Daten (Username, Passwort etc.) verbindet sich nicht die App direkt sondern ein Microsoft-Server mit dem konfigurierten E-Mail-Server, wie aus den Protokolldateien des Servers ersichtlich ist:

```
Aug 28 11:07:56 cyrus imaps[68216]: login: [52.125.140.74] lft2 LOGIN+TLS User
logged in SESSIONID=<mail.a-blast.org-68216-1598605676-1-7251846154066095578>


[...]
Aug 28 11:12:39 cyrus imaps[75933]: login: [52.125.138.94] lft2 LOGIN+TLS User
logged in SESSIONID=<mail.a-blast.org-75933-1598605959-1-1865504613446843484>
```

Die IP-Adresse 52.125.141.94 ist Microsoft zuzuordnen, siehe Anlage 1 (Auszug aus dem Whois).

Zu späteren Zeitpunkten erfolgen weitere Zugriffe von Microsoft-Servern:

```
Aug 28 13:40:18 cyrus imaps[88817]: login: [52.125.138.94] lft2 LOGIN+TLS User
logged in SESSIONID=<mail.a-blast.org-88817-1598614817-1-10708460015531101292>
Aug 28 13:40:18 cyrus imaps[87882]: login: [52.125.138.94] lft2 LOGIN+TLS User
logged in SESSIONID=<mail.a-blast.org-87882-1598614818-1-8872240340624646673>
```

Auch beim Versenden erfolgt der Versand über Microsoft-Server (Ausschnitt aus dem Protokoll des SMTP-Servers):

```
Aug 28 11:08:49 exim exim[75221]: no host name found for IP address 52.125.140.74
Aug 28 11:08:49 exim exim[75221]: 1kBaNN-000JZF-ET <= lft2@mte.lfdibw.de
H=(mail.outlook.com) [52.125.140.74]:36622 P=esmtpsa L- X=TLS1.2:ECDHE-RSA-AES256-
SHA384:256 CV=no SNI="mail.a-blast.org" A=sasl_login:lft2 S=1242 M8S=0 RT=0.161s
id=5EADD75739850053.400b0a2c-3232-458a-85c4-4b71ab5a11a9@mail.outlook.com from
<lft2@mte.lfdibw.de> for Freude@lfdi.bwl.de
Aug 28 11:13:49 exim exim[75221]: SMTP command timeout on TLS connection from
(mail.outlook.com) [52.125.140.74]:36622
```

Ausschnitte: Anlage 3 - Analyse Outlook Android und iOS via IMAP und SMTP.pdf, Seite 2 f.

Landesbeauftragter für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

Internationaler Datentransfer

Kapitel 5 DS-GVO

Landesbeauftragter für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

Internationaler Datentransfer

Warum problematisch?

EU-U.S. Safe Harbor (Oktober 2015)

- EuGH Entscheidung Schrems I
  - nationales U.S.-Recht schränkt Datenschutz ein
  - insbesondere: Zugang U.S.-Behörden wegen „nationaler Sicherheit“
  - kein mit EU vergleichbares Schutzniveau
  - keine justiziablen Rechte für Betroffene
- **=> ungültig**

EU-U.S. Privacy Shield (Juli 2016)

- EuGH Entscheidung Schrems I
  - nationales U.S.-Recht schränkt Datenschutz ein
  - insbesondere: Zugang U.S.-Behörden wegen „nationaler Sicherheit“
  - kein mit EU vergleichbares Schutzniveau
  - keine justiziablen Rechte für Betroffene
- **=> ungültig**

Neue Standardvertragsklauseln, „zusätzliche Garantien“

- Information des Betroffenen über Datenanforderung durch Behörde
- Beschreiten des Rechtswegs gegen Datenanforderung
- Entschädigungsklausel zu Lasten des Datenimporteurs

- Microsoft bewegt sich!

Zusätzliche Maßnahmen notwendig

- Konfiguration, z.B. Customer Lockbox
- Haupt-Standort der Server
  - Aber: Es kommt auf Ort des Zugriffs, nicht auf Speicherort an!
- Vertragliche Regelungen
- Technische Maßnamen
  - Insbesondere Verschlüsselung
- Ausschluss bestimmter Daten

Verschlüsselung?

Landesbeauftragter für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

Fazit


Kann Microsoft 365
datenschutzkonform
eingesetzt werden?

Landesbeauftragter für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

Die richtige Antwort ist immer …

Es kommt drauf an!

Vielen Dank für Ihre Aufmerksamkeit!

Fragen?

LfDI Baden-Württemberg
https://www.baden-wuerttemberg.datenschutz.de/
poststelle@lfdi.bwl.de