Sind MS-365 und Teams in Schulen datenschutzkonform?

Category: Blog
geschrieben von Ralf Lankau | 14. September 2022

Prof. Dr. phil. Ralf Lankau: US-Recht bricht EU-Recht.

Der datenschutzkonforme Einsatz von US-Software in Europa ist laut Urteil des Europäischen Gerichtshofs (EuGH; Schrems II) nicht möglich. Der Grund dafür ist, „dass das von der EU-Kommission mit den USA ausgehandelte Privacy Shield-Abkommen EU-Bürger nicht wirksam davor schützt, dass US-Geheimdienste anlasslos, zeitlich unbegrenzt und ohne wirksame Zweckbindung Daten von Europäern bei als Dienstleistern fungierenden US-Unternehmen abgreifen können“ (LfDI 2022a). Dagegen wehrt sich Microsoft mit einer Stellungnahme, die allerdings von falschen Voraussetzungen ausgeht (Datenschützer würden besonders Microsoft kritisieren) und letztlich als Polemik (die EU-DSGVO sei technologiefeindlich) endet (Microsoft 2022).
Das Urteil des Europäischen Gerichtshofs richtet sich nicht gegen einzelne Unternehmen, sondern adressiert alle US-Unternehmen, die Software und/oder z.B. Clouddienste anbieten. Das betrifft Amazon Web Services (AWS) genauso wie Google- oder Microsoft-Clouddienste oder jede andere Software von US-Unternehmen. Denn sobald eine US-Behörde Daten von einem US-Unternehmen anfordert, muss diese personenbezogene Daten herausgeben, auch wenn die Daten in Europa gespeichert sind und durch dort geltende Verträge die Herausgabe von Daten „an sich“ untersagt ist. US-Recht bricht EU-Recht. Da Unternehmen und/oder Behörden in Deutschland oder Europa „Dienstleister wie Microsoft, Zoom und Co. nicht dazu bringen [können; rl], die Daten auf Servern in den EU-Mitgliedstaaten wirksam vor dem Zugriff der US-Behörden zu schützen, dürften sie diese Dienstleister nicht mehr nutzen“ (LfDI 2022a).

Richtig und falsch

Das bestreitet Microsoft auch gar nicht, sondern argumentiert informatisch binär mit „Richtig“ (Seite 1) und „Falsch“ (Seite 2 und 3) sowie mit Marketing-Phrasen, wenn es z.B. heißt „Microsoft bietet zukunftsweisende Technologien mit branchenführendem Sicherheitsstandard“ (1.1), „Microsoft ist ein zuverlässiger und verantwortungsbewusster Partner. Unser Unternehmensziel ist es, jede Person und jede Organisation zu befähigen, mehr zu erreichen.“ (1.2) oder “Microsoft ist im Bereich der Cybersecurity führend und hat eine Vielzahl technischer Maßnahmen implementiert, um Kundendaten vor Cyberattacken zu schützen.” (1.6). Das bestreitet niemand, ist aber nicht das Thema. (Die Zahlen nennen die Seite und den jeweiligen Unterpunkt.)

> *Das EuGH-Urteil bestätigt, dass Microsoft die Anforderungen des geltenden Datenschutzrechts nicht sicherstellen kann, weil jedes US-Unternehmen dem*

US-Recht unterworfen ist und Daten auf Anfrage herausgeben muss.

Entscheidend ist anderes. Unter Punkt 1.3 etwa steht bei Microsoft als “Richtig”, ist aber laut EuGH-Urteil falsch: “Alle Microsoft Produkte und Dienste können in der Privatwirtschaft und im öffentlichen Sektor (z.B. an Schulen) datenschutzkonform eingesetzt werden und sind auch selbst datenschutzkonform. Microsoft hält die Anforderungen des geltenden Datenschutzrechts ein.” Das EuGH-Urteil bestätigt, dass Microsoft genau das nicht sicherstellen kann, weil jedes US-Unternehmen dem US-Recht unterworfen ist und Daten auf Anfrage herausgeben muss. Es ist zwar richtig, dass Microsoft mehrmals dagegen geklagt und die Kunden nachträglich informiert hat (2.2). Aber die Daten wurden und werden an US-Behörden weitergereicht.

Europäische Dienstleister müssen sich überlegen, wie sie sich den US-Behörden und dem US-Recht entziehen können.

Spannend ist die Argumentation im nächsten Punkt (2.2), wenn es heißt: „Die pauschale Empfehlung seitens einzelner Behörden, nur Anbieter aus der EU zu nutzen, verkennt im Übrigen, dass auch Anbieter mit Stammsitz innerhalb der EU US-Überwachungsgesetzen unterliegen können, z.B. durch eine Präsenz in oder minimalen Kontakt mit den USA.“ Es stimmt, dass europäische Unternehmen mit Niederlassungen und/oder Kontakten mit den USA aus Sicht der US-Regierung ebenfalls dem US-Recht unterliegen und laut US-Jurisdiktion europäisches Recht nicht gilt. Das dürfte sehr viele EU-Unternehmen betreffen. Nur leuchtet die Logik von Microsoft nicht ein, als Lösung das Speichern von Daten „weitgehend regional in Rechenzentren in der EU“ anzubieten, „obwohl es keine gesetzliche Verpflichtung dazu gibt“. (1.5) Das nützt doch gar nichts, da US-Behörden überall Zugriff auf Daten haben. Europäische Dienstleister müssen sich überlegen, wie sie sich den US-Behörden und dem US-Recht entziehen können.

Ein Interesse von US-Behörden z.B. an Daten aus einem Schulunterricht in Deutschland kann nicht ernsthaft behauptet werden.

Welche Daten fliessen überhaupt ab, wer hat Zugriff darauf und wofür werden diese Daten genutzt?

Kein Interesse an Nutzerdaten?

Die Behörden hätten doch gar kein Interesse, heißt es im MS-Papier weiter. “Ein Interesse von US-Behörden z.B. an Daten aus einem Schulunterricht in Deutschland kann nicht ernsthaft behauptet werden.” (2.2) Eines der führenden IT-Unternehmen für Betriebssysteme und Office-Programme, behauptet, dass US-Behörden gar kein Interesse an Nutzerdaten hätten? Als bestünde nicht das gesamte Fundament der Daten-Ökonomie aus Nutzerdaten. In der US-Version von MS-Office sind z.B. Tools zur Workplace Surveillance (Arbeitsplatzüberwachung) integriert, die alle Aktionen der Mitarbeiter aufzeichnen. Für wen und zu welchem Zweck? (In Europa ist diese Funktion aus Rechtsgründen deaktiviert.) Arbeitet Microsoft als Unternehmen, das Software gezielt an Schulen vertreibt, nicht mit Learning Analytics, einer Technik, um personalisierte Daten erfassen und für individualisierte Angebote auswerten zu können? Das ist weltweit die Basis der Global Education Industrie (GEI), eines milliardenschweren Bildungs-Marktes, in dem Microsoft mit MS365, Teams und Clouddiensten aktiv ist. Der Einsatz dieser Software wurde in einigen Bundesländern untersagt, da bei Pilotinstallationen nicht geklärt werden konnte, welche Daten überhaupt abfließen, wer Zugriff darauf hat und wofür diese Daten genutzt werden (LfDI 2022b; Pagalski 2022; rnd 2022).

Die Aussage, dass es “keinen Anhaltspunkt dafür [gebe; rl], dass die US-Regierung §702 FISA nutzt, um (i) Industriespionage zu betreiben oder US-amerikanische wirtschaftliche Interessen zu verfolgen oder (ii) Regierungen im

Europäischen Wirtschaftsraum ins Visier zu nehmen“ widerspricht sowohl der Aufgabenbeschreibung der US-Dienste wie der Praxis, wenn man sich an die Abhörskandale „unter Freunden“ erinnert.

> *Mit Hilfe von Section 215 Patriot Act bzw. Section 501, 502 FISA könne “die Herausgabe jeglicher Unterlagen, inklusive Daten auf Servern, verlangt werden.”*

Patriot act: Der Staat kennt keine Grenzen mehr.

Man auch kann behaupten, dass die US-Regierung §702 FISA „im Wesentlichen zur Sammlung von Informationen für Ermittlungen zu schwerwiegenden Bedrohungen der nationalen Sicherheit, wie Terrorismus, Cybersecurity-Angriffe und Waffenproliferation“ nutzt. (2.2) Man sollte dann aber ergänzen, was der wissenschaftliche Dienst des Bundestages zu USA Patriot Act, USA Freedom Act, Cloud Act und Section FISA 207 schreibt. „Durch die weitreichenden Änderungen an FISA durch den Patriot Act wurden die zuvor ohnehin nach FISA bestehenden Eingriffsmöglichkeiten stark ausgeweitet. (WD 2020, 1) Section 702 FISA diene „der Überwachung von Nicht-US-Bürgern, die sich außerhalb des US-Territoriums aufhalten. Danach dürfte alle elektronische Kommunikation von und zu der Zielperson sowie über die Zielperson abgefangen werden.“
Mit Hilfe von Section 215 Patriot Act bzw. Section 501, 502 FISA könne “die Herausgabe jeglicher Unterlagen, inklusive Daten auf Servern, verlangt werden.” (ebda S. 6) Wie üblich bei Geheimdiensten weiß man nicht, was davon bereits praktiziert wird. Alles nur zu wessen Bestem? Interessant ist auch die Aussage, dass Diagnosedaten notwendig seien, um Produkte und Dienste sicher und stabil zu betreiben, um die Anfälligkeit für Fehler und die Wahrscheinlichkeit von Sicherheitsrisiken zu verringern. (3.4)

> *Es ist höchste Zeit, dass die europäischen Länder eine eigene Infrastruktur aufbauen und digital souverän werden.*

Das mag man so sehen, aber warum sind dann Umfang und Inhalt dieser Diagnosedaten intransparent statt öffentlich? Auch die Aussage „Die technische Verbindung zwischen Nutzer und Microsoft (z.B. über Server und Rechenzentren) ist in vielen Fällen zwingende Voraussetzung für die vertraglich geschuldete Diensterbringung. Nichts davon kann als ein Ausspähen von Kunden angesehen werden." (5.3) träfe nur zu, wenn klar belegt wäre, welche Daten für welche Zweck übertragen, gespeichert, ausgewertet und nach dem Einsatz auch wieder gelöscht werden. Zu fragen ist zudem, nicht nur für Bildungseinrichtungen, welche Dienste überhaupt in der Cloud gespeichert werden sollten und was man – schon als Schutz vor immer umfangreicheren Angriffen aus dem Netz – besser lokal installiert und verwaltet. Cloud-Computing ist zwar ein profitables Geschäftsfeld der IT, schafft aber mindestens so viele Probleme wie es Lösungen anbietet, wenn man die Jahresberichte des Bundesamtes für Sicherheit in der Informationstechnik (BIS) studiert.

> *Dann bleibt es immer noch schwierig genug, sich gegen die massiven Angriffe aus dem Netz zur Wehr zu setzen, aber anders als von Microsoft behauptet, sind die dafür notwendigen Strukturen nicht Zentralisierung, sondern Datensparsamkeit, Dezentralisierung, Transparenz der Algorithmen und Separierung der Nutzer in geschützte und geschlossene Teil- und Unternetze (Edge-Computing).*

Zum Ende wird das Microsoft-Papier polemisch. „Eine Analyse jedes einzelnen Prozesses eines Diensts durch den Verantwortlichen/Nutzer ist datenschutzrechtlich weder erforderlich noch geboten und geht weit über die Rechenschaftspflichten unter Art. 5 DSGVO hinaus", heißt es zum Schluss, das „Errichten solcher Hürden" sei „unrealistisch und technologiefeindlich". Hier wird versucht, technischen Fortschritt, der als positiv nur behauptet wird, gegen demokratische Strukturen und Grundrechte der Menschen (informationelles Selbstbestimmungsrecht, Privatsphäre) auszuspielen. Umgekehrt wird ein Schuh daraus: Demokratische Rechtsstaaten und z.B. die EU legen juristisch fest, welche Daten erhoben und ausgewertet werden dürfen, Unternehmen haben sich danach zu richten. Grundrechte sind wichtiger als technische Möglichkeiten und

Geschäftsmodelle. Wenn US-Unternehmen die Einhaltung dieser Rechtsgrundlagen nicht gewährleisten können, weil die US-Regierung EU-Recht außer Kraft setzt, dürfen US-Dienste in der EU nicht genutzt werden. Das ist die Logik von Rechtsstaatlichkeit. Daher ist es höchste Zeit, dass die europäischen Länder eine eigene Infrastruktur aufbauen und digital souverän werden.

> *Intelligent und ehrlich wäre, wenn Unternehmen wie Microsoft deutlich machen würden, dass auch sie der Paranoia der US-Regierung nach 9/11 unterliegen, nach der die mehr als 30 US-Dienste auf alle nur erdenklichen Daten zugreifen, wie es Edward Snowden öffentlich gemacht hat.*

Dann bleibt es immer noch schwierig genug, sich gegen die massiven Angriffe aus dem Netz zur Wehr zu setzen, aber anders als von Microsoft behauptet, sind die dafür notwendigen Strukturen nicht Zentralisierung, sondern Datensparsamkeit, Dezentralisierung, Transparenz der Algorithmen und Separierung der Nutzer in geschützte und geschlossene Teil- und Unternetze (Edge-Computing). Die digital vernetzte technische Infrastruktur ist schon heute, neben, Land, Wasser und Luft das vierte Schlachtfeld für Konflikte, angegriffen wird die Zivilbevölkerung.

Intelligent und ehrlich wäre, wenn Unternehmen wie Microsoft deutlich machen würden, dass auch sie der Paranoia der US-Regierung nach 9/11 unterliegen, nach der die mehr als 30 US-Dienste auf alle nur erdenklichen Daten zugreifen, wie es Edward Snowden öffentlich gemacht hat (Snowden 2019). Die Frage, die auch Microsoft&Co. beantworten sollten, ist, wie man überhaupt weiter mit Informationstechnik und Netzwerken arbeiten kann, wenn schon heute wenigstens 10% der Investitionskosten in Unternehmen für IT-Security aufgewendet werden müssen und es immer mehr, zudem automatisierte Angriffe aus dem Netz gibt. Google etwa hat am 19. August 2022 erfolgreich einen DDOS-Angriff abgewehrt, bei dem mit bislang nicht vorstellbaren 46 Millionen https-Anfragen in einer Sekunde versuchte wurde, eine Serveranwendung zu blockieren (Sokolov 2022). Je vernetzter die Geräte des Internet of Things (IoT) werden, desto höher sind Aufwand und Kosten, diese Infrastruktur zu schützen.

Statt die Wege der Vernetzung immer weiter zu gehen, wäre es intelligenter zu fragen, was überhaupt im Netz erreichbar sein muss und welche Anwendungen lokal laufen können. Intelligent wäre, sich neue Strukturen für eine digitale Souveränität in Europa zu überlegen, um Datensicherung und Datenschutz nach

dem EU-Rechtssystem gewährleisten zu können statt zu behaupten, dass die bisherigen Systeme die Bedingungen doch erfüllen würden – was laut EuGH-Urteil definitiv nicht stimmt. „Probleme kann man niemals mit derselben Denkweise lösen, mit der sie entstanden sind.“, hat Albert Einstein formuliert, und das bedeutet, dass man Lösungen eher nicht von Anbietern erwarten darf, deren Geschäftsmodell auf den bisherigen Strukturen basieren.

Quellen

LfDI (2022a) Verunsicherung nach Schrems II-Urteil: LfDI Baden-Württemberg bietet Hilfestellung an (24.8.2020); https://www.baden-wuerttemberg.datenschutz.de/verunsicherung-nach-schrems-ii-urteil-lfdi-baden-wuerttemberg-bietet-hilfestellung-an/ (16.8.2022)

LfDI (2022b) Nutzung von MS 365 an Schulen. Ab dem kommenden Schuljahr ist die Nutzung von MS 365 an Schulen zu beenden oder deren datenschutzkonformer Betrieb ist von den verantwortlichen Schulen eindeutig nachzuweisen. https://www.baden-wuerttemberg.datenschutz.de/nutzung-von-ms-365-an-schulen/ (16.8.2022)

Microsoft (2022) Stellungnahme von Microsoft Deutschland zur Datenschutzkonformität von Microsoft 365 und Microsoft Teams; https://news.microsoft.com/wp-content/uploads/prod/sites/40/2022/08/ Microsoft-Statement_Datenschutzkonformitaet-von-Microsoft-365-und-Microsoft-Teams.pdf (16.8.2022)

Pakalski, Ingo (2022) Bedenken beim Datenschutz: Schulen dürfen Teams bald nicht mehr nutzen, in: https://www.golem.de/news/bedenken-um-datenschutz-schulen-duerfen-teams-bald-nicht-mehr-nutzen-2206-166424.html (16.8.2022)

Pressemitteilung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 28.07.2020;https://datenschutzkonferenz-online.de/medi/pm/20200616_pm_schrems2.pdf (16.8.2022)

Snowden, Edward (2019) Permanent record. Meine Geschichte.

Sokolov, Daniel AJ (2022) Rekord-Angriff mit DDoS auf Layer 7 scheitert an Google; https://www.heise.de/news/Rekord-DDoS-auf-Layer-7-Google-wehrt-ab-7235554.html (20.8.2022)

rnd (2022) Redaktionsnetzwerk Deutschland: Strengerer Datenschutz bei Kindern. Microsoft Teams ist an Schulen in Rheinland-Pfalz bald nicht mehr erlaubt; https://www.rnd.de/digital/microsoft-teams-ist-an-schulen-in-rheinland-pfalz-bald-nicht-mehr-erlaubt-FSFYEY4K7UEMEFWMER2LA7DJU4.html (16.8.2022)

MD (2020) US-Datenrecht: Zugriff US-amerikanischer Behörden auf Daten, https://www.bundestag.de/resource/blob/796102/ea53ffe8e08a9ab11e270719263d8c53/WD-3-181-20-pdf-data.pdf (16.8.2022)

MD (2019) Wissenschaftliche Dienste des Deutschen Bundestages, Datenübermittlung an US-Ermittlungsbehörden auf Grundlage des CLOUS Acts im Geltungsbereich des EU-Datenschutzrechts, AD 3 – 3000 – 205/19 vom 20. August 2019; https://www.bundestag.de/resource/blob/662608/67dbc571f4d96be9adddcac99f016eb6/WD-3-205-19-pdf-data.pdf (16.8.2022)