RESEARCH & INNOVATION

CII WHITE PAPER

Zwischen Quasi-Monopol und Souveränitäts-Washing:

Hindernisse auf dem Weg zu einer souveränen Cloud-Infrastruktur der deutschen Verwaltung

Michael Kolain, *Senior Fellow am cyberintelligence.institute*

CYBER|INTELLIGENCE
.Institute

Inhalt

Der Autor

Michael Kolain, Senior Fellow

Michael Kolain ist Volljurist und Experte für Digitalpolitik. Am FÖV Speyer hat er im Team von Prof. Mario Martini den Programmbereich „Digitalisierung" aufgebaut und zu KI-Regulierung, Digitalisierung der Verwaltung und Daten(schutz)recht geforscht. Als Fraktionsreferent für Digitalpolitik hat er an der Gesetzgebung der Ampelregierung mitgewirkt. Er arbeitet an der Schnittstelle zwischen Gesetzgebung, Wissenschaft und der Entwicklung digitaler Technologien.

Executive Summary

Die öffentliche Verwaltung in Deutschland ist in zentralen Bereichen ihrer IT faktisch von Microsoft abhängig. Mit geschlossenen Ökosystemen, gezieltem Product-Bundling, restriktivem Lizenzmanagement und massiver Lobbyarbeit hat der Konzern eine Quasi-Monopolstellung aufgebaut. Diese steht einem offenen, freien und fairen Wettbewerb im europäischen Cloud-Markt systematisch im Weg.

Die Folge sind eingeschränkte Wahlfreiheit, wachsende Sicherheitsrisiken, mangelnde Transparenz und eine schwindende Budgethoheit in öffentlichen Haushalten. Lock-in-Effekte wirken dabei als Hebel: Proprietäre Standards, die enge Verzahnung von Client, Server und Cloud sowie hohe Migrationskosten zu alternativen Lösungen halten Behörden im Microsoft-Ökosystem. Digitalsouveräne Alternativen bleiben trotz vorhandener vielfältiger Angebote praktisch chancenlos. Parallel verschärft die angekündigte Abkehr von unbefristeten On-Premises-Lizenzen und der Übergang zu verpflichtenden Abomodellen mit Azure-Anbindung ab 2029 die Abhängigkeit. Preise und Konditionen wandern in den Einflussbereich von Microsoft – Währungs- und Eskalationsrisiken inklusive.

Für die digitale Souveränität der öffentlichen Verwaltung ist diese Konstellation toxisch. Der Staat verliert Kontrolle über Code, Update-Politik und Datenflüsse.

Für die digitale Souveränität der öffentlichen Verwaltung ist diese Konstellation toxisch. Der Staat verliert Kontrolle über Code, Update-Politik und Datenflüsse. Denn Microsoft schirmt zentrale Komponenten als Geschäftsgeheimnis ab und rollt globale Updates aus, die vorab weder umfassend auditierbar noch hinreichend individuell an deutsche Behördenbedürfnisse anpassbar sind. Sicherheitsvorfälle der letzten Jahre – vom Supply-Chain-Desaster bis zu Datenschutzverletzungen – haben gezeigt, wie verwundbar ein zentralisiertes Cloud-Modell ist: Jede Schwäche im Kern strahlt in die Peripherie und macht die Verwaltung potenziell angreifbar. Hinzu kommen Rechts- und Compliance-Unsicherheiten, etwa durch eine intransparente Verarbeitung von Diagnosedaten, extraterritoriale data dominance und eine begrenzte Prüfbarkeit, was bei Fernzugriffen zur Wartung der Systeme genau passiert. Auch scheinbar souveräne Betriebsmodelle ändern daran wenig: Teilsouveräne Konstruktionsvarianten mit nationalen Rechenzentren oder „EU-Datengrenzen“

Solange Code, Updates und Architekturkontrolle bei einem Einzelkonzern verortet sind, bleiben juristische wie technische Abhängigkeiten bestehen.

adressieren Symptome, nicht Ursachen. Solange Code, Updates und Architekturkontrolle bei einem Einzelkonzern verortet sind, bleiben juristische wie technische Abhängigkeiten bestehen; höhere Preise solcher „Sicherheits-Hülsen“ ohne echte Unabhängigkeit verschlechtern zusätzlich die Kostenkontrolle.

Wettbewerbspolitisch verschiebt Microsoft durch eine strategische Bündelung einzelner Produkte und eng verflochtene Vertriebsnetze die Marktlogik: Wo das Kommunikationstool Teams faktisch „mitgeliefert“ wird und Schnittstellen nicht hinreichend offen sind, verlieren interoperable Alternativen ihre Zugkraft. Jahrzehntelange Lobbyarbeit, dichte Partnerstrukturen und mehrjährige Rahmenverträge verfestigen die Dominanz – und erschweren es öffentlichen Beschaffern, herstellerunabhängige, modulare Architekturen im digitalen Maschinenraum zu verankern. So entsteht ein digitaler Teufelskreis: Die Politik reagiert auf kurzfristige Betriebsfähigkeit, der Markt passt sich der Dominanz an, und die strategische Fähigkeit des Staates, seine IT-Arbeitsumgebung selbstbestimmt zu steuern, sinkt.

Mit dem politischen Ziel der digitalen Souveränität ist dieser Zustand nicht vereinbar. Denn digitale Souveränität braucht echte Wahlfreiheit – technisch, rechtlich und ökonomisch. Den nun bis 2028 laufenden Zyklus des BMI-Rahmenvertrags mit Microsoft, der die Grundlage für das Gros der Beschaffungsvorgänge in Bund, Ländern und Kommunen bildet gilt es als Übergangsphase zu nutzen, um eine schrittweise Abkehr von monolithischen IT-Abhängigkeiten zu planen und umzusetzen. Dazu gehören: die verbindliche Verankerung offener Standards und Schnittstellen in künftigen Verträgen (Portabilität, Interoperabilität, Exit-Regeln), herstellerübergreifende Referenzarchitekturen mit klaren Workload-Kriterien statt Cloud-Zwang, verpflichtende Audits mit Code-Einblick unter Vertraulichkeit, unveränderbare und kontinuierlich überprüfbare Protokollierung sämtlicher Fernzugriffe, Schlüsselhoheit beiden Behörden sowie belastbare Kosten- und Abhängigkeitsbilanzen über alle Verwaltungsebenen hinweg.

> **Der Staat selbst muss hier gleichsam in die Vorhand kommen, statt sich von Versprechungen eines – wie es die Gesellschaft für Informatik es auf den Punkt bringt – „Souveränitäts-Washings“ becircen zu lassen.**

Der Staat selbst muss hier gleichsam in die Vorhand kommen, statt sich von Versprechungen eines – wie es die *Gesellschaft für Informatik* es auf den Punkt bringt – „Souveränitäts-Washings“ becircen zu lassen. Kartellrechtliche Prüfverfahren sollten alle Lizenz- und Bündelpraktiken, die Wahlfreiheit faktisch aushebeln, detailliert ausleuchten und durch geeignete aufsichtsrechtliche Maßnahmen adressieren. Parallel sind die Mitgliedstaaten der EU aufgerufen, europäische und offene Alternativen gezielt zu fördern – durch Konsortien, Referenzimplementierungen und eine koordinierte EU-Beschaffungsstrategie, die Deutschland als Ankerkunden positioniert und die Verhandlungsmacht der öffentlichen Hand länderübergreifend bündelt. Frankreich und Deutschland sollten den „Gipfel zur digitalen Souveränität 2025“am 18. November 2025 nutzen, um die entscheidenden Weichen für eine souveräne Verwaltungscloud, die diesen Namen verdient hat, zu stellen.

Der öffentliche Sektor muss dabei mit gutem Beispiel vorangehen: bestehende Microsoft-Abhängigkeiten jetzt aktiv reduzieren, Pilot- und Migrationspfade für offene, interoperable Lösungen aufsetzen, Kompetenzaufbau finanzieren und in der Beschaffung strikt auf modulare Lösungen zu setzen. Digitale Souveränität ist kein PR-Label, sondern ein staatlicher Steuerungsauftrag: Sie entsteht durch politische Führung, technische Umsetzung und wettbewerbliche Durchsetzung. Wer heute konsequent auf offene Ökosysteme setzt, senkt morgen Sicherheits- und Lieferkettenrisiken, stärkt die Budgethoheit und schafft eine belastbare, europäisch tragfähige IT-Basis. Denn nur ein Staat, der seine Arbeitsgrundlagen, Infrastrukturen und Kommunikationsprozesse selbst beherrscht und souverän steuert, ist resilient gegen Bedrohungen von außen.

Kapitel 1:
Einleitung

Wer in eine deutsche Amtsstube geht, wird dort nicht nur Aktenstapel, Büroklammern und Stempel auf den Schreibtischen vorfinden. Sondern – wie in den meisten deutschen Büros – auch Computer. Selbst wenn es aus Sicht der Bürger:innen, die im Kontakt mit der Verwaltung oftmals noch auf dem Postweg kommunizieren (müssen), stellenweise anders wirkt: die Arbeitsroutinen der öffentlichen Verwaltung haben sich in den letzten Jahrzehnten weitgehend digitalisiert. Ohne Hardware und Software sind die meisten Behörden heute nicht arbeitsfähig. Doch mit der zunehmenden digitalen Ausstattung sind intensive Geschäftsbeziehungen zu privaten IT-Dienstleistern entstanden. Auf Ebene der Software dominiert der Microsoft-Konzern die digitale Verwaltung.

Wer als Mitarbeiter der öffentlichen Verwaltung einen staatlichen Computer hochfährt, wird in aller Regel das Logo des Betriebssystems *Windows* sehen. Wer einen Verwaltungsakt vorbereitet oder Vermerke schreibt, wird dafür auf die Office-Suite von Microsoft zurückgreifen: *Word* für Texte, *Excel* für Tabellen, *PowerPoint* für Präsentationen. Der sichere Umgang mit Microsoft-Anwendungen fehlt auf fast keiner Stellenanzeige des öffentlichen Dienstes. Doch wenn es um die Ausstattung der Verwaltung und die Arbeitsfähigkeit geht, sollte es ausgeschlossen oder jedenfalls die seltene Ausnahme für einen Übergangszeitraum sein, Abhängigkeiten von einem einzelnen Anbieter zu begründen. So ist es völlig selbstverständlich, dass sich die Verwaltung Druckerpapier, Schreibtische, Laptops und Aktenschränke am Markt beschafft, und dabei auf unterschiedliche Produzenten mit dem jeweils besten Preis und Angebot setzt. Dadurch bleibt der Staat unabhängig von einzelnen Lieferanten und kann seine Beschaffungsroutinen stets flexibel halten. Doch fast jedes Budget von Kommunen, Bundesländern und Bundesministerien hat Microsoft-Lizenzen in erheblichem Umfang auf der Soll-Seite des Haushaltsplans – und alternative Anbieter und Wettbewerber führen ein auffälliges Schattendasein.

Dass die Verwaltung gleichsam am Tropf eines Konzerns hängt, der laut Bundeskartellamt eine „überragende marktübergreifende Bedeutung für den Wettbewerb“ innehat, kann mit dem rechtsstaatlichen Gebot in Konflikt geraten, dass die Verwaltung ihre Aufgaben eigenständig und nach gesetzlichen Vorgaben wahrzunehmen hat. Was könnte die Bundesregierung tun, wenn Microsoft bei einer Neuverhandlung des BMI-Rahmenvertrags auf stur stellt und die Preise einfach verdoppelt oder verdreifacht? Umso relevanter ist letztlich auch die Antwort auf ebenjene Frage, wenn in Deutschland mit Microsoft ein einzelner Konzern im Wesentlichen das Monopol über Produktivitätssoftware aus der Cloud inne- und aufrechterhält und hierdurch den Wechsel zu alternativen Anbietern in einem freien, offenen und interoperablen Markt gezielt behindert.

> **Trotz der geopolitischen Umwälzungen steht Deutschland im Jahre 2025 kurz davor, die Zusammenarbeit mit Microsoft weiter zu vertiefen – obwohl der US-Konzern eine Geschäftspolitik verfolgt, die den Staat noch abhängiger von seinen Diensten machen soll.**

Trotz der geopolitischen Umwälzungen steht Deutschland im Jahre 2025 kurz davor, die Zusammenarbeit mit Microsoft weiter zu vertiefen – obwohl der US-Konzern eine Geschäftspolitik verfolgt, die den Staat noch abhängiger von seinen Diensten machen soll. Hinzu kommt: Der Konzern aus Redmond will seine Nutzer dazu bringen, seine Standardsoftware von Outlook über Teams bis hin zu PowerPoint nicht mehr über unbefristete Einzellizenzen zu erwerben, sondern nur noch mit Anbindung an die Microsoft-Cloud Azure zu nutzen. Andere Anbindungen der Office-Programme sollen bis 2029 auslaufen, insbesondere die sog. on-premise Softwarelizenzen.

Obwohl es am Markt einzelne Alternativen zu Windows, Office, Microsoft365 und Azure gibt und erste staatliche Akteure bereits auf alternative Anwendungen umsatteln: Microsoft ist weiterhin der Platzhirsch in der öffentlichen IT – sowohl in den Mitgliedstaaten als auch in der EU. Eine aktuelle Studie der Open Cloud Coalition hat den dominanten Marktanteil von Microsoft im Bereich Bürosoftware (*Office*, 90%) und Zusammenarbeit (*collaboration*, 84%) noch einmal unterstrichen. Ein hoher Marktanteil von über 80 Prozent führt selbstverständlich auch zu hohen Einnahmen für den Quasi-Monopolisten: Für Lizenzen für Office und Betriebssysteme gingen zuletzt schätzungsweise 198 Millionen Euro deutsches Steuergeld an Microsoft. Die Gewinne investiert Microsoft wiederum in umfangreiche Lobbytätigkeit, die das Lizenzregime und die Produktlogik weiter auf gezielte und dauerhafte Abhängigkeiten programmiert.

Es gibt unterschiedliche Vorschläge, mit der Abhängigkeit der deutschen Verwaltung von Microsoft umzugehen: von einem strategischen Ausstieg aus dem Microsoft-Ökosystem bis zu einem bestimmten Stichtag, über einen verbindlichen Open-Source-Anteil in der öffentlichen IT-Vergabe, den Betrieb der Microsoft-Produktpalette mitsamt Speicherung der Verwaltungsdaten bei einem deutschen Unternehmen bis hin zu strengen vertraglich garantierten Sicherheitsmaßnahmen und -verpflichtungen durch Microsoft selbst.

Auch unter dem Eindruck der aktuellen geopolitischen Situation streben Deutschland und viele andere EU-Regierungen politisch einen Zustand der „digitalen Souveränität“ an. Ein Großteil dieser Debatte konzentriert sich auf die Förderung der digitalen Infrastruktur und Industrie in der EU. Diese Bemühungen sind zwar auf politisch-abstrakter Ebene lobenswert, erfordern aber in der konkreten Umsetzung viel Zeit, klare Strategien und umfangreiche Investitionen. Sich aus den Abhängigkeiten zu lösen, die über Jahrzehnte entstanden sind, ist ein langfristiger Kraftakt. Das Whitepaper zeigt auf, welche Hindernisse der digitalen Souveränität im Wege stehen und was innerhalb des derzeitigen technologischen Umfelds politisch möglich wäre, um der Verwaltung zu mehr Wahlfreiheit über ihre digitale Arbeitsumgebung zu verhelfen.

In diesem Whitepaper beschreiben wir, wie abhängig sich europäische Behörden und Unternehmen von einzelnen Microsoft-Produkten gemacht haben, und zeigen auf, welche Nachteile damit für Staat und Wirtschaft einhergehen (Kapitel 2). Die Aktivitäten des Microsoft-Konzerns im Bereich Lobbyarbeit und Geschäftsmodellentwicklung, die darauf zielen, die faktische Monopolstellung für Betriebssystem und Standardsoftware bei staatlichen Digitalarbeitsplätzen zu erhalten, zeichnen wir in Kapitel 3 nach. In Kapitel 4 suchen wir nach Szenarien, die einen Weg vom Status Quo zum politischen Ziel einer „souveränen Cloud-Infrastruktur“ in Deutschland und Europa ebnen können. Abschließend formulieren wir Handlungsempfehlungen für politische Entscheidungsträger:innen (Kapitel 5).

Digitale Souveränität
zielt nicht auf Autarkie oder digitalen Isolationismus, sondern soll dem Staat die Möglichkeit eröffnen, überhaupt die technologische Wahlfreiheit zu gewährleisten, seine digitale Arbeitsumgebung strategie- und rechtskonform auszugestalten. Das Ziel lässt sich nicht dadurch erreichen, nach Unabhängigkeit von außereuropäischen Anbietern zu streben, also nur auf europäische oder deutsche Unternehmen zurückzugreifen. Digitale Souveränität bedeutet vielmehr, Praktiken zu reduzieren, die dem Staat die Wahlfreiheit über seine digitale Infrastruktur nimmt. Digitale Souveränität heißt, dass die Bedingungen für ein faires Marktumfeld vorliegen, in dem Kunden eine echte Wahl zwischen Software- und Cloud-Anbietern innerhalb und außerhalb Europas haben. Im besten Fall stellt sich der Staat seine IT-Landschaft modular und bedarfsorientiert aus interoperablen Komponenten zusammen, die über offene Schnittstellen miteinander kommunizieren. Das Gegenteil von digitaler Souveränität sind faktische Abhängigkeiten von Quasi-Monopolisten sowie ein „Kill Switch“ im Ausland, der die digitale Verwaltungsarbeit überwachen oder ganz lahmlegen kann.

Kapitel 2:

Der Status Quo – Das Microsoft-Imperium und seine Hintergründe

Der IT-Konzern, den Bill Gates im Jahre 1975 in den USA gegründet hat, versteht es auch zu Beginn des proklamierten Cloud-Zeitalters, Kundenbindung aufzubauen, aufrechtzuerhalten und zu verstärken. Dies ist ein Erfolg jahrelangen und intensiven Marketings und Lobbyismus des Konzerns mit Hauptsitz in Redmond,

> **Es liegt im legitimen ökonomischen Interesse eines international erfolgreichen IT-Konzerns, seinen Marktanteil im öffentlichen Sektor zu festigen und zu erweitern.**

USA. Es liegt im legitimen ökonomischen Interesse eines international erfolgreichen IT-Konzerns, seinen Marktanteil im öffentlichen Sektor zu festigen und zu erweitern. Es ist deshalb nicht verwunderlich, dass hinter den neuen Angeboten Methode steht: Wenn die Behörden schon in großem Umfang auf Microsoft setzen, warum dann nicht auch andere Segmente der staatlichen IT erschließen?

I. Die Marktmacht von Microsoft im öffentlichen Sektor und ihre Ursachen

Eine aktuelle Studie der Open Cloud Coalition hat den dominanten Marktanteil des Microsoft-Konzerns im Bereich der Standardsoftware im Vergleich zu Amazon *Web Services* und *Google* analysiert: Im Bereich „Office“ berechneten die Autor:innen einen Marktanteil von 90%, bei „Collaboration“ sind es 84%. Das Whitepaper legt seinen Fokus auch deshalb auf den „strongest player in the game“ und nicht auf seine aktuellen Wettbewerber aus den USA. Die Marktmacht drückt sich für Microsoft in hohen Einnahmen aus dem öffentlichen Sektor aus. In Deutschland fallen allein auf Bundesebene (also noch ohne Zahlen aus den 16 Bundesländern und den über 11.000 Kommunen) Lizenzkosten in Höhe von 197,7 Millionen Euro gegenüber Microsoft an. Tendenz steigend: Seit 2017 sind die Kosten auf Bundesebene um mehr als 250 Prozent nach oben gegangen, wie das IT-Magazin heise berichtet. Von den Gesamtkosten entfallen 98,5 Millionen auf unbefristete Lizenzen, 29 Millionen auf Abo-Modelle und 69 Millionen auf „weitere Leistungen und Produkte“.

Eine Kleine Anfrage im Deutschen Bundestag hat Anfang 2025 zu Tage gebracht: Bei den Betriebsausgaben für Cloud-Anwendungen setzt der Bund zu 99,9 Prozent auf proprietäre Software. Microsoft hat hier den deutlich höchsten Anteil. Doch obwohl im digitalpolitischen Diskurs viel Zweifel und Kritik an einem sinnvollen und rechtskonformen Einsatz der Microsoft-Software aufkommen und viele Fragen noch nicht final geklärt sind (dazu unten X.): Zahlreiche öffentliche Stellen rüsten bereits aktuell auf Microsoft Teams um – und können dann über die durch Microsoft-Lizenzen oder -Abos flankierten Server chatten, an Dokumenten arbeiten und Videokonferenzen abhalten.

Doch ist es politisch sinnvoll, dass der Ankerkunde Staat von strategischen Entscheidungen eines einzelnen Providers abhängig ist? In den folgenden Abschnitten stellen wir einige Ursachen dafür vor, warum die deutsche Verwaltung in eine so starke Abhängigkeit von einem einzelnen Anbieter hat kommen können.

1. Plattform- und Lock-in-Effekte begünstigen dominante Marktstellung

Dass Microsoft auf den Rechnern der deutschen Verwaltung so weit verbreitet ist, lässt sich nicht alleine dadurch erklären, dass es am Markt keinerlei Alternativen zu Microsoft gibt oder die „MS“-Produkte unschlagbar gut sind. Vielmehr hat Microsoft in seiner Produktentwicklung vom Betriebssystem (Windows), über Standardsoftware (MS Office) bis hin zu E-Mail-Servern (Exchange) und nun Cloud (Azure / OneDrive) stets auch seine politischen und administrativen Zugänge,

die der Konzern durch Lobbyaktivitäten und umfangreiche Öffentlichkeitsarbeit seit Jahrzehnten aufgebaut und bespielt hat, sein Marktwissen und sein Lizenzmanagement strategisch genutzt, um den Marktanteil im öffentlichen Sektor immer weiter auszubauen. Dem Unternehmen selbst lässt sich der unternehmerische Erfolg schwerlich vorwerfen – der Konzern versucht seine Umsätze und Gewinne zu verbessern und seine Produkte unter die Leute zu bringen. Das ist legitim und der unternehmerische Erfolg verdient durchaus auch Anerkennung.

In seiner marktdurchdringenden Rolle jedoch bedient sich Microsoft Mittel, die das Ziel eines fairen Wettbewerbs auf dem EU-Binnenmarkt tendenziell untergraben. In der ökonomischen Literatur spricht man von sog. *Lock-In-Effekten*: Ist der Wechsel zu einem anderen Anbieter aufgrund faktischer Umstände bewusst so aufwändig gestaltet, dass Organisationen auf einen Wechsel zum Wettbewerber verzichten, versagt das Prinzip von Angebot und Nachfrage. Befürchten Verantwortliche, dass ein Umstieg enorm viel Zeit und Geld kostet, mit großen internen Umstellungen und im schlimmsten Fall mit Datenverlust einhergeht, scheuen sie den – ökonomisch oder qualitativ womöglich naheliegenden – Wechsel. Der Professor für Wettbewerbsrecht *Ruppert Podszun* beschreibt Lock-In-Effekte in einem Buchkapitel wie folgt: „Auf Grund durchintegrierter, geschlossener Ökosysteme sind Nutzer und Nutzerinnen verleitet, diese Ökosystem nicht zu verlassen, um alternative Angebote, sofern überhaupt interoperabel, wahrzunehmen“. Durch seine Strategie der Produktentwicklung in einem exklusiven und durch Microsoft dominierten Ökosystem hat es der Konzern geschafft, Lock-In-Effekte zu seinem eigenen Vorteil zu nutzen.

> **Microsoft nutzt seine dominante Marktstellung und finanziellen Spielräume auch, um die Lieferkette nach eigenen Vorstellungen zu formen.**

Microsoft nutzt seine dominante Marktstellung und finanziellen Spielräume auch, um die Lieferkette nach eigenen Vorstellungen zu formen. Dem Konzern ist es mehrfach gelungen, europäische Wettbewerber als Microsoft Vertriebspartner auf das eigene Ökosystem einzunorden oder auf andere Weise aus dem Wettbewerb zu drängen. Immer wieder geriet das System der Lizenzvergabe und der Vertriebskanäle unter Kritik. Im Bereich Cloud-Computing soll Microsoft unabhängige Anbieter von Cloud-Infrastruktur gezielt in die Rolle eines Resellers für Microsoftlizenzen gedrängt haben.

2. Never change a winning team – oder: Souverän ist (nur), wer Wahlfreiheit hat.

Nachdem Windows und Office bereits der Platzhirsch auf Behördencomputern sind, will Microsoft auch im Bereich Cloud die Marktanteile ausbauen. Dabei nutzt der Konzern mehrere Vorteile. Zunächst kommt einem Quasi Monopolisten die Macht der Gewohnheit in den Behörden („Das haben wir schon immer so gemacht“) entgegen (1.). Darüber hinaus kann Microsoft durch seine Unternehmenspolitik im Bereich Preis- und Produktentwicklung und sein Vertriebsnetzwerk Angebot und Nachfrage beeinflussen (2.). Da Microsoft seine globalen Umsätze kontinuierlich steigert und im Jahr 2024 einen Nettogewinn von 72 Milliarden € erwirtschaftet hat, nutzt der Konzern seine finanziellen Spielräume auch für umfangreiche Marketing- und Lobbyismus-Aktivitäten in Brüssel und Berlin (3.).

a) Die Macht der Gewohnheit in der öffentlichen Verwaltung und der Fachkräftemangel

Es ist kein Klischee, dass in der öffentlichen Verwaltung besonders starke Beharrungskräfte am Werk sind. Wer hier die gewohnte Outlook-Umgebung aufkündigen oder Microsoft Word abschaffen will, kann im ersten Reflex mit viel Widerstand rechnen. „Das haben wir doch schon immer mit Microsoft gemacht“ kann schnell zum Schlachtruf einer Fundamentalopposition avancieren, der jegliche Veränderungen im digitalen Arbeitsumfeld im Keim erstickt. Hinter vorgehaltener Hand nennen politische Entscheidungsträger:innen solche verwaltungskulturellen Herausforderungen als den eigentlichen Grund für die politische Scheu, den Weg zu einer post-Microsoft-Ära einzuschlagen. Vielleicht ist es aber auch eine angenehme Ausrede. Klar ist jedenfalls: Wenn Mut und Tatendrang für so ein Großprojekt auf hoher politischer Ebene fehlen, gewinnt meist die Trägheit der (behördlichen) Masse.

Aber nicht nur bei den Anwendern der Standardsoftware in den Amtsstuben, sondern auch bei den IT-Abteilungen der Verwaltung kann eine Abkehr vom

gewohnten Microsoft-Ökosystem zu enormen Mehraufwänden führen. Der kommunale IT-Referent gerät schnell an seine Grenzen, wenn die Mailkonten im behördlichen Rechenzentrum bereits über Exchange aufgesetzt sind und die Software automatisiert geupdatet wird, wenn das Lizenzmanagement mit den Microsoft-Vertrieblern, die sich um die Geschäftsbeziehung bemühen, mit dem Vergabereferat schon so gut eingespielt ist und wenn sich bereits etliche Laptops mit Windows und Office-Suite im Umlauf befinden. Denn es ist alles andere als ein Kinderspiel, eine komplette IT-Infrastruktur, die tief durch Microsoft-Produkte und -Anwendungen geprägt ist, durch Alternativen zu ersetzen – insbesondere, wenn das Referat nebenbei noch OZG-Leistungen implementiert, die bestehende IT betreibt und wartet, IT-Supportanfragen à la „Warum druckt mein Drucker nicht mehr“ abarbeitet und aus den zuständigen Ministerien keinerlei Hilfestellung oder Anreiz für einen Umstieg erfolgt. Hinzu kommt, dass der IT-Fachkräftemangel auch und gerade vor der Verwaltung keinen Halt macht: Die Arbeitsbedingungen können mit der Digitalwirtschaft kaum mithalten, die Behördenleitung hat oftmals wenig Interesse an Digitalisierung. Und am Ende sind auch Schulen und Berufsschulen so an Microsoft gewöhnt, dass in der Ausbildung zum Fachinformatiker die Microsoft-Produktpalette und ihre Integration im Vordergrund steht. Es fehlt also nicht nur am Mut für Veränderung, sondern an den personellen und kompetenziellen Ressourcen für große Sprünge in der Verwaltungs-IT.

b) Wenn strategische Produktentwicklung und dynamische Preisentwicklung Hand in Hand gehen…
Die Verkündung einer strategischen Entscheidung im Hauptsitz in Redmond hat viele Kunden im öffentlichen Sektor unter Zugzwang gesetzt: Mit der Umstellung auf Microsoft 365 soll es nach dem Willen der Microsoft-Spitze ab spätestens 2029 faktisch nicht mehr möglich sein, die on-premise Varianten der Microsoft-Programme zu nutzen (z.B. Microsoft Office 2024) – zwingend ist immer eine Anbindung an die von Microsoft bereitgestellte Cloudinfrastruktur Azure. Wenn die öffentliche Verwaltung also weiterhin auf die vertraute Office-Umgebung zurückgreifen will, hätte sie ab 2029 keine Wahl mehr: Sie müsste sich zwangsläufig noch tiefer in das Microsoft-Ökosystem integrieren und ihre Budgetierung für Software umstellen.

Zugzwang durch Unternehmensentscheidung statt reflektierte Cloud-Strategie der Verwaltung
Obwohl die deutsche Verwaltung bislang keinen allzu starken Willen hatte, großflächig auf Cloud-Computing umzusteigen, versucht Microsoft sie mit der Ankündigung „ab 2029 nur noch Abomodell“ nun faktisch in ein Angebot zu „nudgen“, das nicht zwingend den tatsächlichen Bedürfnissen der Behörden entspricht. Das Signal aus Redmond ist klar: Wollen Behörden Outlook und Office weiter nutzen, bietet es sich doch angesichts der Marketingkampagnen im Cloud-Zeitalter an, die „Public Cloud“ direkt als neues Speichermedium und Datendrehscheibe für die öffentliche Verwaltung

> **Die Folgen einer faktischen Abhängigkeit von Microsoft zeigen sich an dieser Stelle besonders deutlich.**

zu nutzen. Die Folgen einer faktischen Abhängigkeit von Microsoft zeigen sich an dieser Stelle besonders deutlich. Statt im ersten Schritt in einer Cloud-Strategie für sich zu entscheiden und zu analysieren, wann ein Cloud-Service im Workflow der Verwaltung sinnvoll zum Einsatz kommen kann, um sich dann nach passenden Anbietern umzuschauen, lässt sich der Staat durch die unternehmerischen Entscheidungen Microsofts, vollständig in die Cloud zu gehen, vor sich hertreiben. Selbstbestimmung und strategische Wahlfreiheit über die eigene IT-Infrastruktur des Staates sieht anders aus.

Die angekündigte Abkehr vom Lizenzmodell wird absehbar auch Auswirkungen auf das zentrale Vehikel haben, mit dem die deutsche Verwaltung Microsoft-Lizenzen zu besonderen Konditionen erhält: der Rahmenvertrag Microsofts mit dem Bundesministerium des Innern (BMI). Er bildet die rechtliche Grundlage für den Kauf von Softwarelizenzen durch deutsche Behörden und öffentliche Stellen. Auf die darin enthaltenen vergünstigten Konditionen können sich nicht nur Bundesbehörden, sondern auch Länder, Kommunen und andere Körperschaften berufen, wenn sie Microsoft-Lizenzen beschaffen. Sie können die sog. Konditionenverträge zum Gegenstand ihres Vergabeverfahrens machen. Über die sog. Licensing Solution Partner (LSP) des Microsoft-Konzerns – darunter etwa Bechtle oder die SoftwareONE – kaufen Städte und Landesbehörden dann Microsoft-Lizenzen für Stan-

dardsoftware und Server-Umgebungen. Alle drei Jahre verhandeln Microsoft und das BMI neue Konditionen für stetig wachsende Lizenzgegenstände. Erst im Frühjahr 2025 begann die nächste dreijährige Laufzeit. Die Ankündigung Microsofts, das on-premise Angebot auslaufen zu lassen, würde nicht nur den BMI-Rahmenvertrag in seiner Struktur und seinem Rechtscharakter beeinflussen. Für die Neuverhandlungen bis zum Jahre 2028 ist zu klären, wie der sog. „Select Plus-Vertrag" in Anbetracht künftiger Abo-Modelle angepasst werden muss. Zugleich muss sich die Bundesregierung fragen, ob sie ihre bisherigen vertraglichen Beziehungen mit Microsoft angesichts stetig wachsender Bindungen und Abhängigkeiten tatsächlich verlängern soll.

Preise, Preise, Preise – wohin geht die Reise?
Über die Preisgestaltung seiner Cloud hat Microsoft einen wirkmächtigen Hebel gebaut, denn mit dem Umstieg kann der Konzern die Preise seinen Bestandskunden in einem ersten Schritt sehr günstig anbieten, um die öffentliche Verwaltung zu einem schnellen und niedrigschwelligen Übergang zu motivieren – dann später aber die Preise sukzessiv ansteigen lassen. Verwunderlich wäre das nicht: Im privatwirtschaftlichen Markt mit Cloud-Lösungen führte ein Preisanstieg um 11 Prozent zum 1. April 2023 zu massiver Kritik in Deutschland und Europa. Manche Wettbewerber konstatierten, dass die Preissteigerungen „an Erpressung grenzten". Auch das Bundeskartellamt beobachtet die Preispolitik des Konzerns seit September 2024 näher – und stellt Microsoft unter die sog. „erweiterte Missbrauchsaufsicht" (§19a GWB). Gegenüber Privatkunden hatte sich Microsoft zudem darauf berufen, die Preise müssten auch Kursschwankungen des US-Dollars abbilden und würden deshalb künftig regelmäßig angepasst. Eine Währungskrise in den USA oder veränderte Einfuhrbedingungen könnte dann dazu führen, dass der deutsche Fiskus auf einen Schlag mit exponentiell wachsenden IT-Budgets konfrontiert ist, die eigentlich für den Ausbau der Verwaltungsdigitalisierung und die Förderung souveräner Cloud-Lösungen eingeplant waren.

Hinzu kommt: Wird einem privaten oder behördlichen Nutzer des Betriebssystems Windows oder der Office-Suite direkt – auf den ersten Blick kostenlos – ein Kommunikationstool (Microsoft Teams) oder eine Cloud-Anwendung (OneDrive) mitgeliefert, beeinträchtigt das den freien und fairen Wettbewerb – insbesondere, wenn andere Lösungen mit dem Microsoft-Ökosystem überhaupt nicht interoperabel sind. Statt einen datenschutzfreundlichen Messenger für die Behördenmitarbeiter:innen zu implementieren, der nach Möglichkeit interoperabel ist und im Sinne der DSGVO dadurch ein höchstmögliches Maß an Datenportabilität gewährleistet, nutzt eine Behörde dann gleich kostenfrei oder für geringen Aufpreis auch Microsoft Teams, der genau ebenjene Funktionen nicht bietet. Die EU-Wettbewerbsbehörde sieht solche Geschäftsmodelle kritisch. Denn für die IT-Abteilungen der Behörden kann es aus verschiedenen Gründen naheliegen, für die interne Kommunikation Teams zu nutzen, weil Server und Laptops ohnehin auf Microsoft programmiert sind. Mit dem nächsten Produktupdate des Herstellers ist dann direkt auch eine neue Kommunikationsplattform integriert und ausgerollt. Dieses strategische Vorgehen hat dazu geführt, dass sich die Verwaltung in einen goldenen Käfig begeben hat, aus dem sie nun nicht mehr ohne Weiteres herauskommt. Für die Verwendung von ebenfalls aus der Cloud kommender künstlicher Intelligenz aktualisiert sich diese Entwicklung zurzeit.

c) Enormer Aufwand für Lobbying und strategische Kommunikation
Der hohe Marktanteil von Microsoft-Produkten in der öffentlichen Verwaltung ist kein Zufall, sondern zumindest auch das Ergebnis intensiver Lobby- und Öffentlichkeitsarbeit des Microsoft-Konzerns. Nach Angaben von Lobbypedia betreibt Microsoft in Brüssel „ein eigenes Lobbybüro mit 17 Lobbyist:innen (10 Vollzeitäquivalente)" – es sei die „größte Lobby-Truppe unter den Tech-Konzernen in Europa". Im Geschäftsjahr 2019 gab der Konzern nach eigenen Angaben „zwischen 5.000.000€ und 5.250.000€ aus" für Lobbytätigkeiten aus. Im Geschäftsjahr 2023 investierte Microsoft laut statista bereits sieben Millionen Euro in die politische Kommunikation – im Vergleich dazu lag die Deutsche Telekom bei 1,75 Mio. €, und nur Meta Platforms Ireland Limited gab mit 9 Mio. € mehr aus. Die PR-Arbeit endet auch nicht mit unternehmenseigenen Lobbyisten, sondern Microsoft ist laut Lobbycontrol Mitglied oder Förderer in mehreren Think Tanks, Arbeitsgruppen und Branchenverbänden – von *Digital Europe* über das *European Internet Forum* bis hin zum *Centre on Regulation in Europe* (CERRE) und dem European Policy Centre (EPC). Hinzu kommt ein Netzwerk an Agentu-

ren für politische Kommunikation, Werbung, Politikberatung und internationalen Großkanzleien.

In Deutschland fehlen verlässliche Zahlen zu den Lobbyausgaben von Microsoft. Im Lobbyregister des Deutschen Bundestages sind für die Microsoft Deutschland GmbH neun Personen eingetragen, die „die Interessenvertretung unmittelbar ausüben"; hinterlegt sind auch Mitgliedschaften in 50 Vereinigungen. Die Microsoft Deutschland GmbH ist zudem Partner des IT-Branchenverbands BITKOM und Mitglied im Bundesverband Digitale Wirtschaft (BVDW), die regelmäßig die Interessen der Digitalwirtschaft in Gesetzgebungsverfahren und öffentlichen Anhörungen vertreten.

Im Zusammenspiel mit der Gesamtstrategie des Konzerns, den über 3.000 Mitarbeitern in Deutschland und 221.000 Personen weltweit, verfügt der Microsoft-Konzern über ein weitläufiges Netzwerk, um sich gegenüber Politik, Verwaltung und Gesellschaft für die eigenen geschäftlichen Interessen einzusetzen. Der starke Einfluss von Big-Tech-Unternehmen während des Gesetzgebungsprozesses für die neuen EU-Digitalgesetze hat vielmals zu kritischer Berichterstattung geführt – Microsoft war dabei oftmals die kommunikative Speerspitze.

II. Proprietär, unsicher, rechtswidrig? – Kritik am Microsoft-Einsatz in der Verwaltung

Die Kritik daran, dass sich die deutsche Verwaltung in großem Umfang in eine Abhängigkeit von Microsoft-Produkten begeben hat, entfaltet sich in verschiedenen Facetten. Die zentralen Punkte fassen wir im Folgenden zusammen.

1. Keine eigene Kontrolle über Funktionsweise und Sicherheit der Software

Viele staatlichen Stellen setzen bei der IT-Beschaffung in erster Linie deshalb auf Microsoft, weil es in einem digitalen Umfeld, das bereits durch Microsoft-Produkte geprägt ist, leicht und bequem ist, weitere Produkte von der Stange und aus einer Hand zu kaufen. Gegenüber GovTech-Startups, einer Community an Open-Source-Entwickler:innen und -Firmen, öffentlichen IT-Dienstleistern von Bund und Ländern oder Konsortien aus dem europäischen Mittelstand fehlt der Politik oftmals der Glaube, dass sie die IT-Infrastruktur Deutschlands auf Jahre sicher, funktionsfähig und zuverlässig entwickeln sowie auf hohem Niveau sichern und betreiben können. Die Abhängigkeit von Microsoft ist auch bequem: Alles, was an IT-Infrastruktur bereits an Microsoft ausgelagert oder von dort eingekauft ist, müsste der Staat dann ja möglicherweise wieder mehr selbst orchestrieren oder auf neue Schultern verteilen. Politische Entscheidungsträger:innen befürchten, dass ihnen der finanzielle Spielraum und die personellen Ressourcen fehlen, auf eigene oder aufwändiger zu betreibende Alternativen umzusatteln. Und wer als Ministerin oder Staatsekretär mit einem solchen Projekt scheitert, gefährdete nicht nur den eigenen politischen Ruf – sondern im schlimmsten Fall auch die Funktionsfähigkeit der Verwaltung, wenn sich die IT-Systeme als unsicher oder unzuverlässig erweisen.

> **Mit dem Einkauf von Lizenzen und Abos von einem marktdominanten Player entsteht aber der Nebeneffekt, dass es dem Staat nicht möglich ist, die Funktionsweise der Software zu steuern oder deren Sicherheit aus eigener Kraft zu gewährleisten, weil er infolge der Monopolstellung des Konzerns keine oder nur unzureichende eigene Verhandlungs- und damit auch inhaltliche Gestaltungsmacht besitzt.**

Mit dem Einkauf von Lizenzen und Abos von einem marktdominanten Player entsteht aber der Nebeneffekt, dass es dem Staat nicht möglich ist, die Funktionsweise der Software zu steuern oder deren Sicherheit aus eigener Kraft zu gewährleisten, weil er infolge der Monopolstellung des Konzerns keine oder nur unzureichende eigene Verhandlungs- und damit auch inhaltliche Gestaltungsmacht besitzt. Ein zentraler Grund dafür ist, dass Microsoft den Code und die Systemschnittstellen als Geschäftsgeheimnis einstuft. Das Geschäftsmodell des Konzerns besteht darin, sog. proprietäre Software über Lizenzen zu vertreiben. Wenn der deutsche Staat seine digitalen Arbeitsabläufe auf Microsoft-Produkte stützt, erhält er nur eine Installationsdatei mit Lizenzschlüssel und ggf. Support, aber keinen Blick in den Quellcode – ganz im Sinne einer Policy „take it or leave it". Aufgrund lizenzrechtlicher Bindungen steht ihm auch kein Weg offen, die Basisprodukte nach eigenen Bedürfnissen anzupassen. Da das Microsoft-Ökosys-

tem bewusst geschlossen aufgebaut ist, also auch die Standards und Schnittstellen nicht darauf angelegt sind, Konkurrenzprodukte einzubinden, kann der Staat seine IT-Landschaft auch nur begrenzt modular aufbauen. Da die Software proprietär ist, sind es auch die Updates. Der Staat kann nicht prüfen, was im Einzelnen auf die Rechner und Server der deutschen Verwaltung ausgerollt wird, wenn Microsoft ein Produkt- oder Sicherheitsupdate verschickt. Die Produktanpassungen erfolgen global, in Privathaushalten und großen Unternehmen, und sind allenfalls peripher an den Bedürfnissen deutscher Behörden orientiert. Wenn Updates ausgespielt werden, kann der Staat nicht aus eigener Kraft zuverlässig prüfen, ob Sicherheitslücken oder Hintertüren im Code vorhanden sind und die IT-Infrastruktur angreifbar machen. Aus diesem Grund darauf zu verzichten, die Softwareanwendungen regelmäßig zu erneuern, wäre aber auch keine gute Idee. Denn ohne Updates werden die Produkte zunehmend unsicher, u.a. weil bereits bekannte Sicherheitslücken (sog. n-days) offenblieben und die Systeme so gleichsam sperrangelweit für mög-

> **Da Deutschland mangels eigener Verhandlungsmasse keinen Einfluss auf die Update-Politik und Produktentwicklung von Microsoft hat, ist der Einfluss auf die eigene digitale Arbeitsumgebung erheblich geschmälert.**

liche Angreifer offen stünden. Da Deutschland mangels eigener Verhandlungsmasse keinen Einfluss auf die Update-Politik und Produktentwicklung von Microsoft hat, ist der Einfluss auf die eigene digitale Arbeitsumgebung erheblich geschmälert.

2. IT-Sicherheit und Cybersicherheits-Vorfälle

Eine Konsequenz davon, dass sich die Verwaltung so tief in das Microsoft-Ökosystem begeben hat, ist: Es liegt außerhalb der eigenständigen Kontrolle des deutschen Staats, ob öffentliche Datenbestände auf Microsoft-Servern dauerhaft sicher sind – vor einem Zugriff durch (ausländische) Hacker, oder durch US-Nachrichtendienste. Wenn Microsoft nicht nur einzelne Softwareanwendungen anbietet, sondern die deutsche Verwaltung weite Teile ihrer digitalen Arbeitsabläufe über komplette Microsoft-Cloud-Umgebung abwickeln sollte, entstünden auch mehr Angriffspunkte auf die Exekutive.

Einige gravierende Sicherheitsvorfälle in der jüngeren Vergangenheit haben gezeigt: Die Treue zum Microsoft-Ökosystem lässt sich nicht (mehr) dadurch erklären, dass der Konzern gleichsam der einzige Garant für IT-Sicherheit in komplexen Organisationen ist. Für Schlagzeilen sorgte es beispielsweise, dass einer der Masterkeys für die Verschlüsselung der Azure-Cloud in China landete. Dadurch erhielt die Hackergruppe Storm-0558 laut BSI „Zugang zu E-Mail-Konten von 22 Organisationen und staatlichen Einrichtungen, vorrangig in den USA, nicht jedoch in Deutschland (...).“ Mutmaßlich habe der Schlüssel aber auch verwendet werden können, um einen Zugang auf andere Cloud-Services von Microsoft zu eröffnen. Die Cybersecurity and Infrastructure Security Agency (CISA) in den USA warf Microsoft in einem Untersuchungsbericht „vielfaches Versagen bei der Cybersicherheit vor“, wie heise.de berichtete.

Zwar hat der Microsoft-Konzern erkannt, dass er ein Manko im Bereich der IT-Sicherheit hat – und ist strategische Partnerschaften mit internationalen IT-Sicherheitsfirmen eingegangen oder hat diese aufgekauft. Der IT-Sicherheitsexperte *Sandro Gaycken* beschrieb gegenüber dem rbb, dass die großen Digitalkonzerne „Cybersecurity-Firmen gekauft, konsolidiert und in ihre Produkte integriert“ haben. Durch die Integration bei Microsoft habe etwa das Unternehmen Crowdstrike „einen Marktanteil von 14 Prozent bekommen“, so Gaycken. Ebendiese Partnerschaft mit Crowdstrike ging im Jahre 2024 aber nach hinten los. In einem Sicherheitsupdate von Crowdstrike für Microsoft-Anwendungen befand sich fehlerhafter Code. In der Folge fielen Systeme aus und waren sensible Systeme für Angreifer offen. Betroffen waren nach Angaben des Konzerns weltweit 8,5 Millionen Windows-Geräte, darunter laut BSI auch Betreiber kritischer Infrastrukturen in Deutschland. Die Opposition im Bundestag ging im Zuge der zögerlichen Aufklärung sogar so weit, Microsoft als „nationales Sicherheitsrisiko“ zu beschreiben.

In geopolitisch turbulenten Zeiten, in denen sich die Welt zunehmend in einem hybriden Krieg und eskalierenden Handelsstreits befinden, ist zu erwarten, dass die Angriffe auf sensible Infrastrukturen künftig eher zu- als abnehmen werden. Von jedem Cyberangriff auf und jede Schwachstelle bei Microsoft kann dann reflexhaft stets auch die deutsche Verwaltung betroffen sein, wenn sie auf deren digitale Infrastruktur zurückgreift.

Der IT-Sicherheitsexperte Sandro Gaycken sieht vor diesem Hintergrund nur eine Lösung: „Man muss die Abhängigkeit von diesen ganz starken Marktführern reduzieren." Er fügt aber zugleich als Warnung hinzu, dass man „ein sehr großes Risiko" eingehe und aufpassen müsse, „mit billigeren Lösungen" nicht „noch schlechter" zu fahren

3. Offene datenschutzrechtliche Fragen bei der Nutzung von Microsoft 365

Wenn die öffentliche Verwaltung personenbezogene Daten der Bürger:innen und ihrer eigenen Bediensteten verarbeitet, ist sie unmittelbar dem Grundrecht auf informationelle Selbstbestimmung bzw. dem Datenschutzgrundrecht unterworfen. Die Datenschutz-Grundverordnung der EU verfolgt das Ziel, „ein hohes Datenschutzniveau zu gewährleisten" (Erwägungsgrund 6 Satz 5 DSGVO) und die „Grundrechte und Grundfreiheiten" der Bürger:innen und „insbesondere ihr Recht auf Schutz personenbezogener Daten ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsorts" zu wahren (Erwägungsgrund 2 Satz 1 DSGVO). Nutzt die Verwaltung Softwareanwendungen eines Unternehmens, um ihre öffentlichen Aufgaben zu erfüllen, müssen auch diese Programme nachweisbar den datenschutzrechtlichen Vorgaben entsprechen. Da Microsoft-Software in den USA entwickelt wird und als Produkt teilweise bereits vor Inkrafttreten der DSGVO auf dem Markt verfügbar gewesen ist, stellen sich komplizierte rechtliche Fragen. Statt eine digitale Arbeitsumgebung für die Verwaltung nach dem Motto „Privacy by Design" (Art. 25 DSGVO) neu aufzusetzen, drehen sich datenschutzrechtliche Analysen deshalb oftmals darum, welche Funktionen der Microsoft-Produkte mit datenschutzrechtlichen Vorgaben in Einklang zu bringen sind – und welche nicht. Frei nach dem Motto: Was nicht passt, wird passend gemacht. Auch dies ist letztlich ein Ergebnis fehlender eigener Verhandlungsparität des deutschen Staates: Wo ein Anbieter das Monopol über Software- und Cloud-Produkte hat, wird es immer schwieriger, eigene datenschutzrechtliche Bedingungen durchzusetzen und effektiv zu überprüfen.

Dieses Dilemma hat verschiedene juristische Unsicherheiten zur Folge: An der Frage, ob der Einsatz der cloudbasierten Anwendung Microsoft365 in der Verwaltung mit der DSGVO vereinbar ist, scheiden sich seit jeher die Geister. Zahlreiche Datenschützer – darunter die Datenschutzkonferenz (DSK) der deutschen Aufsichtsbehörden – vertreten die Auffassung, dass die Anwendungen von Microsoft365 generell nicht datenschutzkonform einsetzbar seien. Die DSK kam im November 2022 zu folgender Feststellung: „Solange insbesondere die notwendige Transparenz über die Verarbeitung personenbezogener Daten aus der Auftragsverarbeitung für Microsofts eigene Zwecke nicht hergestellt und deren Rechtmäßigkeit nicht belegt wird, kann dieser Nachweis nicht erbracht werden." Im Zentrum der Kritik stehen neben der mangelnden Transparenz über die Funktionen und Datenflüsse der Anwendung auch nicht nachvollziehbare Datentransfers und die umfangreiche Diagnosedaten-Erfassung durch Microsoft „im Hintergrund".

Im Juli 2025 kam der Europäische Datenschutzbeauftragte nach einem langen Prüfverfahren im Hinblick auf die Nutzung von Microsoft365 durch die EU-Kommission zu einer anderen Auffassung. Einem Einsatz von Microsoft365 stünden nach zahlreichen Anpassungen technischer und rechtlicher Natur aus seiner Sicht keine Einwände mehr entgegen. Der Europäische Datenschutzbeauftragte argumentiert, dass „zusätzliche vertragliche, technische und organisatorische Maßnahmen, die in Zusammenarbeit mit Microsoft umgesetzt wurden oder geplant sind in Zusammenarbeit mit Microsoft" die datenschutzrechtlichen Bedenken ausgeräumt hätten. Dahinter steht die Überzeugung, dass es durch feinteilige Analysen der Softwareumgebung von Microsoft365 möglich sei, die Bedingungen für Produktanpassungen zu formulieren, die Microsoft365 in Einklang mit der DSGVO bringen würden. Die genauen Dokumente und Zusicherungen, die Microsoft im Rahmen des Verfahrens bereitgestellt hat, sind der Öffentlichkeit aber nicht zugänglich. Es bleibt auch unklar, ob sich andere Aufsichtsbehörden oder gar Gerichte der Einschätzung anschließen. Im Ergebnis wird durch die Entscheidung des europäischen Datenschutzbeauftragten nicht der Datenschutz durch das faire Aushandeln der Rahmenbedingungen für den Cloud-Einsatz verbessert, sondern nur an den Problemen herumgedoktert, ohne die eigentliche Ursache zu beheben, die unter anderem auch in der Monopolstellung des Unternehmens zu verorten ist – die Folge eines jahrzehntelangen Aufbaus der Abhängigkeiten von einem einzelnen Anbieter.

Kapitel 3:

IT can't live – with or without Microsoft? Einmal Cloud mit „souverän", bitte!

Eine digitalisierte öffentliche Verwaltung ganz ohne Microsoft – das gibt es derzeit nicht. Weder in Deutschland noch im internationalen Vergleich. Den Startvorteil, den Bill Gates mit seinem Firmenimperium im Bereich Home- & Work-Computing aufgebaut hat, hat bislang niemand aufgeholt – auch im Cloud-Zeitalter scheint sich daran zunächst nicht viel zu ändern. Nur China kann im Cloud-Markt mit *Alibaba Cloud* und *Tencent Cloud* offenbar auf einheimische Lösungen zurückgreifen.

Doch ist die Abhängigkeit der deutschen Verwaltung von Windows, Office und Teams in Stein gemeißelt?

Klar ist: in einer idealen Welt wäre der deutsche Staat nicht auf einzelne Anbieter angewiesen und könnte sich aus dem Produktportfolio unterschiedlichster IT-Anbieter das passende Angebot zusammenbauen. Laptop von hier, Betriebssystem von da, Office-Umgebung von dort und Mailserver von anderer Stelle – und alles lässt sich interoperabel miteinander verbinden und modular auswechseln. Offene Schnittstellen wären Standard. Als Ankerkunde könnte der Staat sichere und einfach zu bedienende Lösungen beauftragen und sich so maßschneidern lassen, dass sie den regulatorischen und nutzerorientierten Bedürfnissen der Verwaltung entsprechen. Es gäbe Multi-Cloud-Infrastrukturen und klare Open-Source-Pflichten in den Vergabebedingungen. Es gäbe keine Zweifel darüber, dass staatliche Daten nicht in Drittländer übertragen oder die Softwareumgebung per Fernzugriff von einem anderen Kontinent kontrolliert oder gar abgeschaltet werden kann.

Doch die Realität ist: deutsche Behörden haben sich tief in das Microsoft-Ökosystem begeben und sind weiterhin auf die Software des Konzerns für die tägliche Arbeit angewiesen. Ein über das Knie gebrochener Umstieg, gleichsam von heute auf morgen, ist daher realistisch kaum möglich. Aber auch Alleingänge einzelner Bundesländer können sich, wenn sich auf Dauer niemand anschließt, zur Einbahnstraße werden. Denn eigentlich müssten alle Akteure gemeinsam einen so großen Wandel einleiten – und dabei auch gemeinsam die besten Konditionen definieren, vertraglich einfordern und auf gute Preise drängen sowie gemeinsame Schnittstellen für den Austausch im föderalen Staat etablieren. Doch warum passiert das nicht?

In den 1990er Jahren gab es im Bereich der digitalen Büroausstattung zwei Grafschaften: Microsoft und Apple. Sie bauten auf der Basis von Betriebssystemen zwei konkurrierende Reiche, die miteinander – bis heute – kaum interoperabel sind. Da die deutsche Verwaltung dem Gebot der Wirtschaftlichkeit unterliegt, setzte sich in den Amtsstuben der günstigere PC-Arbeitsplatz mit Microsoft Windows und Microsoft Office als Standard durch. Damit begann die Ära der Softwarelizenzen. Die Praxis sah meist so aus: Microsoft vergab Lizenzen an seinen Produkten selbst oder über Drittunternehmen und etablierte dadurch wirtschaftliche Beziehungen und Lieferketten mit nahezu allen deutschen Behörden, die sich digital ausrüsten wollten. Das strategisch angelegte Vertriebsnetz aka Microsoft-Ökosystem hat sich schnell etabliert und dominiert die Entscheidungen in kommunalen und staatlichen Vergabeabteilungen bis heute. Das zugehörige Feld der IT-Beschaffung hat sich parallel zur digitalen Transformation erst über die Jahre rechtlich, organisatorisch und strategisch entwickelt.

Da die deutsche Verwaltung dem Gebot der Wirtschaftlichkeit unterliegt, setzte sich in den Amtsstuben der günstigere PC-Arbeitsplatz mit Microsoft Windows und Microsoft Office als Standard durch. Damit begann die Ära der Softwarelizenzen.

Immer wieder gab es – auch groß angelegte – politische Strategien, um sich aus bestehenden Abhängigkeiten zu lösen und einen souveränen Schritt ins Cloud-Zeitalter zu finden. Im Bereich des Cloud-Computing wimmelt es gerade so an Ideen und Strategieansätzen:

- von der IT-Konsolidierung Bund,
- über Multicloud-Strategien wie die „Deutsche Verwaltungscloud“
- oder den „Sovereign Cloud Stack“.
- Initiativen im Bereich „Cloud Computing“ auf EU-Ebene
- Die „Open Source Week“ auf Ebene der UNO im Jahre 2025

Doch von Strategiepapieren, Pin-Wänden, Mindmaps und schönen Präsentationsfolien bis hin zu einem Kurswechsel im digitalen Maschinenraum der Verwaltung ist es ein weiter Weg. Ohne politische Führung, also die notwendige Durchsetzungskraft „von oben“ auch gegen Widerstände von innen und außen, sowie ein tiefgreifendes Wissen über das bestehende Ökosystem und mögliche Alternativen, kann ein solches IT-Großprojekt nicht gelingen.

Die föderalen Strukturen in Deutschland erschweren es zusätzlich, einen politischen Konsens darüber zu finden, zu neuen Ufern aufzubrechen, eine offene und modulare Verwaltungs-IT auf den Weg zu bringen, und bestehende Abhängigkeiten hinter sich zu lassen. Denn Ländern und Kommunen steht es grundsätzlich frei, wie sie ihre Behörden personell und technisch ausstatten. Dies führt dazu, dass jeder mehr oder weniger sein eigenes Süppchen kocht: Manche Behörden arbeiten bereits mit Microsoft365 und kommunizieren intern über MS Teams; andere setzen offene Videokonferenz-Lösungen und Messenger ein, betreiben ihre Mailserver aber mit MS Exchange; wieder andere sind noch auf dem Stand der on-premise Lizenzen von Outlook, Word, Powerpoint und Co ohne Cloud-Anbindung. Derweil bieten Microsoft, SAP und andere die sog. Delos-Cloud an, über die sich Microsoft365 in einer Cloud, die nicht auf Microsoft-Servern gehostet ist, sondern bei einer Tochtergesellschaft der SAP, betreiben lässt (dazu sogleich).

Und wenn der bewährte Microsoft-Vertriebspartner im IT-Referat vorbeikommt, und die neuen Möglichkeiten anpreist, ist so mancher Amtsleiter verleitet, die notwendigen „Innovationen“ einfach im Hause Microsoft zu kaufen. Die Corona-Pandemie hat die Entwicklung noch verstärkt. Mit den Kontaktverboten und Behördenschließungen war klar: Die Verwaltung muss arbeitsfähig bleiben – und dafür muss sie digital kommunizieren, Daten teilen und gleichzeitig an die bestehende Infrastruktur angeschlossen bleiben. Auf Microsoft zu setzen, war hier aus Sicht vieler Entscheidungsträger:innen der sicherste und schnellste Weg. Es wurden erneut Fakten geschaffen, die sich – nun wo Microsoft365 oder Teams ja „schon da“ sind – nicht mehr ohne Weiteres zurückdrehen lassen.

Im Ergebnis ist die Wahlfreiheit für europäische Nutzer durch gezielte Lizenz- und Bündelungstaktiken, konstantes Lobbying und durch Geschäftsmodelle, die durch Lock-In- und Plattform-Effekte Marktdominanz erlangt haben, faktisch erheblich geschmälert. Zwar arbeiten alternative IT-Konzerne im Rahmen von Vergabeverfahren bereits zusammen, um ebenjene Monopolisierung im Cloud-Sektor aufzubrechen, dass die Unternehmen jedoch dazu bereit sind, von sich aus an einem Strang zu ziehen, ist derzeit aber noch nicht in Sicht. Im Juni 2025 meldete Reuters, dass Telekom, IONOS und Schwarz ihren Hut nicht als gemeinsames Konsortium für neue EU Programme in den Ring werfen wollen. Ein klug aufgesetztes und föderal abgestimmtes Verfahren, um eine offene Alternative zu Microsoft Office und der Microsoft-Cloud-Umgebung in einem Konsortium zu entwickeln und zu betreiben, könnte indes die digitale Arbeitsplattform der öffentlichen Verwaltung der Zukunft in einem offenen, freien und funktionierenden digitalen Ökosystem hervorbringen.

Kapitel 4:

Produktanpassungen und Angebote von Microsoft zwischen ernsthaftem Bemühen und Souveränitäts-Washing

Um auf die datenschutzrechtliche, digitalpolitische und wettbewerbsrechtliche Kritik an seinem Geschäftsmodell zu reagieren und um die politische Entscheidungsträger:innen davon zu überzeugen, dass Microsoft-Produkte weiterhin die beste Wahl für die deutsche Verwaltung sind, hat der Konzern diverse Anpassungen an seinen Produkten vorgenommen oder vorgeschlagen.

I. Europäisches Sicherheitsprogramm

Im Juni 2025 hat Microsoft ein „Europäisches Sicherheitsprogramm“ angekündigt. Im Rahmen des Programms will Microsoft KI-gestützte Bedrohungsinformationen verstärkt mit Regierungen teilen und sicherheitsrelevante Daten in Echtzeit bereitstellen, die u.a. als Folge von fortlaufenden Cyberangriffen auf das Microsoft-Ökosystem generiert wurden. Der Konzern will durch das Programm in lokale Cybersicherheitskapazitäten und die digitale Resilienz von Staaten, Behörden und der Zivilgesellschaft investieren. Durch neue Partnerschaften mit Strafverfolgungsbehörden und Organisationen wie Europol sollen Cyberkriminelle und staatlich gesteuerte Angriffe effektiver bekämpft werden. Bösartige Infrastrukturen und Angriffsszenarien will Microsoft schneller erkennen und automatisch deaktivieren.

Angesichts der hybriden Bedrohungslage im Cyberraum, auf die BSI, Nachrichtendienste und Sicherheitspolitiker:innen seit vielen Jahren hinweisen, ist es durchaus eine sinnvolle Maßnahme, dass Microsoft seine Kapazitäten eines global agierenden Konzerns nutzt, um die Sicherheit staatlicher IT-Systeme zu unterstützen. Insbesondere gegen neue Formen von Cyberangriffen, die mit KI orchestriert und durchgeführt werden, will Microsoft kostenlose Hilfe anbieten. Gleichzeitig wirkt das Europäische Sicherheitsprogramm ein Stück weit wie eine Marketingkampagne. Denn mit mehreren Sicherheitsvorfällen rund um Crowdstrike und den Masterkey für die Azure-Cloud hatte Microsoft in den Jahren zuvor eher negative Schlagzeilen gemacht (siehe oben). Jetzt bietet Microsoft in unsicheren Zeiten mit einem Mal seine Unterstützung als IT-Grandseigneur, um den europäischen Kontinent in stürmischen Zeiten im digitalen Raum zu schützen.

II. Individuell ausgehandelte Datenschutzbedingungen

Die Datenschutzbehörden auf nationaler und auf EU-Ebene haben beim Einsatz von Microsoft-Produkten, insbesondere mit Blick auf das cloudbasierte Microsoft365, stets moniert, dass nicht genügend Transparenz und Kontrolle über die Datenflüsse im Maschinenraum von Microsoft bestünde (siehe oben). Als international agierender Konzern hatte Microsoft darüber hinaus mit der Herausforderung zu kämpfen, für jede Weltregion und jedes regulatorische Umfeld maßgeschneiderte und hinreichende Datenschutzbedingungen zu formulieren – und die Produktpalette technisch anzupassen.

Wenn Organisationen Standardsoftware kaufen, haben sie im Umgang mit internationalen Großkonzernen oftmals keine Möglichkeit, die Bedingungen individuell zu verhandeln – sondern sie müssen sich mit den allgemeinen Datenschutzbedingungen auf ihrem Markt oder in ihrem Sektor begnügen. Diese Abhängigkeit von Standardklauseln in Datenschutzbedingungen haben einige Landesregierungen nach der Kritik der Landesbeauftragten für Datenschutz und Informationsfreiheit (LfDI) und der DSK nunmehr aufgebrochen, wie das Computermagazin c’t 2024 berichtete.

So hat das Land Niedersachsen Sonderregeln mit Microsoft ausgehandelt. Darin hat Microsoft zugesagt,

dass man die Datenspeicherung und -verarbeitung nur auf europäischen Servern durchführen würde, während der IT-Support nur aus Ländern stammt, die es ermöglichen „DSGVO-konform“ mit Microsoft zusammenzuarbeiten. Datenabflüsse aus den EU-Servern und eine Datenübertragung in die USA für „Hintergrundanalysen“ bzw. Support wären dann weiterhin vertragsgemäß möglich, aber im Umfang tendenziell reduziert. Ein Teil individueller Bedingungen könnte auch darin bestehen, dass nur bestimmte Kategorien an Daten für Support-Zwecke verarbeitet und übermittelt werden, wie es offenbar die EU-Kommission mit Microsoft ausgehandelt hat. Doch auch dann bliebe es fraglich, ob die Zusicherung und die tatsächliche Praxis wirklich kompatibel sind. Ungelöst bliebe auch das „Cloud Act“-Problem.

Darüber hinaus stellt Microsoft in Niedersachsen einzelne Dienste, die besonders intransparent im Hintergrund wirken, ab – z.B. Diagnosedaten und Teams Analytics. Auch hier bleibt jedoch offen, ob allein dadurch große Datenabflüsse effektiv untersagt werden bzw. hinreichend kontrollierbar sind und wie die Verwaltung reagieren würde, wenn Microsoft seine Preise später drastisch erhöht oder die Lizenzen oder Abo-Modelle deaktiviert oder beschränkt.

Darüber hinaus wollen die Behörden durch interne Arbeitsanweisungen im Umgang mit Microsoft-Produkten sicherstellen, dass bestimmte besonders sensiblen Daten – z.B. Sozial- oder Gesundheitsdaten – nicht über MS Teams verarbeitet und ausgetauscht werden. Da der Faktor Mensch oft die größte Schwachstelle ist, und sich solche rein internen Vorgaben nur schwer durchsetzen bzw. flächendeckend kontrollieren lassen, verbleibt jedenfalls eine nicht unerhebliche Restunsicherheit.

III. Die Delos-Lösung: Rechenzentren durch europäische Firmen betreiben lassen – (nur) Software kommt von Microsoft

Was wäre aber, wenn cloudbasierte Microsoftprodukte à la Microsoft365 auf abgeschirmten Rechenzentren europäischer Unternehmen bereitgestellt würden, an die nur öffentliche Stellen angebunden sind? Dadurch wäre theoretisch sichergestellt, dass ein Datenrückfluss in die USA „im Hintergrund“ vollständig gekappt ist. Selbst wenn die US-Regierung den Konzern dazu auffordern würde, europäische Daten bereitzustellen, wäre Microsoft dazu faktisch nicht in der Lage. Denn die Kontrolle läge allein bei den Betreibern der Rechenzentren.

Ein Konsortium aus Microsoft, SAP und Arvato hat sich auf den Weg gemacht, um das Dilemma der internationalen Datentransfers zu knacken. Eine Behörde könnte Clouddienste von Microsoft dann über die Delos GmbH buchen, die als Tochterfirma unter der Kontrolle des deutschen Internetriesen SAP steht – und würde es vermeiden, Software und Infrastruktur vom Microsoft-Konzern direkt zu beziehen und auf dessen Infrastruktur betreiben zu lassen. Eine ähnliche Lösung gibt es in Frankreich: Capgemini und Orange haben dort das Joint Venture „Bleu“ gegründet. Das Versprechen von Bleu und Delos lautet: Rechenzentren und Daten unter nationaler Kontrolle, von Microsoft aus den USA kommen nur noch die Software-Updates. Es klingt auf den ersten Blick verlockend, wenn die SAP Tochter Delos verspricht:

> „Die Dienste der souveränen Cloud-Plattform umfassen dabei insbesondere die umfangreichen Kollaborations-Tools und Produktivitätslösungen von Microsoft Office 365. Die Cloud-Plattform wird gemäß den regulatorischen Vorgaben des Bundes technisch, operativ und rechtlich souverän sein. Damit wird Delos Cloud als derzeit einziges Cloud-Angebot die Vorgaben des BSI für IT-Sicherheit und Geheimschutz sowie die gesetzlichen Vorgaben für Datenschutz in Abstimmung mit der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) vollumfänglich erfüllen. Als Eigentümerin der Infrastruktur übernimmt die Delos Cloud GmbH sowohl den Plattform-Betrieb als auch die Lizenzierung ihrer Produkte.“

Ein Nachteil des Unternehmenskonstrukts: Die Preise sind 15 Prozent teurer als die „Microsoft pur“-Variante mit der gängigen Microsoft Cloud, wie die Computerwoche berichtet. Der höhere Preis ist ökonomisch nachvollziehbar, schließlich steckt in den Delos-Clouds weitaus mehr Aufwand als nur ein einfacher Lizenzkauf aus der gängigen Microsoft-Produktpalette. Aus Sicht der einzelnen Landes- oder Kommunalbehörde entstünde dann jedenfalls die Wahl zwischen „Microsoft

pur“ über den BMI-Rahmenvertrag und der teureren Variante „Delos“ – im Ergebnis führten aber erneut alle Wege zu Microsoft.

Ob die Lösung aber wirklich effektiv vor Datenabflüssen an US-Sicherheitsdienste, Hackerangriffen aufgrund mangelnder IT-Sicherheit oder härteren Bandagen in Handelskonflikten mit der Trump-Regierung schützt, steht jedoch bislang auf einem anderen Blatt. Der Delos-Chef Georges Welz berichtete in einem Interview mit heise: „Da die Cloud unter unserer Kontrolle ist, kann niemand unmittelbar den Betrieb einschränken. Und falls es keine Updates mehr geben sollte, könnten wir über Monate weiterarbeiten, weil die Cloud auch autark funktioniert. Insofern bieten wir durchaus Souveränität, nämlich einen Handlungszeitraum, um zu reagieren.“ Damit ist bereits angedeutet, dass im worst case kein langfristiger Betrieb der Delos-Cloud mehr möglich wäre. Dadurch wäre de facto die Arbeitsweise der gesamten Verwaltung in Gefahr. Der Übergangszeitraum, den Welz als „über Monate“ angibt, könnte im Grunde auf 0 Tage abschmelzen, wenn beispielsweise bekannt würde, dass das letzte Update der Systeme – etwa wie im Fall Crowdstrike (s.o.) – zu einer offenen Sicherheitslücke geführt hat.

Und völlig unabhängig von den vorgenannten technischen Argumenten tritt auch hier wieder hinzu: Eine teilsouveräne Lösung wie Delos würde Deutschland keineswegs unabhängiger in seinen Beschaffungsentscheidungen machen, denn der Staat als Primärkunde wäre weiterhin an die Software des Konzerns und seine restriktiven Lizenzbedingungen gebunden. Trotz des juristischen Konstrukts, mit dem Unternehmen Delos einen Vermittler aus Deutschland einzusetzen, würden am Ende alle technischen Wege wieder zu Microsoft zurückführen. Im Ergebnis mag die Lösung somit zwar den Anschein digitaler Souveränität erwecken, in Wirklichkeit aber bestehen die alten Abhängigkeiten nur in neuem Gewand weiter fort.

IV. Datengrenze und lokale Instanzen

Um auf die Befürchtung zu reagieren, dass die US-Regierung auf die Datenbestände und Kommunikationsinhalte der öffentlichen Verwaltung zugreifen könnte, hat Microsoft drei weitere Maßnahmen angekündigt: eine Datengrenze, Data Guardians und lokal betriebene Instanzen.

Zum einen will Microsoft in seine komplexen Verarbeitungsabläufe eine sog. „Datengrenze“ für das Angebot „Sovereign Public Cloud“ einziehen. Inhaltlich deckt sich das insofern mit den von Niedersachsen individuell verhandelten Datenschutzbedingungen, dass alle Kundendaten nur innerhalb der EU-Grenzen verarbeitet werden. Hinzu kommt eine Anpassung beim für die Datensicherheit wichtigen Thema Verschlüsselung: Der Masterkey („Verschlüsselungschlüssel“) soll ausschließlich beim Auftraggeber verbleiben.

Mit der Maßnahme „Data Guardian“ verspricht Microsoft, dass Admin-Zugänge zu den europäischen Cloud-Diensten nur noch durch Microsoft-Mitarbeiter mit Wohnsitz in Europa ausgeübt werden. Sollte es notwendig sein, dass in bestimmten Fällen – z.B. für komplizierte Support-Fragen – ein Fernzugriff aus den USA erfolgt, soll dies nur mit ausdrücklicher Genehmigung der europäischen Kollegen und strikter Protokollierung möglich sein. Auf diese Weise soll es seltener der Fall sein, dass Personen außerhalb der EU Zugriff auf die Cloud-Infrastruktur erhalten.

> **Mit „Microsoft 365 Local“ soll es laut Microsoft zudem auch künftig eine Möglichkeit geben, dass die Softwareumgebung ohne feste und dauerhafte Anbindung an die Microsoft Cloudumgebung läuft.**

Mit „Microsoft 365 Local“ soll es laut Microsoft zudem auch künftig eine Möglichkeit geben, dass die Softwareumgebung ohne feste und dauerhafte Anbindung an die Microsoft Cloudumgebung läuft. So wäre der Betrieb auf eigenen Infrastrukturen weiterhin möglich, wenn es aus Sicht der Behörden keinen Grund dafür gibt, eine cloudbasierte Lösung in Anspruch zu nehmen. Ist das am Ende eine Abkehr von der Ankündigung, ab 2029 keine on-premise-Software mehr anzubieten und fortzuentwickeln – oder eine Integration einer irgendwie stärker abgesicherten Microsoft365-Local-Variante „für Abo- bzw. Cloud-Produkte“, die *Andreas Thys* in seinem Gastbeitrag als „skurril“ beschreibt?

Selbst wenn die Datenverarbeitung künftig ausschließlich innerhalb der EU unter der Verantwortung von

EU-Tochtergesellschaften, die vollständig der DSGVO unterliegen erfolgen sollte, bleibt die Frage offen, wie „souverän" solche Maßnahmen die öffentliche Verwaltung mittel- bis langfristig wirklich machen. Aus Sicht von Andreas Thyen sind die „nun präsentierten Gegenmaßnahmen – EU Data Boundary, Data Guardian, lokal betriebene Instanzen – (...) gezielte PR Maßnahmen. Man erhofft sich maximale Kontrolle, ohne die technische Souveränität abgeben zu müssen." Der Research Director des cyberintelligence.institute Prof. Dr. Dennis-Kenji Kipker kommt zu dem Schluss: „Die Sicherheitsversprechen sind auf Sand gebaut". Denn, so Kipker in einem Kommentar bei IT Daily, handele es sich bei näherem Hinsehen weder um eine echte Datengrenze noch um die Hoheit des Nutzers über seine eigenen Daten, die in der Cloud von Microsoft gespeichert sind. Noch dramatischer drückt es Prof. Dr. Harald Wehnes, Sprecher des Präsidiumsarbeitskreises „Digitale Souveränität" der Gesellschaft für Informatik e. V. aus: „Unter dem Deckmantel der ‚digitalen Souveränität' verfolgen Tech-Konzerne ganz klar das Ziel, Europa in irreversible und teure Scheinlösungen zu locken. Diese sollen ihre Marktmacht festigen und am Ende sogar mehr Kontrolle über Daten

> **Im Ergebnis spielt es somit keine Rolle, welchen Weg Microsoft geht – am Ende vertiefen auch die vorgeschlagenen „Alternativmaßnahmen" die Abhängigkeit weiter und binden die Kunden noch stärker an eine geschlossene Umgebung, die dem Gegenteil von digitaler Souveränität entspricht.**

und Technologien ermöglichen." Diese Aussagen machen deutlich: Im Ergebnis spielt es somit keine Rolle, welchen Weg Microsoft geht – am Ende vertiefen auch die vorgeschlagenen „Alternativmaßnahmen" die Abhängigkeit weiter und binden die Kunden noch stärker an eine geschlossene Umgebung, die dem Gegenteil von digitaler Souveränität entspricht. Die zugrunde liegende Dominanz von Microsoft und dessen Fähigkeit, Bedingungen zu diktieren und Kunden durch Lizenzen und andere Mittel an sich zu binden, ändert sich durch die Vorschläge in keinster Weise.

Kapitel 5:

Zusammenfassung und Handlungsempfehlungen

Microsoft-Produkte dominieren die Arbeitsumgebung der öffentlichen Verwaltung. Auch im Zukunftsmarkt des Cloud Computing will der Platzhirsch seine Marktanteile im öffentlichen Sektor behalten und ausbauen. Denn je vernetzter die Verwaltung agiert, desto wichtiger wird es, Dokumente nicht allein in behördlichen Silos lokal zu bearbeiten und zu speichern, sondern IT-Systeme kollaborativ digital über Behördengrenzen hinweg zu nutzen. Mit seiner Ankündigung, ab 2029 konsequent auf Abo-Modelle mit obligatorischer Azure-Subscription zu wechseln, hat Microsoft die deutsche Verwaltung unter Zugzwang gebracht. Gleichzeitig öffnet sich dadurch ein Zeitfenster, um einen strategischen Wechsel in ein offenes, sicheres und souveränes digitales Arbeitsumfeld für die öffentliche Verwaltung strategisch zu planen und stufenweise umzusetzen. So ließen sich die politischen Prioritäten digitale Souveränität, Datenschutz und Cybersicherheit in der Umsetzung durch maßgeschneiderte Lösungen realisieren, statt in einem geschlossenen Ökosystem mit strategischen Nachteilen zu verharren.

> **Mit seiner Ankündigung, ab 2029 konsequent auf Abo-Modelle mit obligatorischer Azure-Subscription zu wechseln, hat Microsoft die deutsche Verwaltung unter Zugzwang gebracht.**

Da Microsoft seine Marktanteile im öffentlichen Sektor weiter ausbauen und im Bereich Cloud Computing verfestigen will, reagiert der Konzern mit seiner gesamten Marketing-Power auf die vielschichtige Kritik und öffentlich debattierte Sicherheitsvorfälle. Auf dem politisch skizzierten Weg hin zu einer „souveränen Cloud“ in Deutschland und Europa lässt sich insofern ein Katz-und-Maus-Spiel zwischen digitalpolitischer und datenschutzrechtlicher Kritik und immer neuen Ankündigungen des Konzerns beobachten. Auch wenn jede der Maßnahmen einzelne Kritikpunkte aufzugreifen versucht und bestimmte Risiken abmildern will: Die bestehenden Abhängigkeiten der deutschen Verwaltung von der Microsoft-Produktpalette und die Gefahr eines Kontrollverlustes oder erheblicher Datenabflüsse bleibt bestehen.

Die enge Zusammenarbeit der öffentlichen Verwaltung mit Microsoft führt im Ergebnis wiederkehrend zu Kritik in mehreren zentralen Aspekten: Datenschutz und Transparenz, Daten- und Cybersicherheit sowie monopolistischer Cloud-Zwang statt unabhängige Cloud-Strategie. Die umfangreichen Vorschläge und Produktanpassungen, die Microsoft in den letzten Jahren vorgestellt hat, adressieren diese vier zentralen Bedenken jeweils nur teilweise oder rudimentär. Es liegt an der enormen Marktdominanz eines international agierenden Konzerns und dessen Geschäftsmodell aus wettbewerblich seit Jahrzehnten fragwürdigen Verhaltens, geschlossenem Ökosystem und dynamischer Geschäftskonzeptentwicklung sowie Preispolitik, die dem Ziel einer digital souveränen Arbeitsumgebung für die öffentliche Verwaltung in Deutschland im Weg steht. Es ist Zeit für eine strategische Neuausrichtung. Versteht man „digitale Souveränität“ im Wesentlichen als Wahlfreiheit und eigene Steuerungsmöglichkeit der staatlichen IT-Infrastruktur und behördlichen Datenflüsse, kann langfristig nur eine vollständige Neuausrichtung der öffentlichen IT-Landschaft zum politischen Ziel führen.

Das zentrale rechtliche und politische Vehikel, um die konkrete Verflechtung und vertragliche Zusammenarbeit mit Microsoft zu steuern, ist der BMI-Rahmenvertrag mit dem Unternehmen. An den Bedingungen des im Frühjahr 2025 abgeschlossenen Rahmenvertrags lässt sich in den nächsten drei Jahren nichts mehr **kurzfristig** ändern – die Zeit lässt sich aber nutzen, um **mittelfristig** für eine mögliche Verlängerung 2028 bestens aufgestellt und vorbereitet zu sein, und um **lang-**

fristig eine vollständige Neuausrichtung auf das Ziel der „digitalen Souveränität" mit offener Software und einer souveränen Multi-Cloud-Strategie in die Wege zu leiten.

Kurzfristige Maßnahmen bis 2028:

- **Monitoring der Kosten für IT-Beschaffung über den BMI-Rahmenvertrag durch die Bundesregierung**
  Die Bundesregierung und die Digitalministerkonferenz (DMK) sollten sich und der Öffentlichkeit einen präzisen Überblick darüber verschaffen, wie viel Steuergeld Bund, Länder und Kommunen derzeit für Microsoft-Lizenzen insgesamt ausgeben. Neben einer – so weit wie möglich verbindlichen – systematischen Abfrage der jeweiligen Posten bei Bundesbehörden, Ländern und Kommunen, könnten die Finanzbehörden auch die Licensing Solution Partner (LSP) dazu auffordern, offenzulegen, wie viel Umsatz sie mit dem Geschäftsmodell „Lizenzkauf auf der Grundlage des BMI-Rahmenvertrags" jährlich erwirtschaften. Denn ohne zuverlässige Zahlen lässt sich der finanzielle Spielraum für einen Strategiewechsel nicht berechnen und planen.
- **Machbarkeits- und Potentialstudien für die Erhöhung der Wahlfreiheit in einzelnen Produktbereichen**
  Auf Grundlage des Monitorings der Gesamtkosten sollten Bundesregierung und DMK in Machbarkeitsstudien für einen offenen, interoperablen und fairen Cloud-Markt mehrere Szenarien in Richtung Wahlfreiheit und digitale Souveränität sowie deren politische, rechtliche und technische Rahmenbedingungen untersuchen. Ein besonderer Blick sollte hier auf die Produktbereiche Betriebssystem, Bürosoftware, Kommunikation (E-Mail und Messenger), Zusammenarbeit (kollaborative Arbeit an Dokumenten und geteilte Datenablage) und Multi-Cloud-Services fallen, um die bestehende Abhängigkeit von einem einzelnen Anbieter zu lösen. Die ökonomische und technische Untersuchung sollte anhand der jährlichen Ausgaben und derzeitigen IT-Ausstattung für die Zukunft prognostizieren, ob sich Alternativangebote damit strategisch beschaffen und implementieren ließen. Falls Angebotslücken auf dem Markt identifiziert werden, sollte die Untersuchung auch darauf eingehen, wie Bund und Länder diese durch Forschungs- und Unternehmensförderung gezielt schließen könnten. Die Potenzialanalyse sollte auch Interviews mit Unternehmen im Microsoft-Ökosystem, europäischen Wettbewerbern, Vergabestellen in der Landes- und Kommunalverwaltung und mit Verbraucherschutz- und Unternehmensverbänden umfassen, um nicht nur die Zahlen, sondern auch die tatsächliche Geschäftsstrategie näher zu beleuchten.
- **Intensivierung der wettbewerbsrechtlichen Untersuchungen des Microsoft-Ökosystems und der Lizenzvergabe mit Blick auf die öffentliche Verwaltung**
  Das Bundeskartellamt sollte im Rahmen seiner Untersuchungen nach § 19a GWB eine eigenständige Arbeitsgruppe einsetzen, die das Vertriebsnetzwerk des Microsoft-Konzerns und den Einsatz von Microsoft-Produkten in der öffentlichen Verwaltung detailliert in den Blick nimmt. Der Haushaltsgesetzgeber sollte der Behörde ausreichend Ressourcen bereitstellen, um wettbewerbswidrige Monopole zu untersuchen und ggf. aufzubrechen. Eine breit angelegte Untersuchung kann, auch gemeinsam mit der EU-Kommission und anderen Mitgliedstaaten, offenlegen, inwiefern die marktdominante Stellung durch Vertragsbedingungen für Lizenz-, Cloud- und Rahmenverträge, aber auch faktische Einfluss- und Steuerungsmöglichkeiten des Microsoft-Konzerns und seiner oftmals exklusiven Vertriebspartner im Bereich öffentlicher Auftragsvergaben oder bei komplexen Beschaffungsvorgängen aufrechterhalten oder vertieft wird. Alle Geschäftspraktiken, die einem fairen Wettbewerb und echter Wahlfreiheit entgegenstehen – insbesondere einschränkenden Lizensierungsprakiken –, sollten identifiziert und mit angemessenen aufsichtsrechtlichen Maßnahmen verhindert werden.
- **Strategische Digitaldialoge mit internationalen Partnern zur Frage der digital souveränen Verwaltungs-IT**
  Die Bundesregierung sollte strategische internationale Dialogformate aufbauen und forcieren, in denen sich die Bundesrepublik Deutschland mit der EU-Kommission und anderen EU-Mitgliedstaaten (z.B. Italien, Frankreich, Niederlande, Portugal und Estland), aber auch strategischen Partnern weltweit (z.B. Südkorea, Japan, Kanada oder Australien) über den Weg zur einer souveränen Verwaltungs-IT struktu-

riert austauscht. Dabei sollte sie Zivilgesellschaft, Wissenschaft, aber auch europäische Unternehmen und die Open-Source-Community hinzuziehen. Umfang und Reichweite der strategischen Digitaldialoge lassen sich ganz unterschiedlich denken und ausgestalten: Neben einem institutionalisierten Erfahrungsaustausch auf verschiedenen Ebenen über die Sammlung von best practices im Bereich IT-Souveränitäts-Strategien, über gemeinsame Forschungsvorhaben oder gar transnationale Entwicklungsaufträge für einzelne IT-Lösungen bis hin zur Bildung einer gemeinsamen Verhandlungsgruppe für starke und gleichförmige Rahmenverträge mit Microsoft. Wo sich der Microsoft-Konzern mit seinen engmaschigen Vertriebsnetzwerken und hochqualifizierten Anwaltskanzleien einen Verhandlungsvorteil bei Rahmen- und Lizenzverträgen verschaffen konnte, sollen sich öffentliche Auftraggeber durch Erfahrungsaustausch und Wissenstransfer ebenso Verhandlungsvorteile erschließen.

Mittelfristige Maßnahmen für die Verhandlungen zum nächsten BMI-Rahmenvertrag:

- **Wahlfreiheit „light“: Auswahlmöglichkeit zwischen neuen und alten Microsoft-Produkten**
  Es ist ökonomisch nachvollziehbar, dass Microsoft von seinem Modell der unbefristeten Lizenzkäufe nun auf ein Abo-Modell umstellen will. Der Konzern verschafft sich damit vertragsrechtlich mehr Spielraum und kann missbräuchliche Lizenznutzungen effektiver verhindern. Ein Umstieg auf cloudbasierte Lösungen wäre aus Sicht der öffentlichen Verwaltung aber der dritte vor dem zweiten Schritt. Gerade bei Standardsoftware für den Büroalltag verfügt die Verwaltung bereits über Softwarelizenzen und es besteht in vielen Bereichen auch keine dringende praktische Notwendigkeit, den on-premise-Einsatz von Outlook, Office oder Messengern aufzugeben. Dennoch sollte der Staat selbstbewusst verhandeln und dabei auch die Option eines strategischen Wechsels zu Alternativen in die Waagschale werfen. Mit dem angekündigten Wegfall von on-premise-Lösungen ab dem Jahr 2029 und der damit verbundenen Notwendigkeit des erzwungenen Wechsels in die Microsoft-Cloud ist diese Problematik schon jetzt akut und daher ist es zwingend notwendig, so schnell wie möglich die rechtlichen und faktischen Rahmenbedingungen für eine tatsächliche Wahlfreiheit auf dem Cloud-Markt zu schaffen.
- **Kostentransparenz über Lizenzkosten auf allen Ebenen vertraglich verankern**
  Dass Microsoft über genaue Zahlen zu seinem Geschäftsvolumen mit der deutschen Verwaltung verfügt, die Öffentlichkeit aber regelmäßig schätzen muss, wie viel Steuergeld in Micorosoft-Lizenzen fließen, ist ein unhaltbarer Zustand. Die Bundesregierung sollte bei den Verhandlungen zu einem Rahmenvertrag auf ein Monitoring-Instrument bestehen, das es ermöglicht, die jährlichen Ausgaben für Microsoft-Lizenzen oder -Abos niedrigschwellig und öffentlich nachvollziehbar zu dokumentieren. Auf dieser Datengrundlage könnten Bund und Länder viel genauer prognostizieren, welche Preisvorteile und Volumina sie in den jeweiligen Haushaltsjahren benötigen. Im Zusammenspiel der IT-Beschaffer in Bund, Ländern und Kommunen ließen sich Synergieeffekte erzielen und bestehende Informationsasymmetrien gegenüber Microsoft reduzieren. Es entspricht dem Grundsatz der Wirtschaftlichkeit und Sparsamkeit der Verwaltung, mit Steuergeld umsichtig und nachhaltig umzugehen.
- **Modalitäten der Lizenzvergabe an Bedürfnisse der Verwaltung anpassen**
  Zur Vorbereitung der Verhandlungen über einen neuen Rahmenvertrag mit Microsoft sollten sich Bund, Länder und die kommunalen Spitzenverbände – etwa im Rahmen der DMK oder im IT-Planungsrat – gemeinsam sehr gründlich vorbereiten und unter Umständen Hilfe von außen holen. Dazu gehört mindestens, die jeweiligen Bedarfe und Budgets genau zu prognostizieren, sich Gewissheit darüber zu verschaffen, wie stark der Wunsch nach on-premise, Microsoft365 oder Public Cloud jeweils ausgeprägt ist. Darüber hinaus könnte der Staat in Erwägung ziehen, sich Änderungen am bestehenden Vertriebsnetzwerk über Licensing Solution Partner abzubedingen, und bei der Lizenzvergabe selbst eine stärker steuernde Rolle einzunehmen.
- **Verpflichtende Audits und transparente Echtzeit-Analyse der Datenflüsse**
  Die Bundesregierung sollte Microsoft dazu verpflichten, umfangreiche Audits mit Einblick in den

Programmcode zu ermöglichen, bevor neue Softwareanwendungen oder umfangreiche Updates in der öffentlichen Verwaltung zum Einsatz kommen. Nur durch einen echten Einblick lässt sich überprüfen, ob der Datenschutz auf Papier mit den technischen Abläufen im Maschinenraum tatsächlich übereinstimmt. Dem Konzern kann der Staat dafür Vertraulichkeit zusichern. Zudem sollte sich die Bundesregierung dafür einsetzen, dass eine unveränderbare Protokollierung jeglicher Fernzugriffe auf die Microsoft-Infrastruktur stattfindet. Der Staat sollte einen genauen Überblick darüber haben, wann wer zu welchem Grund auf das System zugegriffen hat – und welche Daten dafür in die USA übermittelt wurden.

- **Interoperabilität und offene Schnittstellen als Vertragspflicht**
  Die Bundesregierung sollte aufgrund von Machbarkeitsstudien und den Untersuchungen des Bundeskartellsamts ausloten, an welchen Stellen sie Microsoft in einem Rahmenvertrag zu Interoperabilität mit anderen Produkten und offenen Schnittstellen verpflichten kann. Solange das Microsoft-Ökosystem bewusst geschlossen ist und Lock-In-Effekte ausspielen kann, verfestigt sich die Abhängigkeit, statt sich zu verringern.

  Bei alledem kann die Bundesregierung durchaus auch mit einem Ausstieg aus den Rahmenvereinbarungen bis zu einem bestimmten Stichtag drohen, wenn die geübten Verhandler des Microsoft-Konzerns bestimmte Forderungen abschmettern.

Langfristige Maßnahmen für die Ära digitaler Souveränität in EU und Deutschland:

Die 1990er Jahre, in denen man sich zwischen Apple und Microsoft entscheiden musste, sind längst vorbei – der IT-Markt hat sich stark ausdifferenziert – auch wenn sich das in den Marktanteilen von Microsoft im öffentlichen Sektor aufgrund seiner dominanten Marktstellung nicht widerspiegelt. Deutschland ist langfristig gut beraten, ein funktionierendes und interoperables System mit verschiedenen Anbietern und Produkten aufzubauen – eine Art IT-Kaufhaus, in dem sich die einzelnen Behörden bedienen und die für sie passendste Lösung zusammenbauen können. Mit den – zugegeben inhaltlich noch nicht scharf konturierten – Initiativen „EuroStack“ und „Deutschland Stack“ machen sich Brüssel und Berlin bereits programmatisch auf den Weg hin zu digitaler Souveränität. Den Worten müssen bald Taten folgen. Dabei gilt es aus politischen Misserfolgen wie der Initiative „gaia x“ zu lernen – und Fehler nicht zu wiederholen.

> **Langfristig sollten sich die Bundes- und Landesregierungen fragen: Lassen sich Steuergelder, die jedes Jahr in Lizenzkosten für Microsoft-Produkte fließen, nicht besser in ein vielfältiges Netzwerk von IT-Anbietern investieren, das die übermäßige Abhängigkeit von einem einzigen Monopolisten verringert und digital souveräne Lösungen ermöglicht?**

Langfristig sollten sich die Bundes- und Landesregierungen fragen: Lassen sich Steuergelder, die jedes Jahr in Lizenzkosten für Microsoft-Produkte fließen, nicht besser in ein vielfältiges Netzwerk von IT-Anbietern investieren, das die übermäßige Abhängigkeit von einem einzigen Monopolisten verringert und digital souveräne Lösungen ermöglicht? Dann könnte eine Softwareumgebung und damit eine digitale Arbeitsgrundlage für die Verwaltung entstehen, die für den Staat besser kontrollier- und steuerbar ist. Fachbehörden wie BfDI, Bundeskartellamt und BSI könnten die Anforderungen an Datenschutz, IT-Sicherheit und fairen Wettbewerb definieren – und die konkrete Umsetzung begleiten. Im Ergebnis hätte die Verwaltung Wahlfreiheit, könnte Kosten kurz-, mittel- und langfristig planen. Zur Gewährleistung von Cybersicherheit wäre der Staat nicht mehr auf ein brüchiges Vertrauen angewiesen, dass Microsoft seine Systeme vor Angriffen schützt.

Im besten Fall entstünde eine wettbewerbsoffene digitale Arbeitsumgebung für die öffentliche Verwaltung, die auch andere Staaten in Anspruch nehmen wollen: ein Deutschland-Stack mit einer internationalen Community, stets wachsenden Diensten und den Maximen der Interoperabilität und Modularität als Markenkern. Auf der Grundlage der kurzfristigen und mittelfristigen Maßnahmen, insbesondere einer validen Zahlengrundlage über verwendete Steuermittel und Machbarkeitsstudien, könnte die Bundesregierung ein Datum identifizieren, ab dem der Ausstieg aus dem Microsoft-

Ökosystem hin zu einer souveränen Arbeitsumgebung der Verwaltung stattfinden soll. Auf dieses Ausstiegsdatum könnten alle Akteure dann ihre strategischen Planungen hin ausrichten. Sie werden das aber nur tun, wenn es eine klare „Ansage von oben" gibt – im besten Fall aus dem Bundeskanzleramt und den Staatskanzleien.

> **Es ist ein gutes Zeichen, dass im neuen Bundesministerium für Digitalisierung und Staatsmodernisierung (BMDS) eine ganze Abteilung zum „Deutschland-Stack" geplant ist.**

Es ist ein gutes Zeichen, dass im neuen Bundesministerium für Digitalisierung und Staatsmodernisierung (BMDS) eine ganze Abteilung zum „Deutschland-Stack" geplant ist. Es wäre ein international achtbarer Erfolg für den neuen Bundesminister Dr. Karsten Wildberger, wenn er es schafft, Deutschland von der digitalen Abhängigkeit in die digitale Souveränität zu führen. Wenn er das Mammutprojekt, sich aus der strategischen Abhängigkeit von Microsoft-Produkten zu lösen, in seiner ersten Amtszeit erfolgreich aufgleist, und dabei auch dazu bereit ist, dem bislang nahezu unantastbaren Tech-Giganten Microsoft die Stirn zu bieten, soweit es im Interesse des deutschen Staates liegt, hätte er seinem Ruf als Krisenmanager für große IT-Projekte alle Ehre gemacht. Es wäre nicht nur ein politischer Erfolg, sondern im besten Fall auch ein Konjunkturprogramm für die heimische Digitalwirtschaft und ein werthaltiges Mehr an digitaler Wahl- und Entscheidungsfreiheit für alle.

CYBERINTELLIGENCE
.Institute

Impressum

Der Autor
Michael Kolain ist Volljurist und Experte für Digitalpolitik. Er arbeitet an der Schnittstelle zwischen Gesetzgebung, Wissenschaft und der Entwicklung digitaler Technologien.

---

cyberintelligence.institute (Herausgeberin)
MesseTurm
Friedrich-Ebert-Anlage 49
60308 Frankfurt a.M.

T +69 5050 34-602

www.cyberintelligence.institute
info@cyberintelligence.institute
