CII: Digitale Un-Souveränität der Verwaltung kostet Steuermilliarden

12. November 2025 – Die digitale Abhängigkeit der deutschen Verwaltung von Microsoft droht sich weiter massiv zu verschärfen. Das ist das Ergebnis eines aktuellen Whitepapers des cyberintelligence.institute, das am Mittwoch in Berlin vorgestellt wurde. Ursächlich sind laut Studie gezielte Lock-In-Effekte und Produktbündelungen, die die Wahlfreiheit der öffentlichen Hand faktisch aushebeln - mit erheblichen Beeinträchtigungen der Kostenkontrolle, Cybersicherheit und digitalen Souveränität.

Eine Woche vor dem Gipfel zur Europäischen Digitalen Souveränität warnt das CII in einem Whitepaper vor einer weiter wachsenden preislichen und technologischen Abhängigkeit von Bund, Ländern und Kommunen. Die bereits stark ausgeprägte Marktdominanz von Microsoft drohe künftig in eine unumkehrbare Abhängigkeit umzuschlagen, wenn keine aktive Gegensteuerung erfolge. „Digitale Souveränität braucht Wahlfreiheit. Dass die Verwaltung das Quasi-Monopol eines Anbieters unter wachsender Preisgabe der technischen, rechtlichen und ökonomischen Kontrolle in Kauf nimmt, erscheint unverständlich“, so CII-Fellow und Studienautor Michael Kolain.

Quasi-Monopol und Produktbündelung verhindern Aufbau europäisch digitalsouveräner Alternativen

Die digitale Abhängigkeit der öffentlichen Verwaltung gründet laut der Studie in einer gezielten Bündelung von Diensten und Produkten, die es dritten Anbietern außerhalb des Ökosystems von Microsoft erheblich erschwere, mit alternativen Lösungen Fuß zu fassen. Diese Ausgangslage werde durch die Entwicklung proprietärer Standards und die Vermeidung offener Schnittstellen befördert sowie durch ein eng verflochtenes, über Jahrzehnte gewachsenes Vertriebs- und Partnernetz weiter verschärft.

Darüber hinaus verstärkten Netzwerkeffekte den Sog in ein geschlossenes Ökosystem, dem sich insbesondere kleinere Kommunen und Gemeinden nur schwer entziehen können. „Angesichts der zunehmenden Verlagerung von IT-Infrastrukturen in die Cloud droht eine langfristige Verfestigung dieser Abhängigkeiten“, so Kolain. Diese Marktdominanz behindere einen offenen und fairen Wettbewerb im europäischen Cloud-Markt und erschwere den Aufbau digitalsouveräner Lösungen.

Lock-in-Strategien und Intransparenz beeinträchtigen Kostenkontrolle und Cyberresilienz in der Verwaltung

Als weitere Konsequenz dieser über Jahrzehnte gewachsenen Strukturen benennt CII-Senior Fellow Michael Kolain die erheblichen Auswirkungen auf die Kostenkontrolle der öffentlichen Verwaltung. Er zeigt auf, dass die Lizenzkosten auf Bundesebene seit 2017 um mehr als 250 Prozent zugenommen haben. Die jährlichen Lizenzkosten von über 200 Mio. Euro allein auf Bundesebene würden auf Länder- und Kommunalebene nach konservativen Schätzungen um ein Vielfaches übertroffen, die Aufwände an Steuergeldern deutlich über eine Milliarde Euro bedeuteten. Diese Gelder stünden dadurch nicht mehr für

Ausgaben zur Verfügung, die für alternative und digital souveränere Anbieter getätigt werden könnten.

Zudem gefährdeten die monolithischen Strukturen die Anfälligkeiten für Cyberangriffe und IT-Störungen nachhaltig, wie Ausfälle am Beispiel des Crowdstrike-Vorfalls verdeutlichen, von dem im Jahr 2024 weltweit mehrere Millionen Rechner zeitgleich betroffen gewesen sind. Dem gegenüber seien IT-Infrastrukturen, die auf offenen Schnittstellen und der Interoperabilität von Diensten gründeten, wesentlich resilienter gegenüber Ausfällen sowie von außen kommenden Cyberangriffen.

CII-Punkteplan zur schrittweisen Befreiung aus der digitalen Abhängigkeit

Als Reaktion auf diese Ausgangslage empfiehlt das CII konkrete Maßnahmen zur schrittweisen Abkehr von der „digitalen Unsouveränität", die auf kurzfristige, mittelfristige und langfriste Ziele gründen:

Kurzfristige Maßnahmen

1. **Kostenmonitoring** für IT-Beschaffung auf Grundlage des Microsoft-Rahmenvertrags mit dem Bundesinnenministerium
2. **Potenzialstudie** für verbesserte Wahlfreiheit mit Fokus auf Betriebssystem, Bürosoftware, Kommunikation und Cloud-Redundanz
3. **Wettbewerbsprüfung** des Microsoft-Ökosystems und Lizenzvergabe in Bezug auf die öffentliche Verwaltung
4. **Strategischer Austausch** mit internationalen Partnern und Entwicklung von Best Practices zu digital resilienten Beschaffungsprozessen

Mittelfristige Maßnahmen

1. **Wahlfreiheit „light"** in Bezug auf die Nutzung neuer und alter Microsoft-Produkte, insbesondere kein Zwang zur Migration in Microsoft Cloud Services
2. **Kostentransparenz** über Lizenzkosten auf allen Ebenen vertraglich verankern, um die Höhe der öffentlichen Steuergelder für Lizenzen zu erfassen
3. **Interoperabilität** und offene Schnittstellen werden als Vertragspflicht in künftigen Rahmenverträgen der öffentlichen Hand verankert

Langfristige Maßnahmen

1. **Einrichtung** eines interoperationalen Systems mit verschiedenen Anbietern und Produkten im Sinne eines voll funktionsfähigen Deutschland Stacks
2. **Fachbegleitung** der definierten Anforderungen an IT-Infrastrukturen unter Einbindung sachkundiger Fachbehörden wie BfDI, BSI und Bundeskartellamt
3. **Internationalisierung** der deutschen und europäischen wettbewerbsoffenen Arbeitsumgebung der öffentlichen Verwaltung

---

Das CII-Whitepaper zum Download:
https://cms.cyberintelligence.institute/api/media/file/2025112_cii-wp-cloudzip

Die PM ist auf unserer Website hier abrufbar:
https://cyberintelligence.institute/media-center

CII-Pressekontakt:
Alena Jakobs I Assistant Managerin to the Strategy Director
E-Mail: press@cyberintelligence.institute
Phone (Office): + 49 69 505034 602

Über das cyberintelligence.institute (CII):
An der Schnittstelle von Wirtschaft und Wissenschaft, NGO und Startups entwickelt das CII in Frankfurt am Main neue Lösungen für eine sichere digitale Zukunft. Gefragt sind dabei ganzheitliche Konzepte, die Cybersicherheit nicht nur als abstrakte technisch-organisatorische Gewährleistungsverantwortung, sondern als gesamtgesellschaftliche Aufgabe zum Schutz gemeinsamer europäischer Werte verstehen. Damit tritt das cyberintelligence.institute aktiv für mehr digitale Sicherheit in einem Zeitalter neuer digitaler Herausforderungen ein: www.cyberintelligence.institute