Wie Sie Ihre digitale Unabhängigkeit sichern – bevor es andere für Sie entscheiden

Inhalt

Zusammenfassung für den eiligen Leser

Was ist digitale Souveränität?
Digitale Souveränität bedeutet: Ein Unternehmen hat die volle Kontrolle über seine Daten, Systeme und digitalen Prozesse – unabhängig von einzelnen Anbietern oder politischen Einflüssen. Es geht nicht darum, sofort Open-Source zu nutzen oder alle Dienste selbst zu betreiben, sondern darum, im Ernstfall handlungsfähig zu bleiben – auch wenn ein Cloud-Anbieter ausfällt oder politische Entscheidungen (z. B. aus den USA) den Zugriff auf digitale Ressourcen einschränken.

Warum ist das gerade jetzt wichtig?

1. Politische Risiken: US-Gesetze wie der CLOUD Act erlauben Behörden Zugriff auf Daten, selbst wenn sie in Europa gespeichert sind. Ein geopolitischer Konflikt kann damit zum digitalen Betriebsrisiko werden.
2. Marktmacht & Abhängigkeiten: Anbieter wie Microsoft erhöhen Preise, ändern Bedingungen – ohne echte Alternativen für viele Mittelständler.
3. Technische Ausfälle: 40 % der deutschen Unternehmen hatten zuletzt Cloud-Ausfälle. Gleichzeitig stufen viele Manager Deutschlands digitale Unabhängigkeit als unzureichend ein.

Was kann man konkret tun – ohne Microsoft den Rücken zu kehren?

- Lokale Datensicherung: Automatisierte Backups auf betriebseigenen Servern.
- Hybride Strategien: Kombination aus Microsoft-Cloud und europäischen Alternativen.
- Datenklassifizierung: Sensible Daten gezielt schützen, weniger Kritisches flexibel speichern.
- Notfallpläne: Wer tut was, wenn Systeme ausfallen? – Schwarz auf Weiß definiert.
- Kommunikation absichern: Alternative Kanäle für Krisenfälle vorbereiten.

- Mitarbeiter schulen: Nur wer vorbereitet ist, kann souverän reagieren.

Fazit:
Digitale Souveränität ist kein IT-Projekt – sie ist eine strategische Notwendigkeit. Wer heute vorsorgt, schützt sich vor Abhängigkeit, Kostenfallen und Kontrollverlust. Schrittweise, aber entschlossen – das ist der Weg zu mehr Unabhängigkeit und Sicherheit für Ihr Unternehmen.

Was versteht man unter digitaler Souveränität?

Unter digitaler Souveränität versteht man die selbstbestimmte Kontrolle über die eigenen digitalen Daten, Infrastrukturen und Technologien. Ein Unternehmen mit hoher digitaler Souveränität kann frei entscheiden, wie und wo Daten gespeichert und verarbeitet werden, welche Software zum Einsatz kommt und wer darauf Zugriff hat – und zwar **ohne in unerwünschte oder riskante Abhängigkeiten zu geraten**. Für Geschäftsführer bedeutet das ganz praktisch: die Gewissheit, dass man *Herr über die eigenen Daten und Systeme* bleibt.

Besonders im Mittelstand, der oft auf Standardlösungen großer Anbieter (wie Microsoft Windows und Office) setzt, ist dieses Konzept entscheidend. Digitale Souveränität heißt nicht zwangsläufig, alles selbst zu entwickeln oder sofort Open-Source-Software einzusetzen – es heißt vor allem, **die Kontrolle zu behalten**: Darüber, dass vertrauliche Geschäftsunterlagen sicher und gemäß eigenen Compliance-Vorgaben gespeichert sind. Darüber, dass im Fall von Änderungen der Anbieter-Politik (etwa plötzliche Preiserhöhungen oder neue Nutzungsauflagen) Ausweichmöglichkeiten bestehen. Und darüber, dass das Unternehmen seine Prozesse und Datenflüsse im Griff hat, selbst wenn ein Dienstleister ausfällt.

Anders formuliert: Digitale Souveränität ist die *digitale Unabhängigkeitserklärung* des Unternehmens. Sie bildet die Grundlage, um Innovationen nach eigenen Regeln voranzutreiben, **rechtliche Vorgaben einzuhalten** (z.B. Datenschutz), sensible Informationen zu schützen und den Geschäftsbetrieb auch bei externen Störungen aufrechtzuerhalten. Kurz: Je höher der Grad an eigener digitaler Souveränität, desto robuster und zukunftsfähiger ist das Unternehmen in der heutigen vernetzten Wirtschaft.

Warum gewinnt digitale Souveränität gerade jetzt an Dringlichkeit?

Die Frage nach digitaler Souveränität ist nicht neu, doch aktuelle Entwicklungen verleihen ihr eine nie dagewesene **Dringlichkeit**. Ein zentraler Treiber ist die *geopolitische Abhängigkeit* Europas – insbesondere Deutschlands – von einigen wenigen ausländischen Tech-Giganten. **Fast alle** Unternehmen hierzulande stützen sich in irgendeiner Form auf US-Plattformen oder -Clouds. Dies hat lange gut funktioniert, birgt aber erhebliche Risiken:

1. Geopolitische Risiken und US-Politik: Politische Entscheidungen oder Krisen in den USA können unmittelbare Auswirkungen auf deutsche Firmen haben. Ein vielzitiertes Beispiel ist der CLOUD Act, ein US-Gesetz, das amerikanischen Behörden den Zugriff auf Daten erlaubt, die bei US-Anbietern gespeichert sind – selbst wenn diese Daten physisch in Europa liegenap-verlag.de. **Die Folge:** Wer z.B. sämtliche Firmendaten in der Microsoft-Cloud hat, läuft Gefahr, im Ernstfall die Kontrolle darüber zu verlieren. Dass dies keine theoretische Debatte ist, zeigte ein extremer Vorfall: Ein US-Präsident ließ dem Chefankläger des Internationalen Strafgerichtshofs

kurzerhand den Zugang zu dessen Microsoft-E-Mail-Konto sperren[1]. Diese Aktion machte deutlich, dass politische Konflikte rasch zu digitalem Kontrollverlust führen können. Marietje Schaake, ehemalige EU-Abgeordnete und Expertin am Stanford Cyber Policy Center, bringt die wachsende Sorge auf den Punkt: *Europa will das Risiko minimieren und sich von der übermäßigen Abhängigkeit von US-Technologie lösen*ap-verlag.de. Selbst **führende Cloud-Anbieter** aus Europa spüren diesen Trend: *„Es geht nicht mehr nur um Datenschutz, sondern um die Angst vor einer **Abschaltung durch die amerikanische Seite**“*, erklärt etwa Falk Weinreich von OVHcloud Deutschland[2].

2. Wirtschaftliche und rechtliche Unsicherheit: Die Marktmacht von Microsoft & Co. führt zu Abhängigkeiten, die auch wirtschaftlich gefährlich sind. Die *Gesellschaft für Informatik (GI)* warnt, dass eine Monopolstellung von Anbietern zu Preiserhöhungen und geringerer Verhandlungsfähigkeit der Kunden führt. Tatsächlich hat Microsoft seine Preise für Cloud- und Softwaredienste in letzter Zeit mehrfach angehoben – oft nahezu alternativlos für bestehende Kunden. Zudem besteht rechtliche Unsicherheit: US-Unternehmen unterliegen US-Gesetzen, was im Konfliktfall auch europäische Kundendaten betreffen kann. **Prof. Harald Wehnes** von der GI zählt im Zusammenhang mit der Microsoft-Abhängigkeit zahlreiche Risiken auf, u.a. *eingeschränkte Sicherheit, rechtliche Unsicherheit und sogar eine mögliche **wirtschaftliche oder politische Erpressbarkeit** ganzer Volkswirtschaften*[3]. Man denke an Szenarien wie Exportbeschränkungen oder Sanktionen, die plötzlich bestimmte Software-Lieferungen untersagen – was bedeutet das für ein Unternehmen, das komplett darauf angewiesen ist?

3. Aktuelle Ausfälle und „Wake-Up-Calls“: Jenseits der großen Politik häufen sich praktische Warnsignale. Cloud-Ausfälle etwa sind keineswegs selten: Laut Bitkom haben 40 % der deutschen Unternehmen in den letzten 12 Monaten mindestens einen Cloud-Dienst-Ausfall erlebt[4]. Auch der **Digitalverband Bitkom** selbst schlägt Alarm: Die digitale Souveränität Deutschlands wird von Führungskräften im Schnitt als *mangelhaft* bewertet. Anfang 2023 warnte der Bitkom-Präsident gar vor einem *„digitalen Kolonialstatus“* Europas, denn einer Studie zufolge sind **94 % der Unternehmen in Deutschland auf digitale Technologien und Komponenten aus dem Ausland angewiesen**[5]. Diese Zahlen zeigen: Die Abhängigkeit ist allgegenwärtig – und die möglichen Folgekosten bei Störungen enorm.

In Summe entsteht ein klares Bild: **Jetzt ist die Zeit zu handeln.** Digitale Souveränität ist kein Luxusproblem der IT-Abteilung, sondern Chefsache. Sie entscheidet mit darüber, ob ein mittelständisches Unternehmen in Krisenzeiten handlungsfähig bleibt. Im nächsten Abschnitt zeigen wir, welche konkreten Schritte Sie **sofort** einleiten können, um Ihre Abhängigkeiten zu verringern und Ihre digitale Resilienz zu stärken – auch wenn ein vollständiger Technologiewechsel aktuell (noch) nicht in Frage kommt.

---

[1] ap-verlag.de
[2] ap-verlag.de
[3] *security-insider.de*
[4] gruender-mv.de
[5] **security-insider.de**

Konkrete Handlungsempfehlungen für mehr digitale Unabhängigkeit

Auch ohne einen sofortigen Wechsel des Betriebssystems oder der Office-Software können mittelständische Firmen **viel tun**, um ihre digitale Souveränität zu erhöhen. Wichtig ist ein *schrittweises, planvolles Vorgehen* – kein Aktionismus, sondern durchdachte Maßnahmen, die im Ernstfall den Fortbestand des Betriebs sichern. Nachfolgend finden Sie **praktische, niedrigschwellige Empfehlungen**, die sich bewährt haben. Viele dieser Schritte lassen sich mit vertretbarem Aufwand umsetzen und entfalten doch eine große Wirkung für Ihre Unabhängigkeit und Krisenfestigkeit.

1. **Lokale Datenhaltung und Backups einführen:** Stellen Sie sicher, dass Ihre wichtigsten Firmendaten **lokal verfügbar** sind – etwa durch regelmäßige Backups auf betriebseigenen Servern oder Speichermedien. So behalten Sie auch dann Zugriff, wenn Cloud-Dienste ausfallen oder externe Anbieter den Zugang sperren sollten. Ein gutes Backup-Konzept umfasst automatisierte **Sicherungen kritischer Daten und Anwendungen**, sowohl in der Cloud als auch lokal im Unternehmen. Testen Sie die Wiederherstellung im Notfall regelmäßig, damit Sie im Ernstfall Daten und Systeme schnell wieder zum Laufen bringen können.

2. **Hybride Cloud-Modelle und Multi-Cloud nutzen:** Reduzieren Sie die Abhängigkeit von einem einzelnen Anbieter, indem Sie auf eine **Hybrid-Cloud-Strategie** setzen. Das bedeutet: Kombinieren Sie die Nutzung von öffentlichen Cloud-Diensten (z. B. Microsoft Azure) mit privaten Clouds oder lokalen Servern, und erwägen Sie zusätzlich **europäische Alternativen** als zweite Bezugsquelle. Viele Unternehmen wählen diesen pragmatischen Weg – eine Mischung aus US- und EU-Services –, um Risiken zu streuen und die eigene Resilienz zu erhöhen. So profitieren Sie weiterhin von den Stärken der großen Anbieter, sind aber vorbereitet, im Notfall schnell auf einen anderen Dienst auszuweichen. *Tipp:* Halten Sie **redundante Systeme** vor: Zum Beispiel einen zweiten Cloud-Speicher bei einem anderen Provider oder eine on-premise Lösung, auf die Sie umschalten können. Auch geografisch verteilte Datenspeicherung (etwa ein Rechenzentrum in Deutschland und eine Kopie in einem anderen EU-Land) erhöht die Ausfallsicherheit.

3. **Daten klassifizieren und Schutzbedarf festlegen:** Verschaffen Sie sich einen Überblick, *welche Daten besonders kritisch oder sensibel* sind. Teilen Sie Ihre Daten in Klassen ein (z.B. *öffentlich, intern, vertraulich, streng vertraulich*). Diese **Datenklassifizierung** hilft Ihnen, passende Schutzmaßnahmen zu ergreifen und Ressourcen effizient einzusetzen. Hochsensible Unternehmensgeheimnisse oder personenbezogene Daten sollten z.B. bevorzugt **verschlüsselt und auf lokalen bzw. europäischen Systemen** gehalten werden, während weniger kritische Daten bedenkenloser in der Cloud liegen können. Durch klare Klassifizierung können im Notfall zuerst die wichtigsten Daten geschützt und wiederhergestellt werden – ein entscheidender Vorteil, um den Betrieb aufrechtzuerhalten. Definieren Sie für jede Kategorie, wer darauf zugreifen darf, wo sie gespeichert werden soll und welche Backup-Strategie gilt.

4. **Notfallpläne (Business-Continuity-Plan) erstellen:** Entwickeln Sie einen detaillierten **IT-Notfallplan** für den Fall, dass wichtige digitale Dienste ausfallen oder unzugänglich

werden. Dieser Plan sollte **schriftlich festhalten**, welche Schritte bei einem Ausfall zu unternehmen sind, und er sollte allen Schlüsselpersonen bekannt sein. Wichtige Bestandteile sind zum Beispiel:

- **Rollen und Verantwortlichkeiten:** Benennen Sie ein Notfall-Team und klare Ansprechpartner, die im Krisenfall Entscheidungen treffen und Maßnahmen koordinieren.
- **Eskalationswege und Kommunikation:** Legen Sie fest, *wie* im Ernstfall alarmiert wird (z.B. telefonische Alarmkette, SMS-Benachrichtigungen) und wie die interne Kommunikation abläuft. Halten Sie Kontaktdaten aller relevanten Personen – Geschäftsführung, IT-Dienstleister, Cloud-Anbieter – in einem Notfallhandbuch bereit.
- **Kernprozesse identifizieren:** Führen Sie eine Liste der wichtigsten Anwendungen und Daten, die für den Geschäftsbetrieb nötig sind. Planen Sie für jede dieser Komponenten Alternativen oder Workarounds. (Beispiel: Wenn die Cloud-ERP ausfällt, gibt es eine lokale Lesekopie der letzten Datenbank? Wenn E-Mail nicht geht, gibt es einen Fax oder Telefonprozess für Bestellungen?)
- **Backup- und Wiederanlaufstrategie:** Definieren Sie, wie Backups eingespielt werden und wer das technisch übernimmt. Stellen Sie sicher, dass die benötigte Hardware oder Cloud-Alternative unmittelbar zur Verfügung steht.

Ein durchdachter Notfallplan minimiert Ausfallzeiten und *stellt sicher, dass Ihr Unternehmen handlungsfähig bleibt*. Üben Sie den Ernstfall in regelmäßigen Abständen (z.B. jährliche Simulation eines Cloud-Ausfalls), um die Wirksamkeit des Plans zu überprüfen und Mitarbeiter mit den Abläufen vertraut zu machen. Viele Branchenstandards (etwa die neue EU-NIS2-Richtlinie) fordern solche Pläne inzwischen explizit ein, inklusive dokumentierter Kommunikationswege und Alarmierungsverfahren – es lohnt sich also doppelt, hier proaktiv zu sein.

5. **Alternative Kommunikationswege sicherstellen:** Überlegen Sie sich, wie Ihre Mitarbeiter kommunizieren können, *wenn zentrale Tools ausfallen*. Gerade in Microsoft-zentrierten Umgebungen hängt viel an Diensten wie Outlook (E-Mail) oder Teams (Chat/Meetings). **Planen Sie Alternativen für den Notfall:** Zum Beispiel eine Telefonkonferenz-Brücke über eine Festnetznummer, einen sekundären E-Mail-Dienst (etwa einen einfachen Webmail-Server auf Ihrem Firmenserver oder bei einem zweiten Anbieter) oder Messenger-Dienste, die nicht vom selben Ökosystem abhängig sind. Im Krisenfall muss klar sein, *wie die Belegschaft und Partner erreichbar sind*. Eine Möglichkeit ist, im Voraus einen **„Kommunikations-Notfallkasten“** bereitzustellen: Dieser enthält z.B. eine Liste aller Mobilnummern der Mitarbeiter, Anleitungen für den Zugang zu einem alternativen Mail-System sowie ggf. vorformulierte Informationsmeldungen an Kunden und Partner. So eine Vorbereitung stellt sicher, dass Sie auch bei einem Totalausfall der primären Kommunikation (z.B. durch einen großflächigen Cloud-Blackout) nicht im Blindflug agieren. Wichtig ist ebenfalls, die **Kommunikationswege abzusichern** – auch im Notfall sollten vertrauliche Informationen nur über *sichere Kanäle* ausgetauscht werden (Stichwort Ende-zu-Ende-Verschlüsselung, VPN für Heimarbeit etc. gemäß Ihren Vorgaben).
6. **Schlüsselpersonal schulen und sensibilisieren:** *Menschen* sind ein Schlüsselfaktor für digitale Souveränität. Stellen Sie sicher, dass Sie im Unternehmen genügend Know-

how haben, um im Zweifel eigenständig handeln zu können. Dazu gehört zum einen die **Schulung von IT-Schlüsselpersonal**: Ihre IT-Administratoren (ob intern oder externe Dienstleister) sollten Notfallverfahren, Backup-Restore-Prozesse und alternative Systeme im Schlaf beherrschen. Überlegen Sie, ob Sie ausgewählte Mitarbeiter in wichtigen Technologien zertifizieren oder durch Trainings auf den neuesten Stand bringen. Zum anderen geht es um die allgemeine Sensibilisierung aller Mitarbeiter für IT-Risiken und Abläufe. Jeder im Team sollte grundlegende Sicherheitsregeln kennen (Phishing-Erkennung, sicheres Passwortmanagement, Umgang mit sensiblen Daten) und wissen, was im Ernstfall zu tun ist. Die *digitale Resilienz* eines Unternehmens ist nur so stark wie die Kenntnisse seiner Mitarbeiter. Regular Schulungen und klare Richtlinien zahlen sich aus: Sie minimieren die Wahrscheinlichkeit von Fehlern und stellen sicher, dass im Krisenfall alle an einem Strang ziehen. Experten betonen, dass digitale Souveränität ohne kompetente Mitarbeiter nicht zu haben ist – investieren Sie daher in Ihre *Mannschaft*. Im Umkehrschluss schafft ein souveräner Umgang mit Technik auch neue Chancen: Ihr Team lernt, Technologien bewusster einzusetzen, und entwickelt *Innovationskompetenz*, statt nur passiv den Vorgaben eines Monopol-Anbieters zu folgen.

Fazit

Digitale Souveränität ist ein fortlaufender Prozess, kein einmaliges Projekt. Der Ausstieg aus etablierten Abhängigkeiten gelingt nicht über Nacht – aber *jeder Schritt in Richtung Unabhängigkeit zahlt sich aus*. Durch lokale Datenhaltung, hybride Strategien, Notfallvorsorge und geschulte Mitarbeiter verschaffen Sie Ihrem Unternehmen mehr **Handlungsfreiheit**. Sie reduzieren das Risiko, von externen Schocks überrascht und lahmgelegt zu werden. Gleichzeitig stärken Sie das Vertrauen Ihrer Kunden und Partner, da ein souverän aufgestelltes Unternehmen Auskunft über Datenwege geben kann und sich als zuverlässiger, sicherer Dienstleister präsentiertnta.de. Nutzen Sie die hier vorgestellten Empfehlungen, um in kleinen, machbaren Schritten die Weichen für mehr digitale Unabhängigkeit zu stellen – **jetzt ist der ideale Zeitpunkt** dafür. Die Politik und Verbände rufen den Mittelstand längst zum Handeln auf, doch letztlich liegt es an jedem Unternehmen selbst, die Schlüssel in die Hand zu nehmen. Wer *proaktiv* vorsorgt, stellt sicher, dass er im Zweifel auf eigenen Beinen stehen kann. Oder wie es ein Experte formulierte: *Wer nicht riskieren möchte, plötzlich und unverschuldet seiner Geschäftsgrundlage beraubt zu werden, sollte jetzt für Resilienz sorgen*– insbesondere im deutschen Mittelstand. In diesem Sinne: Machen Sie Ihr Unternehmen **digital souverän** und damit fit für eine unsichere Zukunft.