Behördensoftware 1995 Kommentar: Rückblick mit Perspektive

Category: Opinion
geschrieben von Tobias Hager | 14. August 2025

Behördensoftware 1995 Kommentar: Rückblick mit Perspektive

Stell dir vor, du sitzt 1995 im Amtszimmer, Windows 3.11 läuft, Lotus Notes rödelt im Hintergrund, und irgendein IT-Sachbearbeiter erklärt dir, dass das jetzt „State of the Art“ sei. Heute lachen wir darüber – damals war das die Realität deutscher Behörden-IT. Doch wer glaubt, die digitale Steinzeit wäre vorbei, hat das Regierungsnetz noch nie von innen gesehen. Zeit für den schonungslosen Rückblick: Was lief 1995 schief, warum spüren wir das 2024 noch – und was muss jetzt endlich anders werden?

- Behördensoftware 1995: Status Quo, zentrale Systeme und Paradigmen der

damaligen IT
- Die größten technischen und organisatorischen Fehler – und warum sie sich bis heute rächen
- Legacy-Systeme, Schnittstellenhölle und Update-Furcht: Wie Altlasten Innovation ausbremsen
- Sicherheitslücken als Designfeature: Warum Behörden-IT ein Einfallstor blieb
- Modernisierung 2024? Zwischen föderalem Chaos, E-Government und Digitalpakt-Illusionen
- Warum Open Source, Cloud und API-First keine Buzzwords, sondern Überlebensstrategien sind
- Eine Schritt-für-Schritt-Anleitung: So kommt die Verwaltung aus dem 90er-Loch
- Fazit: Wer jetzt nicht radikal umbaut, bleibt digital ewiger Zweiter

Wer 2024 glaubt, der Rückstand deutscher Behörden bei der Digitalisierung sei eine Art Naturgesetz, hat das Elend von Behördensoftware 1995 nie erlebt. Was damals als „zukunftssicher“ verkauft wurde, ist heute ein Paradebeispiel für technische Selbstsabotage: monolithische Anwendungen, proprietäre Datenbanken, Insel-Lösungen ohne Schnittstellen, Authentifizierung via Passwort auf Post-it. Und nein, das ist kein Klischee – das war der Standard. Wer wissen will, warum deutsche Ämter immer noch mit Fax und USB-Stick hantieren, muss genau hier ansetzen: Der Rückblick ist keine Folklore, sondern ein Lehrstück in digitaler Selbstverhinderung.

Behördensoftware 1995 war der feuchte Traum von IT-Abteilungsleitern mit IBM-Bindung, SAP-Sucht und einem chronischen Hang zur Risikovermeidung. Modularität? Pustekuchen. Anbindung an externe Systeme? Wer braucht schon Austausch mit Bürgern oder anderen Ämtern. Hauptsache, die eigene Abteilung kann auf ihr „Fachverfahren“ zugreifen – und wehe, jemand fragt nach Datenmigration oder Systemintegration. Willkommen im Behörden-Labyrinth, aus dem selbst Theseus digital nicht mehr rausfände.

Eines vorweg: Die Folgen dieser Epoche spüren wir bis heute. Wer glaubt, die Zettelwirtschaft sei übertrieben, sollte mal einen Blick in die IT-Landschaft der öffentlichen Verwaltung werfen. Dort ticken noch Server, deren letzte Sicherheitsupdates aus dem Jahr der Wiedervereinigung stammen. Digitalisierung? Gibt’s nur als Powerpoint-Folie. Und jetzt kommen Cloud, KI und E-Government – und treffen auf ein Fundament aus 90er-Jahre-Software. Was soll da bitte schiefgehen?

Behördensoftware 1995: Der technische und organisatorische Sündenfall

Wer sich die Architektur von Behördensoftware 1995 anschaut, versteht sofort, warum sich deutsche Verwaltung digital selbst blockiert. Zentrale Fachverfahren, fast immer proprietär, oft als monolithische Anwendungen auf

Lotus Notes, Oracle Forms oder – für die ganz Mutigen – Access-Datenbanken. Das Wort „Modularisierung“ war ungefähr so populär wie WLAN im Plenarsaal. Die Folge: Jede Behörde entwickelte oder kaufte ihre eigene Softwarelösung, ohne Rücksicht auf Interoperabilität, Schnittstellen oder künftige Wartbarkeit.

Was damals als „Sicherheit“ verkauft wurde, war in Wirklichkeit ein technischer Lock-In. Einmal IBM, immer IBM. Wer einmal SAP eingeführt hatte, musste sich für die nächsten 20 Jahre mit kryptischen ABAP-Skripten, abenteuerlichen Releasezyklen und Supportverträgen zu Mondpreisen abfinden. Austausch zwischen Systemen? Nur mit individuellen Schnittstellen, gebaut von externen Beratern, die nach dem Projektabschluss verschwunden sind. Von API-Standards, Microservices oder gar Cloud-Nutzung keine Spur – das wäre ja „unsicher“ gewesen.

Organisatorisch wurde die technische Rückständigkeit noch verstärkt: Entscheidungswege, die so lang waren wie die Lebensdauer der eingesetzten Server, Gremien, deren Hauptaufgabe es war, Risiken zu vermeiden, und eine IT-Beschaffung, die Innovation systematisch blockierte. Wer Neues einführen wollte, musste erst mal 17 Freigaben einholen – von Leuten, die das Internet für einen Hype hielten. So entstand ein Ökosystem der Selbstverhinderung, das Innovation systematisch ausbremste.

Die Angst vor Veränderung führte dazu, dass Systeme viel zu lange im Einsatz blieben – oft weit über das Support-Ende hinaus. Sicherheitsupdates? Kamen irgendwann, sofern das Budget reichte. Ergebnis: Eine IT-Landschaft, die schon 1995 veraltet war und seither nur noch notdürftig geflickt wurde. Willkommen im digitalen Mittelalter – made in Germany.

Legacy-Systeme, Schnittstellenhölle und Update-Paralyse: Altlasten als Innovationskiller

Was passiert, wenn man 1995er Software 2024 noch produktiv betreibt? Richtig: Man landet in der Legacy-Hölle. Die meisten Fachverfahren der öffentlichen Verwaltung sind heute noch die direkte Fortsetzung von Systemen, die in den 90ern entwickelt wurden. Das Problem: Sie laufen auf Hardware, die längst aus dem Support gefallen ist, verwenden Datenbanken, die niemand mehr patcht, und sind so individuell angepasst, dass jeder Versuch einer Migration zum Millionengrab wird.

Die berüchtigte „Schnittstellenhölle“ ist das Produkt dieser Ära: Jedes System spricht eine eigene Sprache, Datenformate sind proprietär, und jedes Update kann zum kompletten Blackout führen. Integration? Nur über kostspielige Middleware-Lösungen, die wiederum eigene Spezialisten und

Wartungsverträge brauchen. Jeder Versuch, moderne Anwendungen, etwa E-Government-Portale oder Cloud-Dienste, anzubinden, endet in einem Spaghetti-Kabelwirrwarr aus Datenkonvertern, Batch-Jobs und halbautomatisierten Workarounds.

Das größte Problem: Die Angst vor Updates. Jede Änderung an einem dieser Systeme ist ein unkalkulierbares Risiko. Niemand weiß mehr genau, wie die Software funktioniert, weil die ursprünglichen Entwickler längst in Rente sind. Dokumentation? Wenn überhaupt, dann in Papierform im Aktenschrank. Das Resultat: Sicherheitslücken bleiben offen, weil niemand sich traut, das System anzufassen. Modernisierung ist ein Wort, das in Sitzungen zwar oft fällt, aber selten umgesetzt wird – aus blanker Angst vor dem digitalen GAU.

Die Folge: Jeder Digitalpakt, jedes Modernisierungsgesetz, jede noch so gut gemeinte E-Government-Initiative prallt an dieser Mauer der Legacy-IT ab. Wer glaubt, dass sich das Problem mit neuen Fördermitteln oder ein paar Cloud-Workshops lösen lässt, hat das Ausmaß der Altlasten nicht verstanden. Hier hilft nur der radikale Schnitt – alles andere ist digitales Pflasterkleben.

Sicherheitslücken als Systemfehler: Behörden-IT als Einfallstor

Ein besonders bitteres Erbe der 1995er Behördensoftware: Sicherheitslücken, die von Anfang an systemimmanent waren. Authentifizierung? Meistens simple Benutzername-Passwort-Kombinationen, oft ohne jegliche Verschlüsselung. Zugriffsrechte wurden auf Basis von Abteilungszugehörigkeit vergeben, ein echtes Rollen- und Rechtemanagement war die Ausnahme. Wer das System kannte, konnte sich oft mit minimalem Aufwand Zugriff verschaffen – der legendäre „Admin“-Account mit Standardpasswort war allgegenwärtig.

Update-Strategien existierten bestenfalls auf dem Papier. Patch-Management? Fehlanzeige. Sicherheitsupdates wurden nur dann eingespielt, wenn „etwas passiert“ war – also meistens nach einer Panne oder einem Vorfall. Firewalls und Netzwerksegmentierung waren exotisch, VPN-Zugänge mit 40-Bit-Verschlüsselung galten als Hochsicherheit. Hinzu kam eine gefährliche Mischung aus Unwissenheit und Gleichgültigkeit: IT-Sicherheit war ein Thema für Spezialisten – und die saßen selten in der Führungsriege.

Die Folge: Behördennetzwerke wurden zu einem beliebten Ziel für Angriffe. Ransomware, Datenlecks und komplette Systemausfälle sind kein modernes Phänomen – sie sind das Ergebnis jahrzehntelanger Nachlässigkeit. Wer heute über Datenschutz und IT-Sicherheit in der Verwaltung redet, muss sich fragen, warum grundlegende Prinzipien wie Zero-Trust, Zwei-Faktor-Authentifizierung oder Verschlüsselung erst 25 Jahre später zum Standard werden. Die Antwort: Weil man es sich zu lange bequem gemacht hat.

Der traurige Witz: Viele Schwachstellen sind bis heute nicht behoben. Solange

Legacy-Systeme laufen, bleiben sie potenzielle Einfallstore – und jeder Versuch, sie zu ersetzen, scheitert an denselben bürokratischen Hürden wie 1995. Sicherheit bleibt ein frommer Wunsch, solange die technische Basis aus der Zeit stammt, als das Internet noch mit Modem piepte.

Modernisierung 2024: Zwischen Digitalpakt-Placebo und föderalem Digital-Dschungel

Natürlich gibt es heute Initiativen zur Modernisierung der Behörden-IT: E-Government-Gesetze, Onlinezugangsgesetz (OZG), Digitalpakt, diverse Förderprogramme. Klingt nach Fortschritt – ist aber oft nur Fassade. Die Realität: Jedes Bundesland, jede Kommune, jede Behörde kocht ihr eigenes technisches Süppchen. Zentralisierung? Föderaler Horror. Einheitliche Standards? Wunschdenken. Wer versucht, einheitliche Plattformen zu etablieren, strandet regelmäßig am Klein-Klein der Zuständigkeiten und an der politischen Angst vor Kontrollverlust.

Das Ergebnis: Ein Flickenteppich aus Insellösungen, der Integration fast unmöglich macht. Während in Estland digitale Verwaltung radikal durchgezogen wurde, verheddert sich Deutschland in Paralleluniversen aus SAP, Eigenentwicklungen und externen Dienstleistern. Der Versuch, Legacy-Systeme mit neuen Frontends oder „Middleware“ zu modernisieren, führt zu absurden Konstrukten, in denen die eigentliche Datenhaltung weiterhin auf 90er-Jahre-Infrastruktur basiert.

Cloud, Open Source, API-First? Werden als Buzzwords in Strategiepapieren abgefeiert, aber in der Praxis selten umgesetzt. Die Angst vor Kontrollverlust ist größer als der Wille zur Innovation. Selbst einfache Dinge wie Single-Sign-On oder Self-Service-Portale scheitern an inkompatiblen Alt-Systemen und Datenschutz-Bedenken, die in Wahrheit oft nur die Angst vor Veränderung kaschieren.

Der Digitalpakt ist deshalb häufig ein Placebo: Viel Geld, wenig Wirkung. Solange die technischen und organisatorischen Grundprobleme nicht gelöst werden, bleibt jede Modernisierung Flickwerk. Wer ernsthaft Digitalisierung will, muss die 90er-Jahre-IT konsequent ausmustern – und nicht versuchen, sie mit neuen Oberflächen zu kaschieren.

Open Source, Cloud, API-First: Die radikale Perspektive für

eine echte Modernisierung

Wer aus dem 1995er-Dilemma rauswill, muss mehr tun als nur neue Software kaufen. Die Perspektive für eine moderne Verwaltung besteht aus drei zentralen Prinzipien: Open Source, Cloud und API-First. Warum? Proprietäre Lösungen haben gezeigt, dass sie teuer, unflexibel und innovationsfeindlich sind. Nur offene Standards ermöglichen echte Interoperabilität – und verhindern, dass sich die Fehler der Vergangenheit wiederholen.

Open Source bedeutet nicht billiger, sondern besser: Transparente Codebasis, keine Abhängigkeit von einzelnen Anbietern, Community-getriebene Weiterentwicklung, und vor allem: Sicherheit durch Sichtbarkeit. Wer seine Fachverfahren auf Open-Source-Basis entwickelt, kann sie flexibel anpassen, auf Sicherheitslücken sofort reagieren und spart langfristig Kosten für Lizenzgebühren und Supportverträge.

Cloud-Technologien ermöglichen Skalierbarkeit, Hochverfügbarkeit und Automatisierung – alles Dinge, die Legacy-IT nicht leisten kann. Natürlich muss Datenschutz bedacht werden, aber moderne Cloud-Angebote lassen sich auch in der behördlichen IT sicher betreiben. Wer immer noch glaubt, die eigene Serverfarm im Keller sei sicherer, hat die Bedrohungslage nicht verstanden.

API-First ist der Schlüssel zu echter Integration: Jedes System, das nicht über standardisierte, dokumentierte Schnittstellen verfügt, ist ein digitales Fossil. Nur mit klaren APIs lassen sich Daten effizient austauschen, neue Anwendungen anbinden und Prozesse automatisieren. Microservices-Architekturen, Containerisierung und Infrastructure as Code sind längst Standard in der Wirtschaft – höchste Zeit, dass sie auch die Verwaltung erreichen.

Die Umstellung ist kein Selbstläufer, aber zwingend notwendig. Wer 2024 noch auf proprietäre Monolithen setzt, zementiert den Rückstand und macht sich weiter abhängig von teuren Beratern und Herstellern. Der Weg führt nur über Transparenz, Offenheit und die Bereitschaft, auch unpopuläre Entscheidungen zu treffen. Alles andere ist digitaler Selbstbetrug.

Schritt-für-Schritt-Anleitung: Wie Behörden aus dem 90er-Loch kommen

Es ist möglich, den Sprung aus der Legacy-Falle zu schaffen – aber nur mit System, Mut und technischer Kompetenz. Hier die zehn Schritte, die wirklich rausführen:

1. Bestandsaufnahme
   Vollständige Inventarisierung aller eingesetzten Systeme, inkl. Abhängigkeiten, Schnittstellen und Supportstatus. Ohne ehrliche Analyse

bleibt jede Modernisierung Flickwerk.
2. Risikoanalyse
   Identifikation der kritischsten Legacy-Systeme, insbesondere im Hinblick auf Sicherheit, Wartbarkeit und Integrationsfähigkeit.
3. Abschaltstrategie entwickeln
   Für jedes Altsystem einen klaren Migrationspfad oder eine Abschalt-Roadmap definieren. Keine heiligen Kühe mehr.
4. Open Source als Standard festlegen
   Bei jeder Neuentwicklung offene Technologien und Standards priorisieren. Proprietär nur nach dokumentiertem Ausnahmefall.
5. API-First-Architektur einführen
   Schnittstellen nach offenen Standards (REST, GraphQL, OData) dokumentieren und zur Pflicht machen. Ohne API keine neue Software.
6. Cloud-Readiness schaffen
   Infrastruktur modernisieren, Containerisierung (z.B. Docker, Kubernetes) einführen, Pilotprojekte in der Cloud realisieren. Sicherheit und Compliance von Anfang an mitdenken.
7. IT-Sicherheitskonzept aufbauen
   Zero-Trust-Ansatz, Zwei-Faktor-Authentifizierung, durchgängige Verschlüsselung. IT-Sicherheit als laufenden Prozess etablieren, nicht als einmalige Maßnahme.
8. Kompetenzen intern stärken
   Weiterbildungsprogramme für IT-Mitarbeiter, Aufbau von Open-Source- und Cloud-Expertise, Kooperation mit Hochschulen und Tech-Community.
9. Agile Methoden einführen
   Projektmanagement nach Scrum oder Kanban, schnelle Iterationen, MVPs und kontinuierliche Verbesserung. Schluss mit Wasserfall und Endlos-Gremien.
10. Monitoring und Transparenz leben
    Alle Projekte offen dokumentieren, Fortschritte und Probleme sichtbar machen. Beteiligung der Nutzer und ständiges Feedback sichern nachhaltigen Erfolg.

Fazit: Wer jetzt nicht radikal umbaut, bleibt digital ewiger Zweiter

Der Rückblick auf Behördensoftware 1995 ist kein Nostalgietrip, sondern ein Mahnmal für technisches Versagen mit Langzeitfolgen. Die digitale Verwaltung Deutschlands leidet bis heute unter den Fehlern der Vergangenheit: Monolithen, Schnittstellenchaos, Sicherheitslücken und Modernisierungsangst. Wer glaubt, mit kleinen Schritten und Placebo-Projekten lasse sich das Problem lösen, irrt gewaltig. Nur der radikale Umbau – technologisch, organisatorisch und mental – führt raus aus dem 90er-Loch.

Die Perspektive ist klar: Offene Standards, Cloud-Technologien und API-First sind keine Zukunftsmusik, sondern Überlebensstrategien. Wer weiter auf proprietäre Insellösungen setzt, verspielt Anschlussfähigkeit, Sicherheit und

Innovationskraft. Die Verwaltung muss jetzt beweisen, dass sie mehr kann als Fax und Aktenordner. Wer es nicht tut, bleibt digital ewiger Zweiter – und das ist 2024 keine Option mehr.