



Zukunftsstark handeln – wie Deutschlands Verwaltung Digitalisierung jetzt souverän gestalten kann.

Deutschland befindet sich in puncto Digitalisierung mitten in einer wichtigen Phase. Noch nie waren die Erwartungen an eine moderne Verwaltung so hoch, noch nie waren die Risiken durch Cyber-Angriffe, geopolitische Spannungen und technologische Abhängigkeiten so spürbar. Die Handlungsfähigkeit des Staats hängt heute direkt von stabilen und sicheren IT-Strukturen ab.

Während Bürger:innen erwarten, dass Anträge online gestellt und Dokumente digital abgerufen werden können und Services jederzeit verfügbar sind, kämpfen viele Behörden im Alltag mit über Jahrzehnte hinweg gewachsenen Fachverfahren. Unterschiedliche Insellösungen, fehlende Standards und hohe Wartungskosten prägen die Realität. Hinzu kommen ein akuter Fachkräftemangel in der IT und die wachsende Bedrohungslage durch Cyber-Angriffe. Das Ergebnis ist ein Reformstau, der die Modernisierung der Verwaltung bremst, bei gleichzeitig steigenden Erwartungen von außen.

Digitale Souveränität als Leitprinzip.

In dieser Gemengelage rückt ein Begriff in den Mittelpunkt: digitale Souveränität. Gemeint ist die Fähigkeit, über Daten, Systeme und Technologien selbstbestimmt entscheiden und Abhängigkeiten kontrollieren zu können. Es geht nicht darum, alles selbst zu entwickeln oder internationale Anbieter auszuschließen. Vielmehr umfasst Souveränität eine Reihe von Kompetenzen: von Datenlokation und Schlüsselhoheit über Portabilität und Interoperabilität bis hin zu Transparenz und Kontrolle. Der IT-Dienstleister Bechtle sieht digitale Souveränität nicht als statischen Zustand, sondern als gestaltbaren Prozess. Sie bedeutet ausdrücklich keine technologische Isolation, sondern die Fähigkeit, belastbare Gesamtarchitekturen zu entwickeln. Souveränität zeigt sich dort, wo Organisationen über Wahlfreiheit verfügen, Robustheit nachweisen können und im Krisenfall Resilienz unter Beweis stellen.

Prinzipien einer souveränen Verwaltung.

Diese drei Prinzipien – Wahlfreiheit, Robustheit und Resilienz – bilden das Fundament für eine digitale Verwaltung, die ihre Aufgaben souverän erfüllt und gleichzeitig offen für Innovationen bleibt. Behörden brauchen die

Freiheit, Technologien und Anbieter nach Bedarf auszuwählen. Sie benötigen Systeme, die auch unter Belastung zuverlässig funktionieren. Und sie müssen in der Lage sein, im Ernstfall schnell wieder arbeitsfähig zu werden. Ein Landesrechenzentrum, das bei einem Stromausfall innerhalb weniger Stunden kritische Dienste über Ersatzkapazitäten aufrechterhalten kann, zeigt, was Robustheit bedeutet. Eine Kommune, die ihre Fachverfahren modular und standardisiert entwickelt, beweist Wahlfreiheit. Und eine Behörde, die regelmäßig Wiederanlaufübungen durchführt, lebt Resilienz – nicht nur auf dem Papier, sondern in der Praxis.

Vier zentrale Herausforderungen – und ein Signal aus der Politik.

Die öffentliche Verwaltung steht heute vor vier besonders drängenden Herausforderungen. Erstens: den gewachsenen Strukturen. Über Jahrzehnte wurden Fachverfahren individuell entwickelt – oft teuer, schwer integrierbar und kaum wiederverwendbar. Allein auf Bundes- und Landesebene laufen mehrere Tausend solcher Verfahren parallel. Zweitens: dem Tempo. Politische Erwartungen und gesellschaftliche Bedürfnisse entwickeln sich schneller, als klassische IT-Projekte umgesetzt werden können. Das Onlinezugangsgesetz hat eindrucksvoll gezeigt, wie groß die Lücke zwischen Anspruch und Geschwindigkeit ist. Drittens: der Sicherheit. Cyber-Angriffe auf Verwaltungen nehmen kontinuierlich zu. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) registrierte 2024 so viele sicherheitsrelevante Vorfälle wie nie zuvor. Und viertens: dem Fachkräftemangel. Nach Berechnungen fehlen in der öffentlichen Verwaltung mehrere Zehntausend IT-Expert:innen. Mit dem neuen Bundesministerium für Digitales und Staatsmodernisierung (BMDS) hat die Politik bereits ein starkes Signal gesetzt. 100 Tage nach der Gründung ist es gelungen, zentrale Strukturen zu

schaffen und erste Projekte anzustoßen. Dazu gehören die Bündelung digitaler Kompetenzen, der Startschuss für das „National Once-Only Technical System“ (NOOTS) sowie Impulse für Glasfaser- und Mobilfunkausbau. Das Ministerium versteht sich als Zukunfts- und Effizienzressort. Seine eigentliche Bewährungsprobe liegt nun darin, den Reformstau zu lösen und die vielen Einzelmaßnahmen zu einem kohärenten Ganzen zu verbinden.

Stimmen aus der Praxis.

Gerade weil die Aufgaben komplexer werden, steigt die Bedeutung verlässlicher Partner. Steven Handgrätinger, Bereichsvorstand Public Sector bei Bechtle, betont: „Digitale Souveränität ist für uns kein Schlagwort, sondern ein Arbeitsauftrag. Sie verlangt, dass wir Behörden in die Lage versetzen, ihre IT so zu gestalten, dass sie unabhängig entscheiden können. Sei es beim Wechsel von Plattformen, beim Betrieb kritischer Systeme oder bei der Integration neuer Technologien. Es geht nicht darum, ein Entweder-oder-Szenario zwischen nationalen und internationalen Lösungen aufzubauen, sondern um die Fähigkeit, Wahlfreiheit zu sichern.“ Auch Prof. Dr. Martin Kaloudis, Bereichsvorstand im Bechtle Cluster Mitte/West, weist auf die Dringlichkeit: „Wir haben es in Deutschland mit einem enormen Reformstau zu tun. Über Jahrzehnte gewachsene Fachverfahren sind nicht nur teuer in der Wartung, sie sind auch ein Innovationshemmnis. Low-Code, Cloud-Lösungen und KI bieten die Chance, diesen Knoten zu lösen – aber nur, wenn wir es schaffen, sie in eine souveräne Architektur einzubetten. Das bedeutet: Standards, klare Governance und das Denken in Gesamtarchitekturen.“

Der Baukasten für das digitale Deutschland.

Die Lösung liegt nicht in einem einzigen Großprojekt, sondern in einem Baukasten, bei dem die einzelnen

Komponenten nahtlos ineinandergreifen. Sichere Netze und Konnektivität schaffen die Grundlage für einen verlässlichen Betrieb. Mobile Arbeitsplätze ermöglichen flexible Zusammenarbeit – ob im Büro, unterwegs oder im Homeoffice. Low-Code- und No-Code-Plattformen beschleunigen die Entwicklung neuer Fachverfahren und reduzieren Abhängigkeiten von externen Anbietern. Cyber-Security-Lösungen schützen vor Angriffen und garantieren Handlungsfähigkeit. Multi-Cloud-Strategien verbinden Flexibilität mit Souveränität, indem Daten und Workloads portierbar bleiben. Resilienzlösungen stellen sicher, dass Systeme auch im Krisenfall schnell wieder verfügbar sind. Und künstliche Intelligenz eröffnet neue Möglichkeiten, wenn sie verantwortungsvoll eingebunden wird. Erst das Zusammenspiel dieser Bausteine schafft eine moderne, effiziente und souveräne Verwaltung.

Verwaltung 2030 – ein Zukunftsbild.

Wie könnte eine Verwaltung aussehen, die digitale Souveränität konsequent umgesetzt hat? 2030 beantragt eine Bürgerin online einen Baukostenzuschuss. Ihr Antrag wird über eine Low-Code-Anwendung gestellt, die automatisch mit Datenregistern verknüpft ist. Der Bearbeitungsstand ist jederzeit transparent einsehbar. Die Anwendungsumgebung läuft in einer souveränen Multi-Cloud, die Ressourcen dynamisch skaliert. Zugleich liegen alle Daten verschlüsselt in Deutschland und können bei Bedarf portiert werden.

Im Hintergrund sichern Cyber-Resilienz-Lösungen alle Systeme regelmäßig. Recovery-Übungen haben gezeigt, dass selbst im Fall eines großflächigen Angriffs die Kernsysteme in wenigen Stunden wieder verfügbar sind. Mitarbeitende arbeiten flexibel im Homeoffice oder mobil, ohne Sicherheitsrisiken – durch geprüfte Endgeräte und klare Governance. KI unterstützt bei der Vorprüfung von Anträgen, bleibt aber nachvollziehbar und überprüfbar. Ein

solches Szenario zeigt: Digitale Souveränität ist kein Schlagwort, sondern ein handlungsleitendes Prinzip, das Bürgernähe, Effizienz und Sicherheit verbindet.

Bechtle als Partner.

Bechtle bündelt in einem einzigartigen Portfolio Kompetenzen in allen relevanten Bereichen. Von sicheren Netzwerken über mobile Arbeitsplätze, Low-Code-/No-Code-, Cyber-Security-, Multi-Cloud- und Resilienzlösungen bis hin zu Künstliche Intelligenz. Dabei geht es nicht um den Verkauf einzelner Produkte, sondern um die Verzahnung.

Bechtle versteht sich als ganzheitlicher Möglichmacher, der Behörden in die Lage versetzt, souveräne Entscheidungen zu treffen und gleichzeitig auf bewährte Technologien zurückzugreifen. Erfahrungen aus zahlreichen Projekten zeigen: Standardisierung und Wiederverwendung sind ebenso entscheidend wie individuelle Anpassung. Dabei verfügt Bechtle über eine breite Rahmenvertragsbasis, die eine Beschaffung für Behörden ohne vorherige Ausschreibung einfach und schnell ermöglicht.

Blick in die Zukunft.

Die kommenden Monate und Jahre werden darüber entscheiden, ob es gelingt, den Reformstau in der Verwaltung zu überwinden. Mit der Registermodernisierung, der Umsetzung der OZG-Nachfolge, neuen Cloud-Strategien und dem zunehmenden Einsatz von künstlicher Intelligenz entstehen große Chancen, aber auch ebenso Risiken. Digitale Souveränität bietet hier den Kompass. Sie stellt sicher, dass neue Technologien nicht zu Abhängigkeiten führen, sondern handlungsfähig machen.

Die Bausteine sind vorhanden, die Prinzipien klar. Jetzt gilt es, sie konsequent einzusetzen – gemeinsam, standardisiert und mit einem klaren Blick auf Sicherheit, Resilienz und Bürgernähe.

Was tun, wenn das Netz ausfällt?

Die Rolle einer sicheren IT-Infrastruktur für Behörden und die öffentliche Verwaltung.....S. 2

Sicheres mobiles Arbeiten in der Bundesverwaltung.

Wie man trotz Geheimhaltungsgrad VS-NfD unterwegs entspannt arbeiten kann.....S. 3

Low-Code als Schlüsseltechnologie für moderne Behörden.

Warum man von Ende-zu-Ende-Digitalisierung ohne großen Programmieraufwand nur profitieren kann...S. 4

Cyber-Security in Zeiten globaler Unsicherheit.

Warum die wachsende Bedrohungslagen die Handlungsfähigkeit des Staates gefährden kann.....S. 5

Multi-Cloud als Staatsaufgabe.

Wie die Verwaltung digitale Souveränität gewinnt.....S. 6

Digitale Resilienz und Datenschutz.

Welche Anforderungen und Ansätze jetzt wichtig sind.....S. 7

Wie souveräne KI & KI-Governance die Demokratie stärken.

Chancen für Behörden und die öffentliche Verwaltung.....S. 8

IT-Automatisierung in der öffentlichen Verwaltung.

Wie man mit vorhanden Kapazitäten wesentlich mehr erreichen kann.....S. 9

Sprechen Sie uns an – gemeinsam gestalten wir das digitale Deutschland.

Mehr unter: [bechtle.com/bund](https://www.bechtle.com/bund)

Was tun, wenn das Netz ausfällt?

Fortschreitende Digitalisierung, technische Innovationen, mobile Kommunikation, Cloud Services und immer größere Datenmengen stellen enorme Anforderungen an IT-Netzwerke. Die Abhängigkeit von stabilen, sicheren Netzen wächst täglich und damit auch das Risiko eines Ausfalls. Ein Ausfall der gesamten IT-Infrastruktur kann Behörden lähmen. Das muss nicht sein.

Ein einziger Klick, ein instabiles System und der Betrieb steht still. Für Behörden kann ein Netzausfall fatale Folgen haben. Während die Digitalisierung der Verwaltung und Gesellschaft neue Möglichkeiten eröffnet, erhöht sie zugleich die Abhängigkeit von reibungslos funktionierenden Netzwerken. Ein Ausfall des eigenen Netzwerks kann nicht nur den Arbeitsalltag zum Erliegen bringen, sondern weitreichende gesellschaftliche, organisatorische und rechtliche Konsequenzen nach sich ziehen. Im schlimmsten Fall droht eine Gefährdung der öffentlichen Sicherheit.

Totalausfall im digitalen Zeitalter undenkbar.

Digitale Verwaltung ist vielerorts bereits Alltag. Anträge werden online gestellt, interne Kommunikation läuft über E-Mail-Server, Bürgerdaten werden in digitalen Archiven gespeichert. Fällt die gesamte IT-Infrastruktur aus, kann das Behörden stark beeinträchtigen. Abläufe, die vollständig auf digitale Prozesse angewiesen sind, kommen zum Stillstand – von der Bearbeitung von Anträgen über die Auszahlung von Sozialleistungen bis hin zur Koordination von Krisenstäben.

Verzögerungen und Prozessstillstand schaffen Unsicherheit.

Ein Netzausfall bedeutet für Behörden in erster Linie eines: Handlungsunfähigkeit. Denn die Liste der Dinge, die dann nicht mehr funktionieren, ist lang. Die Bearbeitung von Bürger:innenanliegen, das Ausstellen von Dokumenten, die Kommunikation mit ande-

ren Behörden sowie die Abstimmung unter Kolleg:innen. In digitalen Fachverfahren gespeicherte Informationen sind nicht mehr abrufbar, interne Datenbanken und Collaboration Tools stehen nicht zur Verfügung, die elektronische Aktenführung ist blockiert. Dadurch können Fristen versäumt, Termine nicht eingehalten werden und laufende Verfahren ins Stocken geraten. Gerade in Ministerien, die häufig an Gesetzesvorhaben oder politischen Abstimmungen beteiligt sind, kann ein Netzausfall den gesamten parlamentarischen Betrieb verzögern.

Hinzu kommt eine Gefahr, die auf den ersten Blick nicht erkennbar ist: Ein Netzausfall kann zum Einfallstor für Cyber-Angriffe werden. Systeme, die instabil oder offline sind, sind besonders anfällig. Hacker greifen solche Phasen gezielt an, um Schwachstellen auszunutzen, Schadsoftware einzuschleusen oder über Social Engineering Zugang zu erhalten. Gerade der Versuch, Systeme unter Zeitdruck wieder hochzufahren, birgt Risiken und kann dazu führen, dass Sicherheitsprotokolle umgangen oder aus Zeitmangel unvollständig geprüft werden. Fehler, die in dieser Situation entstehen, können schwerwiegendere Folgen haben als der Ausfall selbst.

Kritische Infrastrukturen sind besonders schützenswert.

Noch drastischer sind die Folgen für Einrichtungen, die Teil der öffentlichen Sicherheit sind. Polizei, Feuerwehr, Gesundheitsämter oder Krisenstäbe sind in ihrem Handeln unmittelbar auf eine funktionierende IT angewiesen.

Fällt das Netz aus, drohen Verzögerungen bei Notrufen, Koordinationsprobleme im Einsatz oder Lücken in der Krisenkommunikation. Viele Behörden haben Notfallpläne, Redundanzen oder Ersatzsysteme implementiert. Doch absolute Sicherheit gibt es nicht. Entscheidend ist, wie gut die Verwaltung vorbereitet ist und ob im Ernstfall klare Strukturen greifen.

Sichere, resiliente Systeme minimieren die Gefahren.

Die Antwort auf ein solches Szenario ist eindeutig: Resilienz muss zum zentralen Prinzip werden. Dazu gehören robuste technische Strukturen ebenso wie organisatorische Abläufe und geschultes Personal. Redundante Systeme, Backups und Zero-Trust-Architekturen verhindern, dass ein Ausfall die gesamte Infrastruktur lahmlegt. Notfallpläne und klare Kommunikationswege sorgen dafür, dass im Krisenfall jeder Schritt sitzt. Ebenso entscheidend ist die Sensibilisierung aller Mitarbeitenden, damit auch im Ernstfall keine unüberlegten Schnellschüsse erfolgen.

„Netze sind das Rückgrat der öffentlichen Verwaltung. Angesichts dieser vielfältigen Gefahren ist es für Behörden und Ministerien essenziell, in die Sicherheit und Resilienz ihrer Netzwerke zu investieren“, erläutert Thomas Teitge, Mitglied der Geschäftsleitung im Bechtle IT-Systemhaus Bonn und Geschäftsbereichsleiter Bundesbehörden, und ergänzt: „Zero Trust, Automatisierung und kontinuierliche Überwachung sind dafür unverzichtbar. Wer in Netze investiert, setzt nicht

nur auf maßgeschneiderte Lösungen, sondern auch auf regelmäßige Wartung, die Installation von Updates, die Schulung von IT-Personal sowie die intensive Vorbereitung auf Krisenfälle durch Notfallpläne und Backup-Systeme.“

Ein Netzausfall ist mehr als nur ein technischer Defekt – er kann Behörden in ihrer Funktionalität massiv beeinträchtigen und weitreichende Folgen für Staat, Verwaltung und Gesellschaft haben. Es ist daher unerlässlich, der IT-Sicherheit und der Ausfallsicherheit höchste Priorität einzuräumen und alle Mitarbeitenden für die Risiken zu sensibilisieren. Nur so kann die Digitalisierung der öffentlichen Verwaltung zum Erfolg werden – auch, wenn einmal das Netz ausfällt.

Und wenn das System dann doch mal ausfällt?

„Dann gilt es, einen kühlen Kopf zu bewahren, sich auf jeden Fall Hilfe von externen erfahrenen Dienstleistern ins Haus zu holen und vor allem keine unüberlegten Schnellschüsse vorzunehmen. Wir sehen leider sehr häufig, dass der posttraumatische Schaden durch falsche Reaktionen auf einen Ausfall weitaus schwerwiegendere Folgen nach sich ziehen kann als der Schaden selbst“, so Sabrina Wehner, Teamlead im Bechtle IT-Systemhaus Bonn.

Digitalisierung kann nur gelingen, wenn die Grundlage stimmt: ein sicheres und stabiles Netzwerk.



Der vzbv setzt sich für Belange der Bürger:innen ein.

Über den Verbraucherzentrale Bundesverband.

Der Verbraucherzentrale Bundesverband (vzbv) bündelt als Dachverband die Expertise von 16 Verbraucherzentralen und mehr als 30 verbraucherpolitischen Verbänden – darunter über 2.000 Organisationen und sieben Millionen Einzelmitglieder – für einen starken Schutz der Verbraucher:innen in Deutschland. Der vzbv ist die Stimme der Verbraucher:innen – und damit eine entscheidende Kraft in der Politik. Wir wissen, was Verbraucher:innen bewegt und verschaffen ihnen Gehör bei Politik, Wirtschaft und Verwaltung. Strukturelle Missstände decken wir auf, benennen Verbraucherprobleme und entwickeln Lösungen. So tragen wir dazu bei, dass Märkte transparent und gerecht gestaltet werden.

Passend dazu bieten wir Ihnen ein Webinar an:
14.10.2025 | 10:30 bis 12:00 Uhr

Anmeldung unter: <https://www.digitaler-staat.online/programm/>



Netzwerkausfälle sorgen immer wieder für Unmut bei Mitarbeitenden in Behörden und der öffentlichen Verwaltung.

Keine Lust mehr auf Leistungsdefizite.

Monatelang gab es beim Verbraucherzentrale Bundesverband (vzbv) Netzwerkprobleme, die zu wachsender Unzufriedenheit bei Mitarbeitenden und Kunden führten. Ein kompletter Refresh des Netzwerks mit HPE Aruba Networking Komponenten und Bechtle sorgte für Abhilfe.

Nachdem sich die Expert:innen von Bechtle und HPE Aruba Networking Anfang 2022 ein ausgiebiges Bild vom Ist-Zustand des Netzwerks beim vzbv machen konnten, war schnell klar, was passiert war. Über die Jahre war eine komplexe, inhomogene und schwer zu administrierende Infrastruktur herangewachsen, die durch Personalmangel, demografische Veränderungen und eine unvollständige Systemdokumentation noch verschärft wurde. Diese führte am Ende zu erheblichen Einschränkungen bei der Netzwerknutzung.

Um diese Probleme zu lösen, wurden im März und April 2022 auf Wunsch des vzbv bestehende Hardware-Komponenten im Access- und Core-Bereich ausgetauscht. Allerdings stellten die Beteiligten schnell fest, dass ein reiner Austausch noch nicht ganz den gewünschten Erfolg zur Stabilität der Systeme brachte.

Sabrina Wehner war damals schon Teamlead von Bechtle: „Wir hatten es zu Beginn mit einer sehr komplexen Infrastruktur und einer Vielzahl an unterschiedlichen Lösungen von unterschiedlichen Anbietern zu tun. Und als wir dann die neu bestellten Komponenten installiert hatten, ging für einen kurzen Moment nichts mehr.“ Das Team brachte zwar das System schnell wieder zum Laufen, man entschied sich dann aber mit dem Kunden gemeinsam, das Netzwerk noch mal ganzheitlich und strategisch zu planen und neu aufzusetzen.

Neuer Core-Bereich als Startpunkt für neue Gesamtausrichtung und Kostenersparungen.

Dieser Neustart begann mit einem klaren Fundament. Es wurde eine neue LAN-Infrastruktur mit HPE Aruba Networking CX 10.000 Series Switches als 100G-Netzwerkkern implementiert.

Neue Wi-Fi-6-Zugangspunkte wurden zusätzlich ergänzt, um die veralteten Komponenten zu ersetzen. Diese neue Architektur bietet dem vzbv heute eine modernes, skalierbares und leistungsstarkes Netzwerk mit integrierter Security-Asic für noch mehr Sicherheit. Die Wirkung war schnell spürbar. Anwendungen liefen stabil, Mitarbeitende konnten wieder störungsfrei arbeiten, die Zufriedenheit stieg merklich.

Und auch wirtschaftlich lohnte sich der Schritt: „Durch die Fokussierung auf einen Anbieter spart der vzbv heute erhebliche Kosten“, erklärt Wehner. „Teure Workarounds und endlose Abstimmungen zwischen verschiedenen Herstellern gehören der Vergangenheit an.“

Wie geht es weiter?

Doch die Reise ist noch nicht zu Ende. Bis 2026 will der vzbv die Infrastruktur weiter in Richtung Zero-Trust-Sicher-

heitsmodell entwickeln. Ein Proof of Concept für Zero Trust Network Access (ZTNA/SASE) ist bereits gestartet. Parallel sollen Monitoring-Tools vereinheitlicht und die aktuelle NAC-Lösung durch den HPE Aruba Networking ClearPass Policy Manager ersetzt werden. Ziel ist es, Sicherheit und Transparenz weiter auszubauen – und dabei die Netzwerkinfrastruktur so einfach wie möglich zu halten.

Was bleibt, ist die Erfahrung:

Über Jahre gewachsene Strukturen lassen sich nicht nur durch Hardware modernisieren. Erfolgsentscheidend ist die Verbindung von technischer Erneuerung und strategischer Neuausrichtung mit dem Mut aller Beteiligten, das Netzwerkprojekt konsequent umzusetzen.

Netzwerkausfälle von Anfang an vermeiden.

Viele Netzwerkausfälle haben ihren Ursprung nicht im Betrieb, sondern bereits in der Planungsphase. Häufig werden Anforderungen nicht detailliert erhoben, vorhandene Umgebungen nur unzureichend analysiert oder zusätzliche Systeme nicht berücksichtigt. Damit steigen die Risiken für spätere Störungen erheblich.

Ein erfolgreiches Netzwerkprojekt beginnt daher mit einer sorgfältigen Bestandsaufnahme und Simulation. Auf diese Weise lässt sich prüfen, wie eine stabile Abdeckung im gesamten Gebäude oder auf einem Gelände gewährleistet werden kann. Darauf aufbauend folgt die eigentliche Planung: Auswahl der geeigneten Komponenten, Definition der logischen Strukturen für LAN, WLAN und WAN sowie die Einbindung bestehender Systeme.

Ebenso entscheidend ist eine umfassende Dokumentation. Sie schafft Transparenz über alle relevanten Parameter und bildet die Grundlage für klare Notfallpläne. Erst danach beginnt die eigentliche Umsetzung – Konfiguration und Inbetriebnahme der Komponenten sowie die Integration in die bestehende Infrastruktur.

Doch bei einem einmaligen Aufbau darf es nicht bleiben. Netzwerke müssen kontinuierlich gepflegt, überwacht und weiterentwickelt werden. Regelmäßige Wartung, klare Prozesse für Updates und geschulte Techniker:innen sind der Schlüssel, um auch langfristig eine hohe Verfügbarkeit und Sicherheit zu gewährleisten.

Weitere Informationen zum Bechtle Rahmenvertrag über HPE Aruba Networking Lösungen finden Sie unter [bechtle.com/bund](https://www.bechtle.com/bund) sowie beim Beschaffungsamt des BMI (BeschA) unter der Vertragsnummer 21781.

indigo: Sicheres mobiles Arbeiten in der Bundesverwaltung.

Die öffentliche Verwaltung steht mitten in einem tief greifenden Wandel. Digitale Prozesse, neue Arbeitsmodelle und die Erwartungshaltung der Beschäftigten verändern den Arbeitsalltag in den Behörden. Immer stärker rückt dabei eine Frage in den Vordergrund: Wie lässt sich mobiles Arbeiten sicher und zugleich intuitiv gestalten?



Mitarbeitende in Behörden können iPhone und iPad bedenkenlos nutzen - bestätigt das BSI.

Bereits 2021 zeigte eine breit angelegte Studie auf Kommunal- und Landesebene der Universität Potsdam im Auftrag von PricewaterhouseCoopers (PwC): Homeoffice und flexible Arbeitsmodelle haben auch nach Ende der Corona-Pandemie großes Potenzial für die Verwaltung. Beschäftigte sehen darin nicht nur einen Gewinn an Flexibilität, sondern erwarten einen echten Digitalisierungsschub und fordern neue Arbeitsformen. Gleichzeitig kann die öffentliche Hand als Arbeitgeber attraktiver werden – etwa durch mehr Vereinbarkeit von Familie und Beruf. Zudem bietet sich der öffentlichen Verwaltung die Möglichkeit, Büroflächen zu reduzieren und damit Kosten zu sparen.

Die Befragten der PwC-Studie 2021 „Die Verwaltung im Homeoffice“ machten aber auch klar: Neben flexiblen Regelungen braucht es moderne IT-Ausstattung, digitale Kompetenzen und Vertrauen in die Zusammenarbeit. Eine weitere Untersuchung von Owl Labs aus dem Jahr 2023 bestätigt diesen Trend: Knapp drei Viertel der Beschäftigten im öffentlichen Dienst dürfen zumindest teilweise mobil arbeiten. Doch damit steigt auch die Verantwortung, Daten und Abläufe bestmöglich zu schützen. Denn anders als in vielen Unternehmen verarbeitet die Verwaltung sensible Bürger- und Behörden Daten, die höchsten Sicherheitsanforderungen unterliegen.

Mobil ja, aber sicher muss es sein.

Wer unterwegs oder von zu Hause arbeiten möchte, braucht die richtige Ausstattung. Eine, die den Anforderungen sowohl an Sicherheit als auch an eine einfache, unkomplizierte und intuitive Verwendung gerecht wird. Und da stoßen viele Lösungen an ihre Grenzen. Denn Dokumente bis zum Geheimhaltungsgrad VS-NfD sind nicht mit allen Tablets und Smartphones so ohne Weiteres zu öffnen und zu bearbeiten. Und andere Geräte wiederum, die die Sicherheitseigenschaften erfüllen, sind sehr komplex in der Nutzung. Denn Mitarbeitende in der öffentlichen Verwaltung, die auf ihrem Smartphone oder Tablet mit sicherheitskritischen Behörden- oder Bürgerdaten arbeiten wollen, mussten bisher eine kostenaufwendige Installation einer Container-Lösung auf ihrem Gerät in Kauf nehmen. Neben einem stark eingeschränkten Funktionsumfang litt die Benutzerfreundlichkeit dieser Lösungen auch an einem komplizierten und aufwendigen Authentifizierungsverfahren.

iPhone und iPad: Sicherste Mobilgeräte für die Verwaltung.

Im Jahr 2022 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Sicherheitseigenschaften von iPhone und iPad ausgiebig getestet, bestätigt und eine Freigabe von handelsüblichen iPhone und iPad Geräten für

den Einsatz durch die Behörden ausgesprochen. Mit der Einsatzerlaubnis sowie der Zulassung im Jahr 2024 erklärt das BSI, dass vertrauliche Informationen auf den Geräten von Apple ausreichend geschützt sind. Die vorinstallierten Apps für E-Mail, Kalender und Kontakte sind sicher genug für die Verarbeitung von Verschlusssachen der Kategorie „Nur für den Dienstgebrauch“. Damit eignen sich iPhone und iPad ideal für den Einsatz in Behörden und der öffentlichen Verwaltung.

Vorteile für Beschäftigte und Behörden.

Für die Beschäftigten bedeutet indigo eine erhebliche Erleichterung. Sie erhalten ein vorkonfiguriertes Gerät, das sofort einsatzbereit ist. Mail, Kalender und Kontakte sind bis VS-NfD direkt nutzbar, zusätzliche Installationen oder komplizierte Anmeldungen entfallen. Gleichzeitig bleibt die private Nutzung möglich, ohne dass dienstliche Daten kompromittiert werden. Das steigert nicht nur die Akzeptanz, sondern auch die Zufriedenheit – ein entscheidender Faktor für Motivation und Produktivität.

Behörden wiederum profitieren von deutlich vereinfachten Prozessen. Rollouts lassen sich in kurzer Zeit durchführen, Updates laufen automatisiert und der Supportaufwand sinkt. IT-Abteilungen gewinnen Zeit für andere Aufgaben, während die Verwaltung

insgesamt agiler und flexibler wird. Nicht zuletzt entstehen Kostenvorteile: Containerlösungen und zusätzliche Sicherheitssoftware sind nicht mehr erforderlich.

indigo als Faktor im Wettbewerb um Talente.

Die öffentliche Verwaltung konkurriert zunehmend mit der Privatswirtschaft um qualifizierte Fachkräfte. Jüngere Generationen erwarten flexible Arbeitsmodelle und moderne technische Ausstattung. indigo trägt dazu bei, diesen Erwartungen gerecht zu werden. Beschäftigte arbeiten auf Geräten, die sie aus ihrem Alltag kennen, und nutzen sie nun auch im beruflichen Kontext – sicher, komfortabel und ohne Einschränkungen. Das erhöht die Attraktivität des öffentlichen Dienstes als Arbeitgeber und verschafft der Verwaltung im Wettbewerb um Talente wichtige Vorteile für die Zukunftsfähigkeit.

Rahmenbedingungen und Einführung.

Damit Apple Endgeräte mit indigo flächendeckend in der Bundesverwaltung eingesetzt werden können, hat das Beschaffungsamt des BMI (BeschA) mit Bechtle einen mehrjährigen Rahmenvertrag geschlossen. Bis zu 300.000 Geräte können hierüber abgerufen werden, ergänzt um Dienstleistungen wie Beratung, Integration, Lifecycle-Management und Support sowie

Zubehör für iPhone und iPad. Damit ist sichergestellt, dass indigo nicht nur technologisch, sondern auch organisatorisch auf soliden Bahnen eingeführt wird.

iPad Workplace – die ergänzende Grundlage für effizienteres Arbeiten unterwegs.

Mit dem iPad Workplace wird die mobile Transformation in Bundesbehörden vorangetrieben, sodass Mitarbeitende jederzeit und überall arbeiten können. Er bietet nahtlose Kommunikation und Zusammenarbeit von jedem Standort, die Benutzeroberfläche ist intuitiv zu bedienen. Der iPad Workplace ist kosteneffizient, spart Ressourcen und maximiert die Leistung. Das steigert die Motivation der Mitarbeitenden, reduziert administrative Aufgaben und auch den Aufwand für Dokumentationen.

Mobiles Arbeiten ohne Kompromisse.

indigo ist mehr als ein technisches Projekt. Es zeigt, dass mobiles Arbeiten im öffentlichen Dienst ein fester Bestandteil moderner Arbeitsorganisation sein kann. Behörden gewinnen an Effizienz, Mitarbeitende an Flexibilität, der Staat an Attraktivität als Arbeitgeber.

indigo – Konfiguration zum Betrieb von iPhone und iPad unter VS-NfD.

Im Umfeld der Nutzung von Apple Geräten für Bundesbehörden fällt immer wieder der Begriff indigo. Was damit gemeint ist, erklären wir hier.

indigo steht für iOS Native Devices In Government Operation. Die besondere Konfiguration ermöglicht es, Apple Geräte wie iPhone und iPad zu konfigurieren und sicher in deutschen Behörden zu nutzen. Das BSI hat die Wirksamkeit der in iOS und iPadOS eingebetteten Sicherheitsmechanismen bestätigt. Mitarbeitende der Bundesverwaltung haben somit die Möglichkeit, vertrauliche Inhalte wie sicherheitskritische Behörden- und Bürgerdaten, die als Verschlusssache und „Nur für den Dienstgebrauch“ (VS-NfD) eingestuft sind, auf iPhone und iPad zu übertragen und zu bearbeiten.

Nativ auf iOS und iPadOS bedeutet, dass die in der Bundesverwaltung geforderten Sicherheitsmechanismen bereits standardmäßig in die beiden Betriebssysteme integriert sind. Für iPhone und iPad sind daher keine zusätzlichen Sicherheitslösungen eines Drittanbieters mehr notwendig. Alle iPhone Geräte ab iOS 15.6.1 und alle iPad Modelle ab iPadOS 15.6.1 verfügen über die entsprechende Zulassung durch das BSI.

Deutliche Kosteneinsparungen möglich.

Im Interview spricht Thomas Teitge, Mitglied der Geschäftsleitung im Bechtle Systemhaus Bonn und Geschäftsbereichsleiter Bundesbehörden, über die Nutzung von iPad und iPhone für Bundesbehörden, die Freigabe durch das BSI und mögliche Kosteneinsparungen.

Herr Teitge, was genau hat das BSI zur Nutzung von iPhone und iPad für Bundesbehörden gesagt?

Teitge: Mit der Einsatzerlaubnis erklärt das Bundesamt, dass vertrauliche Informationen auf den Geräten von Apple ausreichend geschützt sind. Damit können Informationen bis zum Geheimhaltungsgrad „Verschlusssache – nur für den Dienstgebrauch“ (VS-NfD) auf iPhone und iPad übertragen und verarbeitet werden. Dabei handelt es sich um das handelsübliche Apple Betriebssystem (iOS bzw. iPadOS), in das die geforderten Sicherheitsmechanismen bereits nativ integriert sind.

Der Zugriff auf VS-NfD-Daten über E-Mail, Kalender und Kontakte wird so ohne Notwendigkeit weiterer Sicherheitslösungen möglich. Besonders daran ist, dass es die erste Lösung ihrer Art ist, für die das BSI nach umfassender Prüfung eine Zulassung erteilt hat. Die Informationssicherheit ist bei diesen handelsüblichen Produkten tat-

sächlich von Anfang an mitgedacht und kann schnell und kostengünstig eingesetzt werden.

Welche Vorteile ergeben sich dadurch?

Teitge: Für iPhone und iPad sind keine zusätzlichen Sicherheitslösungen eines Drittanbieters mehr notwendig, denn mit der durch das BSI erteilten Zulassung wird das entsprechende Sicherheitsniveau erreicht. Dies ermöglicht es Mitarbeitenden, auf iPhone und iPad auch mobil mit sicherheitskritischen Behörden- und Bürgerdaten zu arbeiten, während Datenschutz und Datensicherheit bis zum Geheimhaltungsgrad VS-NfD sichergestellt werden. Auch die Einhaltung von DSGVO-Richtlinien bleibt durch die Lösung gewahrt und erlaubt die parallele persönliche Nutzung des Geräts. Die Freigabe des BSI von handelsüblichen iOS Geräten nativ bedeutet nicht nur deutliche Kosteneinsparungen von zirka 65 Prozent je nach Modell, sondern

vereinfacht die IT in den Behörden auch erheblich. So können Zeit und Kosten eingespart werden und wir können für unsere Kunden aus dem öffentlichen Bereich Budget-Engpässe vermeiden.

Was ändert sich für die Mitarbeitenden konkret?

Teitge: Die Geräte sind sofort einsatzbereit. Wir konfigurieren sie vor, registrieren sie im Apple Business Manager und binden sie ins Mobile Device Management der jeweiligen Behörde ein. Nutzer:innen können ihr Gerät einschalten und sind direkt arbeitsfähig. Keine zusätzlichen Container, kein kompliziertes Anmelden – einfach starten.

Wie erfolgt die technische Umsetzung und welche Vorteile ergeben sich für Behörden?

Teitge: Bechtle ist autorisierter Fachhandelspartner von Apple. Unsere

Mitarbeitenden haben ein besonderes technisches Training durchlaufen und folgen einem festen Anforderungskatalog, wie indigo für VS-NfD zu konfigurieren und einzusetzen ist. Die ordnungsgemäße Einrichtung der Geräte attestieren wir in einer Dokumentation und einem Abnahmeprotokoll. iPhone und iPad werden über Bechtle erworben und direkt im Apple Business-Manager-Konto der jeweiligen Behörde registriert. Ebenso erfolgen der Erwerb der vom BSI vorgeschriebenen Dienste – also des Mobile Device Managements (MDM) – und die Integration über ein Virtual Private Network (VPN).

Behörden profitieren von standardisierten Prozessen.

Rollouts lassen sich in sehr kurzer Zeit umsetzen, Updates erfolgen automatisch, der Supportaufwand sinkt. Das reduziert die Komplexität und schafft Ressourcen für andere Aufgaben.



Selbst vertrauliche Inhalte können unterwegs bearbeitet werden.

Weitere Informationen zu den Bechtle Rahmenverträgen über Apple Lösungen finden Sie unter bechtle.com/bund sowie beim Beschaffungsamt des BMI (BeschA) unter der Vertragsnummer 53573 für Los 1 und 53574 für Los 2.

Vor diesem Hintergrund rücken technologische Ansätze wie die Appian Plattform in den Fokus. Sie ermöglicht eine flexible Ende-zu-Ende-Digitalisierung (E2E) und die Automatisierung von Verwaltungsprozessen, sie beschleunigt die Entwicklung von Verwaltungssoftware, senkt Kosten, verbessert zugleich die Bedienbarkeit – und das bei vielen Verwaltungen in Europa und der Welt.

Was bedeutet Low- Code?

Bei klassischen IT-Projekten werden Fachverfahren von Grund auf programmiert – ein Prozess, der viel Zeit, Budget und IT-Know-how erfordert. Low-Code verfolgt einen anderen Ansatz: Anwendungen entstehen auf Basis vorgefertigter Bausteine (LeKa), die zusammengefügt werden. Fachanwender:innen in den Behörden können danach selbst Masken, Workflows oder Schnittstellen umgestalten, ohne tief gehende Programmierkenntnisse, um ihre angepasste Applikation zu erhalten. Nachnutzung ist hier nicht nur ein Vorhaben, sondern Realität.

Treiber für die Verwaltungsmodernisierung.

Für die deutsche Verwaltung eröffnet sich dadurch die Möglichkeit, Prozesse, die bisher Monate oder Jahre in Anspruch nahmen, innerhalb weniger Wochen oder sogar Tage zu digitalisieren. Denn alle wichtigen Fragen bezüglich Sicherheit, Datenschutz und Barrierefreiheit sind vorab durch die Plattformvorgaben entschieden. Besonders in einem föderalen System mit zahlreichen unterschiedlichen Fachverfahren ist dies von großer Relevanz. Lösungen, die in einer Kommune entwickelt wurden, lassen sich ohne Aufwand an die Bedürfnisse anderer Behörden anpassen.

Ein Beispiel macht das Potenzial deutlich: Während bislang Förderprogramme bei jeder neuen Rechtsänderung aufwendig angepasst werden mussten, können Low-Code-Plattformen solche Änderungen in kürzester Zeit abbilden, ohne dass die Bearbeitung laufender Anträge beeinträchtigt wird. Das Versionieren von Prozessen reduziert den Aufwand erheblich und sorgt für mehr Transparenz im Varianten-Management.

„Low-Code ist ein echter Hebel für die Verwaltung.“

Ein Gespräch mit Christian Rupert Maierhofer (CRM), Geschäftsbereichsleiter des Competence Centers AV Software Solutions 360° (AV) von Bechtle.

Herr Maierhofer, Bechtle hat jüngst einen weiteren großen Zuschlag im Bereich Low-Code erhalten. Können Sie uns den Hintergrund erläutern?

Maierhofer: Wir konnten uns bereits 2024 mit dem Produkt Appian ein Los der Rahmenvereinbarung für Low-Code-Lizenzen sichern. Darauf aufbauend hat unser Konsortium in diesem Sommer gemeinsam mit weiteren Anbietern einen Zuschlag für die Bereitstellung von Umsetzungsressourcen erhalten. Das bedeutet: Behörden bekommen alles aus einer Hand – von der Lizenz über die Schulung, Entwicklung und den Rollout bis hin zum Betrieb und der Weiterentwicklung von Applikationen. Bezugsberechtigt sind Bund, Länder und Kommunen. Für uns ist das ein starkes Signal, dass die Verwaltung konsequent auf Low-Code setzt.

Was genau versteht man unter Low-Code und warum ist es für Behörden so relevant?

Maierhofer: Im Kern geht es bei Low-Code darum, Softwareanwendungen ohne klassische Programmierung, also ohne zeilenweise Code, zu entwickeln. Stattdessen werden Module und visuelle Oberflächen genutzt. Das eröffnet zwei wesentliche Vorteile: Zum einen entfallen klassische Wartungskosten der Applikationen. Zum anderen können Mitarbeitende der Verwaltung selbst eingebunden werden, sogenannte „Government Developer“. Sie kennen ihre Prozesse am besten und können aktiv an deren Digitalisierung mitwirken. Dazu haben wir spezielle Lernpfade und Qualifikationen entwi-

Low-Code als Schlüsseltechnologie für moderne Behörden.

Die digitale Transformation der Verwaltung in Deutschland ist ein Langstreckenprojekt, geprägt von komplexen Fachverfahren, gewachsenen IT-Strukturen und oft langwierigen Entwicklungszyklen. Einige Prozesse sind noch immer nur teilweise digitalisiert. Formulare lassen sich zwar online ausfüllen, doch im Hintergrund laufen die Abläufe häufig unverändert analog oder hybrid weiter. Für Bürger:innen bedeutet das lange Bearbeitungszeiten, für Verwaltungen hohen Aufwand, eingeschränkte Flexibilität und einen geringen Automatisierungsgrad.



Deutschland ist bei der Digitalisierung auf einem guten Weg.

Vorteile für Bürger:innen und Bürger.

Die Interoperabilität von Daten ist die DNA, da Daten nur einmal erfasst werden müssen und auf Wunsch allen anderen Applikationen zur Verfügung stehen. Dadurch sinkt die Fehleranfälligkeit und Verfahren werden beschleunigt. Mit Appian werden darüber hinaus die notwendigen technischen Voraussetzungen geschaffen, um das National-Once-Only-Technical-System (NOOTS) flexibel in bestehende Antragsprozesse zu integrieren. So können Nachweise wie etwa Meldebescheinigungen oder Geburtsurkunden künftig digital bereitgestellt und sicher zwischen Behörden übertragen werden.

Herausforderungen und Chancen.

Natürlich lassen sich nicht alle Fachverfahren über Nacht digitalisieren. Viele Abläufe sind komplex, rechtlich

nicht reguliert oder erfordern eine tiefe Integration in bestehende Systeme. Appian bietet mit der Data Fabric die Möglichkeit, aus einer großen Anzahl von Fachverfahren eine völlig neue, prozessorientierte Anwendung zu generieren, ohne die Daten zu kopieren oder die Nachvollziehbarkeit zu diskreditieren. Ebenso können große Fachverfahren modular modernisiert werden, beispielsweise durch eine zeitgemäße Benutzeroberfläche. Gleichzeitig ergeben sich neue Anforderungen: Verwaltungen müssen ihre Mitarbeitenden entsprechend qualifizieren, um die Plattformen effizient nutzen zu können.

Ein Baustein dualer Souveränität.

Mit Appian eröffnet sich für die Verwaltung ein neuer Weg, digitale und individuelle Souveränität zu stärken. Nicht nur die Herkunft eines Produk-

tes und dessen geopolitische Beeinflussbarkeit, sondern auch die mündige Bedienbarkeit stehen im Fokus. Behörden gewinnen die Fähigkeit, Fachverfahren eigenständig zu gestalten und flexibel anzupassen. Damit sinkt die Abhängigkeit von langwierigen Ausschreibungen, und die Verwaltung bleibt in Krisensituationen handlungsfähig.

Low-Code-Technologie allein wird die Herausforderungen nicht lösen. Doch sie bietet einen wichtigen Hebel, um die digitale Modernisierung der Verwaltung zu beschleunigen. Wenn es gelingt, sie klug einzusetzen und in übergreifende Strategien einzubetten, könnte Low-Code-Technologie zu einem Katalysator werden: für eine effizientere Verwaltung, für besseren Bürgerservice und für einen Staat, der digital handlungs- und zukunftsfähig bleibt.

Verbesserte Tierseuchenbekämpfung mit Low-Code.

Eines der aktuellen Projekte des Bechtle Competence Centers für Ende-zu-Ende-Digitalisierung (E2E), AV Software Solutions 360°, umfasste einen Proof of Concept für ein Krisenverwaltungsprogramm bei der Tierseuchenbekämpfung auf Basis moderner Low-Code-Technologie. Ziel war es, die Eignung dieser Technologie für die Abbildung komplexer Verwaltungsprozesse im veterinärmedizinischen Krisenmanagement zu evaluieren und praxisnah zu erproben.

Das Projekt möchte aufzuzeigen, wie die deutschen Veterinärämter durch automatisierte Prozesse entlastet werden können, die behördenübergreifende Zusammenarbeit verbessert und die Einsatzfähigkeit in Krisensituationen erhöht werden kann. Der gezeigte PoC ermöglicht schnelle, regelbasierte Maßnahmenentscheidungen, gewährleistet eine einheitliche und zentrale Datenhaltung und integriert in moderner Weise verschiedenste Beteiligte für maximale Transparenz, operative Effizienz und Reaktionsfähigkeit im Krisenmanagement.

Stefanie Kreitlow, Dezernatsleiterin (Servicezentrum Landentwicklung und Agrarförderung/Dezernat K – Koordinierungs- und Kommunikationsstelle (KKS)) erläutert dazu: „Der PoC zeigt, wie Low-Code-Technologie eine effiziente Prozessautomatisierung ermöglicht, um die Zusammenarbeit zu verbessern, im Krisenfall schnell und koordiniert zu handeln und damit den gesundheitlichen Verbraucherschutz und das Veterinärwesen nachhaltig zu stärken. Low-Code-Technologie erfüllt ihr Geschwindigkeitsversprechen in der Entwicklung und fordert damit alle Mitwirkenden heraus, entsprechend gleichzuziehen und sich fokussiert einzubringen.“



Tierseuchenbekämpfung profitiert von Low-Code.

Alles aus einer Hand.

Nach dem Gewinn eines ersten Rahmenvertrags 2024, der die Bereitstellung von Low-Code-Plattformlizenzen umfasste, erhielt Bechtle Mitte 2025 gemeinsam mit weiteren Anbietern den Zuschlag für einen weiteren Rahmenvertrag im Bereich Low-Code. Im Mittelpunkt steht diesmal die Bereitstellung von Umsetzungsressourcen für Digitalisierungsprojekte. Damit entsteht ein vollständiges Angebot aus einer Hand – von der Lizenz über die Entwicklung, den Rollout und den Betrieb bis hin zur Weiterentwicklung und Qualitätssicherung von Applikationen auf Basis der Plattform von Appian.

Das Angebot erfüllt dabei die aktuellen Anforderungen an IT-Sicherheit, Barrierefreiheit und die nahtlose Integration in bestehende IT-Landschaften vollständig. Die öffentliche Hand erhält damit einen umfassenden und skalierbaren Zugang zu Low-Code-Technologien, die eine beschleunigte Entwicklung digitaler Anwendungen sowie automatisierter Prozesse ermöglichen. Bezugsberechtigt sind alle Einrichtungen des Bundes, der Länder und der Kommunen in Deutschland.

Weitere Informationen zu den Bechtle Rahmenverträgen über Low-Code-Lösungen finden Sie unter [bechtle.com/bund](https://www.bechtle.com/bund), per E-Mail an avs.bonn@bechtle.com sowie bei der PD - Berater der öffentlichen Hand GmbH unter den Vergabenummern 2023-I-055 und 2024-I-097.



gaben, während Bürger:innen von schnelleren Verfahren profitieren.

Ein weiterer Punkt ist die Planung. Oft wird in der Verwaltung lange geplant, bevor überhaupt ein Ergebnis sichtbar wird. Ändert sich das mit Low-Code?

Maierhofer: Ja, das ist ein echter Kulturwandel. Mit klassischen IT-Projekten gab es die Sorge, Fehler zu machen und technische Schulden anzuhäufen. Low-Code erlaubt dagegen ein schnelles Ausprobieren – das sogenannte „fast fail“. Fehler werden früh sichtbar und können ohne großen Aufwand korrigiert werden. Das nimmt die Angst vor dem Scheitern und fördert Innovation.

Wie ordnen Sie die Rolle von Bechtle in diesem Feld ein?

Maierhofer: Mit AV Software Solutions 360° bündeln wir technologische Low-Code-Expertise und Umsetzungskompetenz der öffentlichen Verwaltung. Gemeinsam mit Appian stellen wir nicht nur die Plattform, sondern auch die Projektteams bereit, die Behörden bei Entwicklung, Rollout und Betrieb unterstützen. Wir verstehen uns dabei als Enabler der öffentlichen Verwaltung: Wir schaffen die Voraussetzungen, damit digitale Transformation nicht Theorie bleibt, sondern im Alltag wirkt. Durch die enge Zusammenarbeit sind heute in Deutschland nahezu 600 Menschen verfügbar, die mit der Appian-Plattform die Digitalisierung vorantreiben.

Was macht Appian zum „Perfect Fit“?

Maierhofer: Die Appian-Plattform war

für uns nicht von Anfang an der „Perfect Fit“. Doch im Laufe der Zeit, mit gezielter Vorbereitung und konsequenter Weiterentwicklung, konnten wir die Plattform souveränisieren. Was heißt das genau? Zum einen haben wir uns in die Lage versetzt, selbst Lizenzen auszustellen und mit StackIT einen souveränen MidScaler aufzubauen. Dadurch konnten wir Schritt für Schritt deutsche Firmen und Lösungen integrieren und darüber hinaus auch Eigenentwicklungen des Bundes wie KIPITZ integrieren. Damit ist Appian für uns zum „Perfect Fit“ geworden, denn wir verfügen nun über ein souveränes, vertrauenswürdiges und in Deutschland betriebenes System, das die Basis für zukünftige Innovationen und nachhaltige Digitalisierung schafft.

Und ein Blick nach vorn: Welche Themen werden in den kommenden Jahren wichtig?

Maierhofer: Das Datenvolumen in der Verwaltung wächst weiter und neue Technologien wie künstliche Intelligenz erhöhen die Anforderungen an Flexibilität und Geschwindigkeit. Low-Code gewinnt in diesem Zusammenhang an Bedeutung, da sich KI-Funktionen wie Sprachsteuerung, Mustererkennung oder Barrierefreiheit unkompliziert in Legacy Applications integrieren lassen. Gleichzeitig spielt die digitale Souveränität eine zentrale Rolle. Plattformen müssen so entwickelt werden, dass sie den europäischen Anforderungen entsprechen. An dieser Weiterentwicklung sind wir aktiv beteiligt.

Cyber-Security in Zeiten globaler Unsicherheit.

Rund ein Fünftel aller IT-Sicherheitsvorfälle in der EU betrifft laut dem Sicherheitsbericht des BSI öffentliche Verwaltungen. 2024 gab es im Vergleich zum Vorjahr bereits 26 Prozent mehr neue Malware-Varianten. 20.000 Arbeitsplätze waren 2023 bei einem Ransomware-Angriff auf einen kommunalen IT-Dienstleister betroffen. Diese Zahlen belegen, dass die zunehmende Digitalisierung in der Bundesverwaltung neben großen Chancen auch wachsende Angriffsflächen bietet. IT-Sicherheit muss deshalb oberste Priorität haben. Dazu haben wir uns mit Thomas Teitge, Mitglied der Geschäftsleitung im Bechtle Systemhaus Bonn sowie Geschäftsbereichsleiter Bundesbehörden, und Tabea Breternitz, Head of Federal Government & Defense, von Trend Micro unterhalten.

Was sind aus Ihrer Sicht derzeit die größten Herausforderungen für die IT-Sicherheit in der öffentlichen Verwaltung?

Teitge: Die größte Herausforderung liegt heute in der Kombination aus wachsender Bedrohungslage, begrenzten Ressourcen und der Geschwindigkeit, mit der sich die Angriffsszenarien verändern. Wir sehen, dass Cyber-Security längst nicht mehr nur ein technisches Thema ist. Cyber-Security ist die Grundvoraussetzung für die Handlungsfähigkeit des Staates. Gleichzeitig müssen Behörden ihre Strukturen so aufstellen, dass sie mit den vorhandenen Ressourcen schnell reagieren können, ohne dabei ihre Prozesse zu überfrachten. Das erfordert klare Verantwortlichkeiten, verlässliche Partner und ein strategisches Verständnis für IT-Sicherheit – vom operativen Betrieb bis zur Entscheidungsebene.

Breternitz: Gerade die Bundesbehörden stehen stark im Fokus von Cyber-Angriffen. Besonders gefährlich sind dabei zielgerichtete Angriffe staatlicher Akteure, beispielsweise im Rahmen von Spionage- und Sabotage-Operationen. Gleichzeitig verschimmt zunehmend die Grenze zwischen staatlichen Akteuren und Cyber-Kriminellen, was die Bedrohungslage sehr unübersichtlich macht: Andere Staaten setzen auf Cyber-Söldner oder sogenannte „Hacktivist:innen“ (von „Hacking“ und „Aktivist:innen“), die mit Cyber-Methoden gegen Staaten, Einrichtungen oder Unternehmen vorgehen, die sie als Feindbild betrachten. Und natürlich gibt es auch noch die „ganz gewöhnliche“ Cyber-Kriminalität, für die Behörden ebenfalls ein attraktives Ziel darstellen.

Wie gut sind Bundesbehörden heute aufgestellt, um mit diesen Bedrohungen umzugehen, und wo sehen Sie die größten Lücken oder Risiken?

Teitge: Bundesbehörden haben in den letzten Jahren große Fortschritte gemacht – sowohl bei der Sensibilisierung als auch bei der technischen Absicherung. Trotzdem gibt es noch Hürden. Eine davon ist die hohe Komplexität in der Beschaffung und Integration neuer Sicherheitslösungen. Hinzu kommt, dass sich Fachkräftemangel und steigende Anforderungen oft gegenseitig verstärken. Unsere Erfahrung zeigt: Es braucht klare, standardisierte Beschaffungswege, eine enge Verzahnung zwischen IT-Betrieb und strategischer Sicherheitsplanung sowie den Mut, neue Technologien schnell, aber kontrolliert einzuführen.

Breternitz: Neben den bereits genannten Hürden sehen wir, wenn wir auf die Bundesverwaltung als Ganzes schauen, dass trotz der verbesserten Sensibilisierung immer noch ein Bewusstseinswandel notwendig ist. Alle Mitarbeitenden müssen sich darüber bewusst sein, dass sie ein mögliches Angriffsziel sind. Viele Cyber-Angriffe setzen noch immer auf den Menschen als schwächstes Glied in der Kette der IT-Sicherheit.

Der Rahmenvertrag zur IT-Sicherheit, den das Beschaffungssamt des BMI (BeschA) mit Bechtle geschlossen hat, soll bei der Beschaffung und Integration sicherer IT-Infrastrukturen helfen. Welche Vorteile bietet er konkret für Bundesbehörden?

Breternitz: Eine beschleunigte Beschaffung von technologisch führenden Sicherheitslösungen ohne individuelles Ausschreibungsverfahren. Wir als Trend Micro bringen sichere Lösungen für Endpunkte, Server sowie Netzwerke in den Rahmenvertrag mit ein und sind als weltweit führendes Unternehmen in dieser Branche gemeinsam mit Bechtle vertrauenswürdige und bewährte Partner, die für ein Höchstmaß an Sicherheit und Verlässlichkeit stehen.

Teitge: Darüber hinaus bietet er die Sicherheit, dass alle rechtlichen, technischen und organisatorischen Anforderungen bereits kontrolliert sind und auf geprüfte, standardisierte Lösungen und Dienstleistungen zurückgegriffen wird. Für uns als Partner ist er die Grundlage, um passgenaue Leistungen zu erbringen – von der Beratung über die Integration bis hin zum Betrieb.

Wie ist die Zusammenarbeit zwischen Trend Micro und Bechtle innerhalb des Rahmenvertrags organisiert – und was macht sie besonders effektiv?

Breternitz: Wir haben eine klare Rollenverteilung, die sich in der Praxis sehr bewährt. Wir bei Trend Micro stellen als Technologielieferant unsere Cyber-Sicherheitslösungen zur Verfügung. Kunden profitieren damit von unserer jahrzehntelangen Expertise im Bereich der IT-Sicherheit, globaler Bedrohungsforschung und kontinuierlichen Innovationen. Unsere Forschungsteams sind weltweit angesiedelt und liefern täglich Erkenntnisse zu neuen Bedrohungen, die in unsere Lösungen einfließen und helfen, unsere Kunden noch besser zu schützen.

Teitge: Unsere Aufgabe bei Bechtle ist es, die Technologien von Trend Micro nahtlos in die bestehenden IT-Umgebungen der Behörden zu integrieren, den Betrieb abzusichern und bei Bedarf auch dauerhaft zu begleiten. Als langjähriger Partner kennen wir die Strukturen, Prozesse und Besonderheiten der Bundesverwaltung im Detail und sind immer nah an unseren Kunden.

Mit welchen Anliegen wenden sich Behörden typischerweise an Sie – und wie begegnen Sie diesen Bedarfen?

Teitge: Häufig geht es um drei Themenfelder: erstens die Absicherung der bestehenden IT-Infrastruktur, zweitens den Aufbau resilienter Sicherheitsprozesse und drittens die Qualifizierung der eigenen Mitarbeitenden. Wir unterstützen dabei mit strukturierten Services – vom initialen Sicherheits-Check über praxisnahe Schulungen bis hin zu Managed Services, bei denen wir den Betrieb und die Überwa-

chung dauerhaft übernehmen. Wichtig ist, dass jede Maßnahme in den strategischen Gesamtrahmen der Behörde passt und nicht als isolierte Einzelmaßnahme verpufft.

Gerade im öffentlichen Sektor ist Vertrauen essenziell. Wie gelingt es Trend Micro, als international tätiges, japanisches Unternehmen dieses Vertrauen in Deutschland zu stärken?

Breternitz: Trend Micro ist schon seit über 35 Jahren am Markt und wird bis heute von einer der Gründerinnen, unserer CEO Eva Chen, geführt. Um so lange Zeit erfolgreich zu sein, sind stetige Innovationen und das Vertrauen unserer Kunden essenziell. Um dieses Vertrauen gerade im öffentlichen Sektor zu stärken, legen wir großen Wert auf Verlässlichkeit und Transparenz, auch in engem Austausch mit dem BSI. Als japanisches Unternehmen profitieren unsere Kunden zudem von einer Reihe rechtlicher und politischer Verschränkungen, welche die Beziehungen zwischen Deutschland, der EU und Japan in den Bereichen Cyber-Sicherheit und Datenschutz prägen. Dazu zählen unter anderem ein Angemessenheitsbeschluss für das Datenschutzniveau sowie das deutsch-japanische Geheimschutzabkommen. Gleichzeitig legen wir großen Wert auf lokale Präsenz und sind schon seit vielen Jahren ein verlässlicher Sicherheitspartner für deutsche Behörden auf allen Ebenen der staatlichen Verwaltung.

Mit dem Aufkommen von KI verändert sich auch die Bedrohungslage für Behörden. Inwiefern kann künstliche Intelligenz aber auch zur Stärkung der Cyber-Sicherheit beitragen?

Breternitz: Künstliche Intelligenz kommt in der Cyber-Sicherheit schon seit vielen Jahren zum Einsatz, gerade im Bereich der Bedrohungserkennung. Anders könnten wir der schieren Masse an neuen Angriffen jeden Tag gar nicht wirksam begegnen. Die aktuell aufkommenden, fortschrittlichen KI-Technologien ermöglichen jetzt aber noch viel mehr: Indem sie interne Security-Daten aus der Umgebung analysiert und mit externen Bedrohungsinformationen („Threat Intelligence“) korreliert, kann die KI Cyber-Risiken erkennen, bewerten, priorisieren und auf Wunsch sogar automatisiert beseitigen. Das entlastet die Mitarbeitenden deutlich und ermöglicht es ihnen, Cyber-Sicherheit proaktiv anzugehen, statt ständig nur Warnmeldungen „hinterherzulaufen“.

Teitge: Künstliche Intelligenz hat zudem das Potenzial, die IT-Sicherheit in Behörden auf einen neuen Level zu heben, vorausgesetzt, sie wird verantwortungsvoll eingesetzt. Sie kann enorme Datenmengen in Echtzeit analysieren, Anomalien erkennen und so Bedrohungen identifizieren, bevor sie Schaden anrichten. Gleichzeitig unterstützt sie bei der Automatisierung von Routineaufgaben, sodass IT-Teams mehr

Zeit für strategische Aufgaben haben. Wichtig ist, dass KI nicht als Ersatz, sondern als Verstärker menschlicher Expertise verstanden wird. Dies immer in einem klaren organisatorischen und rechtlichen Rahmen.

Digitale Souveränität ist ein zentrales Thema. Wie sichern Bechtle und Trend Micro gemeinsam die digitale Souveränität für die öffentliche Verwaltung und wie kann ein Gleichgewicht zwischen internationaler Expertise und nationaler Kontrolle gelingen?

Teitge: Digitale Souveränität bedeutet für uns, dass Behörden jederzeit die Kontrolle über ihre Daten, Systeme und Sicherheitsentscheidungen behalten. Dies unabhängig davon, welche Technologien sie nutzen. In der Partnerschaft mit Trend Micro setzen wir auf volle Transparenz, nachvollziehbare Prozesse und eine enge Abstimmung mit den zuständigen Stellen. So stellen wir sicher, dass internationale Expertise und nationale Anforderungen im Gleichgewicht stehen. Das ist die Basis, um langfristig Vertrauen zu schaffen und die Handlungsfähigkeit der Verwaltung zu sichern.

Breternitz: Leider wird digitale Souveränität in der aktuellen Debatte häufig falsch auf das Thema „Autarkie“ verkürzt. Doch Souveränität erschöpft sich eben nicht im Rückzug auf das Eigene, sondern vielmehr, wie Thomas bereits erwähnt hat, darauf, selbstbestimmt zu handeln und zu entscheiden. Dazu zählt auch die Möglichkeit, zwischen Alternativen von leistungsfähigen und vertrauenswürdigen Partnern zu entscheiden und diese bewusst und verantwortungsvoll einzusetzen. Neben anderen EU-Mitgliedstaaten zählt Japan für Deutschland zu den engen „Wertepartnern“, mit denen die Bundesrepublik eine „umfassende strategische Partnerschaft“ pflegt und diese laut aktuellem Koalitionsvertrag auch weiter ausbauen will.

Was unterscheidet Ihre gemeinsame Lösungskompetenz von anderen Anbietern – und warum lohnt es sich für Bundesbehörden, auf diese Partnerschaft zu setzen?

Breternitz: Trend Micro fokussiert sich als Technologieanbieter ausschließlich auf das Thema Cyber-Sicherheit. Dabei nehmen wir durch klare Spezialisierung sowie kontinuierliche Forschung und Entwicklung eine Vorreiterrolle ein. Unsere Lösungen werden regelmäßig von Analystenhäusern wie Gartner und Forrester als technologisch führend eingestuft. Unsere globale Reichweite ermöglicht uns darüber hinaus einen umfassenden Überblick über die weltweite Bedrohungslandschaft. Gleichzeitig zeigen wir eine starke lokale Präsenz und haben dadurch die Anforderungen unserer Kunden stets im Blick. Von dieser Kombination profitieren diese.

Teitge: Das Beste aus zwei Welten verbindet auch die Kooperation zwischen Bechtle und Trend Micro, nämlich ei-

nerseits die von Tabea bereits genannte technologische Innovationskraft und weltweite Erfahrung von Trend Micro und andererseits die tiefe Marktkennntnis, Nähe und Integrationskompetenz von Bechtle. Wir kennen die Herausforderungen der Bundesverwaltung aus der täglichen Praxis und bringen die Strukturen mit, um Lösungen schnell, sicher und nachhaltig umzusetzen. Für Behörden heißt das: ein verlässlicher, erfahrener Partner, der nicht nur liefert, sondern auch langfristig begleitet – und das mit einem klaren Fokus auf Sicherheit, Effizienz und Zukunftsfähigkeit.



Thomas Teitge



Tabea Breternitz

Trend Micro – seit seiner Gründung 1988 eines der führenden Unternehmen weltweit im Bereich Cyber-Sicherheit.

Heute schützt der Technologiekonzern den digitalen Informationsfluss in unterschiedlichsten Infrastrukturen – von PCs und Servern über E-Mail-Systeme bis hin zu komplexen Netzwerk- und Cloudumgebungen. Mit Hauptsitz in Tokio und mehr als 7.500 Mitarbeitenden in über 65 Ländern erwirtschaftet Trend Micro einen Jahresumsatz von rund 1,8 Milliarden US-Dollar und zählt damit zu den wichtigsten Akteuren der Branche.

Die japanische Herkunft prägt die Unternehmenskultur bis heute: Präzision, Beständigkeit und eine langfristige Perspektive bestimmen die Herangehensweise an Innovation und Partnerschaften. Neben technologischer Exzellenz legt Trend Micro besonderen Wert auf Integrität, Leidenschaft und gesellschaftliche Verantwortung. Dieses Verständnis reicht weit über die IT-Sicherheit hinaus. Mitarbeitenden engagieren sich weltweit in sozialen Projekten – vom Wiederaufbau nach Naturkatastrophen in Japan bis zum Hausbau auf den Philippinen. Angesichts einer dynamischen Bedrohungslage setzt das Unternehmen verstärkt auf KI-gestützte Sicherheitsstrategien, um Cyber-Angriffe frühzeitig zu erkennen und abzuwehren. Dabei verbindet Trend Micro Ingenieurskunst mit Innovationskraft. Das schafft sowohl bei großen Unternehmen als auch bei zahlreichen Regierungsbehörden weltweit Vertrauen.

Weitere Informationen zum Bechtle Rahmenvertrag über Trend Micro Lösungen finden Sie unter [bechtle.com/bund](https://www.bechtle.com/bund) sowie beim Beschaffungssamt des BMI (BeschA) unter der Vertragsnummer 22049.



Sicherheits-Expert:innen in Bundesbehörden müssen sich breiter aufstellen, um die Zunahme an Bedrohungen aus dem Netz besser beherrschen zu können.

Multi-Cloud als Staatsaufgabe – wie die Verwaltung digitale Souveränität gewinnt.

Ein verschlüsseltes Bürgerportal, ein lahmgelegtes Register oder der Ausfall einer kritischen Datenbank: Solche Szenarien sind längst Realität. Für Behörden bedeutet das nicht nur organisatorische Probleme, sondern im schlimmsten Fall den Verlust staatlicher Handlungsfähigkeit. Bürger:innen erwarten jederzeit verfügbare digitale Services, Unternehmen fordern effiziente Verfahren, neue Technologien wie künstliche Intelligenz (KI) oder Big-Data-Analysen verlangen leistungsfähige Infrastrukturen. Doch viele IT-Landschaften in der Verwaltung sind historisch gewachsen, hochkomplex und nur begrenzt erweiterbar.



Künstliche Intelligenz und Big-Data-Analysen erfordern leistungsfähige IT-Infrastrukturen.

Vor diesem Hintergrund ist „digitale Souveränität“ zu einem Leitmotiv geworden. Sie entscheidet darüber, ob der Staat in Krisen wie im Alltag handlungsfähig bleibt – unabhängig von geopolitischen Risiken oder einzelnen Anbietern. Die Antwort auf diese Herausforderung liegt nicht in monolithischen Eigenbetrieben, sondern in flexiblen Multi-Cloud-Strategien, die Sicherheit, Effizienz und Innovationsfähigkeit miteinander verbinden.

Von Schlagworten zu überprüfbarer Praxis.

In medialen Debatten wurde digitale Souveränität oft auf wenige Schlagworte reduziert: den US CLOUD Act, das europäische Projekt Gaia-X oder völlige technologische Autarkie. Doch vollständige Unabhängigkeit ist in einer globalisierten Digitalwirtschaft kaum realistisch – und häufig auch nicht sinnvoll. Entscheidend ist nicht die Herkunft einer Technologie, sondern, ob Behörden konkrete Kontrollmechanismen durchsetzen können.

Die Schlüsselfragen lauten: Wo liegen die Daten und wie wird ihre Lokation überprüfbar kontrolliert? Wer hat Zugriff und wie wird dieser eingeschränkt und protokolliert? Welche Exit-Strategien existieren, falls ein Anbieter ausfällt oder Verträge enden? Und wie lassen sich regulatorische Vorgaben wie DSGVO oder die NIS2-Richtlinie lückenlos umsetzen? Souveränität entsteht dort, wo diese Fragen nicht theoretisch, sondern praktisch und überprüfbar beantwortet werden können.

Das ITZBund als Multi-Cloud-Manager.

Genau an diesem Punkt setzt das Informationstechnikzentrum Bund (ITZBund) an. Es entwickelt sich vom klassischen Betreiber hin zum Orchestrator einer vielfältigen Cloud-Landschaft. Mit seiner Multi-Cloud-Strategie schafft es eine Plattform, über die Workloads standardisiert und automatisiert in unterschiedlichen Umgebungen betrieben werden können – in der Bundescloud, in Public Clouds oder künftig in neuen europäischen Angeboten.

Das Ziel ist Wahlfreiheit: Der Schutzbedarf einer Anwendung bestimmt das Betriebsmodell. Hochsensible Daten verbleiben in der Bundescloud, dynamische Workloads mit moderatem Schutzbedarf können in die Public Cloud wandern. Mit der AWS European Sovereign Cloud (ESC), die Ende 2025 startet, entsteht eine weitere Option, die auf maximale Autonomie und EU-only Governance setzt.

Damit wird die Cloud-Landschaft des Bundes diverser – und zugleich steuerbarer. Denn das ITZBund definiert Governance-Regeln, etabliert Standards, steuert Zugriffe und sorgt für Automatisierung. So entstehen einheitliche Verfahren, die es erlauben, Sicherheit, Effizienz und Innovation in Einklang zu bringen.

Meilenstein: Der Zuschlag für die Public Cloud.

Ein entscheidender Schritt erfolgte Ende 2024. Nach einem europaweiten Vergabeverfahren erhielt die Bechtle AG gemeinsam mit Amazon Web Ser-

vices (AWS) den Zuschlag für die Bereitstellung von Public-Cloud-Diensten für die Bundesverwaltung. Die Public Cloud ergänzt die Bundescloud um eine hochskalierbare, agile Plattform, die vor allem für Anwendungen mit moderatem Schutzbedarf vorgesehen ist. Dazu zählen etwa Bürgerportale mit stark schwankendem Zugriff, Analyseprojekte mit großen, aber unkritischen Datenmengen oder Pilotvorhaben mit innovativen Technologien. Behörden können die Leistungen standardisiert und ohne eigene Ausschreibungen abrufen – eingebettet in ein Governance-Modell, das Sicherheit, Nachvollziehbarkeit und Kontrolle gewährleistet.

Das Besondere: Projekte lassen sich dadurch schneller umsetzen, Ressourcen werden geschont, die Verwaltung gewinnt an Flexibilität und gleichzeitig bleibt die Wahlfreiheit gewahrt.

Architekturprinzipien der Souveränität.

Die Multi-Cloud-Strategie basiert auf drei zentralen Prinzipien: **Kontrolle:** Datenlokation, Schlüsselverwaltung und Zugriffsrechte müssen überprüfbar in der Hand der Verwaltung liegen. Kryptografische Verfahren, Audit-Logs und Rollenmodelle sorgen für Nachvollziehbarkeit. **Wahlfreiheit:** Abgestuft nach Schutzbedarf können Workloads in der Bundescloud, in der Public Cloud oder künftig in der ESC betrieben werden. So lassen sich Sicherheit, Effizienz und Innovationsgeschwindigkeit ausbalancieren. **Portabilität:** Containerisierung, offene Schnittstellen und getestete Exit-Szenarien verhindern

Lock-in-Effekte. Nur wenn Behörden die Fähigkeit zum Wechsel behalten, bleiben sie unabhängig – auch in geopolitischen oder technischen Krisen. Diese Prinzipien zeigen: Souveränität ist kein Zustand, sondern ein kontinuierlicher Prozess. Sie muss täglich überprüft, abgesichert und weiterentwickelt werden.

AWS European Sovereign Cloud: Die nächste Stufe.

Bereits 2025 startet die AWS European Sovereign Cloud (ESC). Sie bringt die nächste Stufe digitaler Souveränität: den vollständigen Betrieb innerhalb der EU, EU-basierte Sicherheitsteams, eigene Governance-Strukturen und eine dedizierte Vertrauenskette. Infrastruktur, Schlüsselverwaltung und Support liegen ausschließlich in europäischen Händen.

Das Besondere: Die ESC bietet einen zum Start sehr umfangreichen Servicekatalog, dieselben APIs und dieselbe Performance wie klassische AWS-Regionen. Migrationen bleiben einfach, Funktionsverluste entstehen nicht. Behörden gewinnen damit ein echtes Wahlrecht: heute Workloads in bestehenden Regionen, morgen souverän in der ESC – ohne auf Funktionalität oder Skalierbarkeit verzichten zu müssen. Nach dem Launch der ESC werden weitere Services folgen mit dem Ziel, in naher Zukunft einen so umfangreichen Serviceumfang anzubieten, der der regulären AWS Region in Frankfurt in nichts nachsteht.

Bechtle als Brücke zwischen Hyperscaler und Staat.

Mit dem Zuschlag für die Public Cloud übernimmt Bechtle eine Schlüsselrolle. Als Integrator sorgt das Unternehmen mit Hauptsitz in Neckarsulm bei Stuttgart dafür, dass globale Cloud Services so eingebunden werden, dass sie den Anforderungen der Bundesverwaltung entsprechen – von Architektur und Automatisierung über Kryptografie bis hin zu Auditierbarkeit. Bechtle fungiert damit als Brücke zwischen Hyperscaler und Verwaltung. Die Aufgabe besteht nicht allein darin, Technologie bereitzustellen, sondern sie in souveräne Strukturen zu überführen. Erst dadurch wird gewährleistet, dass die Vorteile der Public Cloud bestmöglich genutzt werden können, ohne Ri-

siken bei Sicherheit oder Compliance einzugehen.

Chancen und Herausforderungen.

Die Multi-Cloud-Strategie eröffnet der Verwaltung erhebliche Chancen. Projekte können schneller umgesetzt werden, da Cloud-Dienste on demand bereitstehen. Skalierbarkeit ermöglicht es, kurzfristige Bedarfsspitzen – etwa bei Wahlen oder Krisen – flexibel abzudecken. Gleichzeitig erhöht die Vielfalt der Modelle die Resilienz, weil Abhängigkeiten von einzelnen Anbietern reduziert werden.

Doch es gibt auch Herausforderungen. Migrationen von Altverfahren sind komplex und Fachkräfte sind knapp. Governance und Compliance müssen konsequent eingehalten werden, um die Vorteile nicht durch neue Risiken zu gefährden. Multi-Cloud ist daher kein Selbstläufer, sondern eine Daueraufgabe, die klare Regeln, kontinuierliches Monitoring und regelmäßige Tests von Exit-Szenarien erfordert.

Vielfalt ist Stärke.

Die digitale Souveränität des Staates entscheidet darüber, wie handlungsfähig er im 21. Jahrhundert bleibt. Sie ist kein abstraktes Schlagwort, sondern eine Praxis, die täglich erarbeitet werden muss. Mit der Multi-Cloud-Strategie legt das ITZBund den Grundstein für diese Handlungsfähigkeit.

Die Kombination aus Bundescloud, Public Cloud und AWS European Sovereign Cloud macht deutlich: Die Verwaltungs-IT der Zukunft ist nicht monolithisch, sondern vielfältig. Souveränität entsteht durch Wahlfreiheit, technische Kontrolle und Portabilität. So wird digitale Souveränität von der politischen Vision zur gelebten Praxis – und die Verwaltung gewinnt den Handlungsspielraum, den sie in einer zunehmend digitalisierten Welt braucht. Multi-Cloud ist daher keine technische Mode, sondern eine Daueraufgabe, die kontinuierliches Monitoring, klare Regeln und getestete Exit-Szenarien verlangt. Nur so bleibt der Staat unabhängig und handlungsfähig – heute wie morgen.

Sicherheit und Governance stehen beim Public-Cloud-Vertrag im Vordergrund.

Der Public-Cloud-Vertrag sieht klare Vorgaben vor – von Datenlokation und Verschlüsselung über Zugriffskontrollen bis hin zu lückenloser Auditierbarkeit. Zugleich ist festgelegt, dass nur Anwendungen mit moderatem Schutzbedarf in die Public Cloud ausgelagert werden dürfen. Für besonders sensible Daten bleiben weiterhin die Bundescloud oder künftige souveräne Angebote wie die ESC reserviert. Damit entsteht eine abgestufte Architektur: maximale Sicherheit für kritische Systeme, Flexibilität für dynamische Workloads. Governance-Regeln, die zentral über den Multi-Cloud-Manager des ITZBund durchgesetzt werden, stellen sicher, dass trotz der Vielfalt keine unkontrollierte Schatten-IT entsteht.



Von der AWS European Sovereign Cloud profitieren auch Bürgerinnen und Bürger im Alltag.

Weitere Informationen zum Bechtle Rahmenvertrag über AWS Lösungen finden Sie unter bechtle.com/bund sowie beim Beschaffungsamt des BMI (BeschA) unter der Vertragsnummer 53435.



Die Dimension dieser Vorfälle macht deutlich: Resilienz ist keine abstrakte Zukunftsfrage, sondern eine akute Herausforderung. Bürgerinnen und Bürger erwarten, dass digitale Services jederzeit zuverlässig funktionieren. Verwaltung bedeutet heute, Daten und Prozesse sicher, nachvollziehbar und dauerhaft verfügbar zu halten. Ein Ausfall führt nicht nur zu organisatorischen Problemen, sondern auch zu einem Vertrauensverlust in die Handlungsfähigkeit des Staates.

Komplexe Ausgangslage.

Die zentrale Herausforderung liegt in der Struktur vieler IT-Landschaften. Über Jahrzehnte sind Infrastruktur und Fachverfahren gewachsen, oft individuell entwickelt und selten durchgängig standardisiert. Schnittstellen fehlen, Systeme sind voneinander isoliert, Wartungsaufwand und Betriebskosten steigen.

Gleichzeitig wächst die Erwartungshaltung: digitale Akten, Bürgerportale, Registermodernisierung, Cloud-Services und neue Technologien wie künstliche Intelligenz sollen integriert und nutzbar sein. So treffen steigende Ansprüche auf eine heterogene und anfällige IT-Basis.

Diese Diskrepanz erhöht die Risiken: Je komplexer die Landschaft, desto schwieriger wird das einheitliche Management, desto größer die Gefahr von Sicherheitslücken – und desto langsamer gelingt die Wiederherstellung nach Ausfällen.

Unzureichende Schutzmaßnahmen.

Mehrere Untersuchungen unterstreichen die Dringlichkeit. Der Global Data Protection Index 2024 von Dell Technologies zeigt, dass drei von vier befragten Organisationen ihre bestehenden Schutzmaßnahmen für unzureichend halten, um einem Ransomware-Angriff standzuhalten. Zwei Drittel äußerten Zweifel, ob sie ihre Daten im Ernstfall vollständig und zeitnah wiederherstellen könnten. Mehr als die Hälfte aller Organisationen verzeichnete im vergangenen Jahr mindestens einen sicherheitsrelevanten Vorfall mit Datenverlust, bei durchschnittlichen Schäden von fast zwei Millionen US-Dollar.

Digitale Resilienz und Datenschutz.

Warum Widerstandsfähigkeit für Behörden jetzt unverzichtbar wird.

Jede Verwaltung, ob Kommune, Land oder Bund, ist heute auf stabile digitale Infrastrukturen angewiesen. Fallen diese aus, steht nicht nur der Arbeitsalltag still, sondern im schlimmsten Fall funktionieren auch elementare staatliche Leistungen nicht mehr. Ransomware-Angriffe, Datenverluste oder technische Defekte haben in den vergangenen Jahren mehrfach gezeigt, wie verletzlich Behörden tatsächlich sind. Der Betrieb musste teilweise auf Papierakten umgestellt werden, Auszahlungen von Sozialleistungen verzögerten sich, ganze Register waren tagelang nicht erreichbar.



Bürger:innen profitieren vielfältig von resilienten IT-Infrastrukturen.

Für Behörden bedeutet das: Ein schwerwiegender Vorfall ist keine theoretische Möglichkeit, sondern eine konkrete Gefahr. Die Folgen reichen von organisatorischen Störungen bis hin zu politischen Krisen, wenn elementare Verwaltungsleistungen nicht mehr erbracht werden können.

Von Prävention zu Resilienz.

Die klassische IT-Sicherheit konzentrierte sich lange auf Prävention: Firewalls, Virenschutz, Monitoring. Diese Instrumente bleiben unverzichtbar, reichen aber allein nicht mehr aus.

Fachleute sind sich einig: Die entscheidende Frage lautet nicht, ob ein Angriff oder Ausfall geschieht, sondern wann.

Resilienz erweitert daher den Blick. Gemeint ist die Fähigkeit, nach einer Störung schnell und kontrolliert wieder arbeitsfähig zu werden. Dazu gehört, Daten zuverlässig zu sichern, Wiederanlaufprozesse zu testen und Systeme so zu gestalten, dass sie im Ernstfall zügig verfügbar sind. Die Verwaltung muss lernen, digitale Krisen so zu bewältigen wie analoge – mit klaren Abläufen, Zuständigkeiten und Strukturen.

Technische und organisatorische Bausteine.

Mehrere Ansätze gelten heute als Schlüsselfaktoren für Resilienz. Dazu zählen isolierte Datenspeicher, die auch bei erfolgreichen Angriffen unangetastet bleiben, unveränderbare Backups, die nicht überschrieben oder gelöscht werden können, sowie Technologien zur Reduktion von Datenvolumen, die eine schnelle Wiederherstellung großer Datenmengen ermöglichen. Ebenso relevant sind standardisierte Wiederanlaufpläne, die regelmäßig erprobt werden, sowie die

Nutzung von Multi-Cloud-Umgebungen, die Daten flexibel und gleichzeitig rechtskonform absichern.

Doch Technik allein genügt nicht. Behörden müssen Resilienz organisatorisch verankern: durch eine klare Priorisierung kritischer Systeme, durch definierte Zuständigkeiten im Ernstfall und durch regelmäßige Recovery-Übungen. Immer mehr Verwaltungen führen Testszenarien durch, in denen Systeme gezielt herunter- und wieder hochgefahren werden. Solche Übungen zeigen, wie realistisch Wiederherstellungspläne sind und ob die Kommunikation zwischen IT, Fachabteilungen und Leitungsebene funktioniert.

Blick nach vorn: Datenmengen und Künstliche Intelligenz.

Die Herausforderungen werden nicht kleiner. Elektronische Akten, Registermodernisierung, Geodaten oder Sensordaten erzeugen jedes Jahr Terabytes neuer Informationen. Hinzu kommen KI-Anwendungen, die Fachverfahren beschleunigen oder Prognosen verbessern sollen, aber stabile, sichere und hochverfügbare Infrastrukturen voraussetzen.

Resilienz bedeutet daher auch, mit diesen wachsenden Datenmengen und Technologien umgehen zu können. Moderne Backup- und Recovery-Systeme müssen skalierbar, flexibel und sicher zugleich sein. Nur so lassen sich zukünftige Anforderungen erfüllen, ohne die Handlungsfähigkeit der Verwaltung zu gefährden.

Digitale Resilienz.

Digitale Resilienz ist mehr als ein Schlagwort. Sie entscheidet darüber, ob Behörden nach einem Vorfall tagelang gelähmt oder binnen Stunden wieder handlungsfähig sind. Sie ergänzt die klassische IT-Sicherheit um die Fähigkeit zur Wiederherstellung und macht damit den Unterschied zwischen einem kontrollierten Krisenmanagement und einem Kontrollverlust.

Für Behörden und die öffentliche Verwaltung gilt: Resilienz ist keine Zusatzoption. Sie ist Teil der Grundversorgung in Deutschland und damit Grundlage für das Vertrauen der Bürgerinnen und Bürger in einen handlungsfähigen Staat.

Digitale Resilienz in der Praxis: Lösungen von Dell Technologies für eine widerstandsfähige Verwaltung.

Viele Behörden kämpfen mit einer unübersichtlichen Systemlandschaft, die den Betrieb verkompliziert und Sicherheitslücken begünstigt. Unterschiedliche Fachverfahren, gewachsene Infrastrukturen und fehlende Schnittstellen erhöhen die Komplexität und damit die Anfälligkeit. Hinzu kommt eine weitere, stetig wachsende Herausforderung: die schiere Menge an Daten. Registermodernisierung, elektronische Akten, Geoinformationssysteme oder Sensordaten erzeugen jeden Tag neue Informationsbestände, die gespeichert, gesichert und im Ernstfall schnell wiederhergestellt werden müssen.

Für Verwaltungen bedeutet das: Speicherinfrastrukturen stoßen schneller an ihre Grenzen, Wiederanlaufzeiten verlängern sich und die Kosten steigen.

Ein zentrales Management für alle Daten- und Anwendungsschutzmaßnahmen vor Ort, in der Cloud oder an dezentralen Standorten schafft hier Abhilfe. Dell Technologies bietet dafür maßgeschneiderte Hard- und Softwarelösungen, die den gesamten Datenlebenszyklus abbilden, Richtlinien einheitlich umsetzen, Prozesse automatisieren und Verantwortlichkeiten klar zuordnen.

Datenspeicherung und Datenmengen.

Das Fundament für eine robuste Datenspeicherung entsteht durch leistungsstarke Server- und Backup-Architekturen. Besonders relevant ist dabei die Frage, wie wachsende Datenmengen effizient verwaltet werden können. Mit der Data-Domain-Technologie setzt Dell Technologies auf intelligente Deduplizierung, die redundante Informationen automatisch erkennt und zusammenfasst. Das reduziert den Speicherbedarf erheblich – um bis zu 65:1 – und ermöglicht es Behörden, Millionen von Dokumenten wirtschaftlich zu archivieren. Gleichzeitig beschleunigt die Technologie die Wiederherstellung, weil nur die tatsächlich relevanten Daten zurückgespielt werden müssen.

Für Szenarien, in denen es auf höchste Geschwindigkeit ankommt, etwa bei Bürgerportalen oder im Katastrophenschutz, kommen All-Flash-Technologien zum Einsatz. Sie verkürzen Sicherungs- und Wiederanlaufzeiten erheblich und stellen sicher, dass kritische Systeme auch nach Störungen schnell wieder verfügbar sind.

Cyber Recovery Vaults.

Neben der Bewältigung großer Datenmengen bleibt der Schutz vor Ransomware zentral. Cyber Recovery Vaults halten eine physisch und logisch vom

Produktionsnetz getrennte, unangreifbare Datenkopie vor. Selbst wenn Angreifende zentrale Systeme kompromittieren, bleibt diese Kopie unberührt und ermöglicht die Wiederherstellung kritischer Fachverfahren innerhalb weniger Tage statt mehrerer Wochen. Ergänzend sichern unveränderbare Backups die Integrität sensibler Daten, weil sie sich weder löschen noch überschreiben lassen. Automatisierte Wiederherstellungsprozesse sorgen dafür, dass definierte Abläufe im Ernstfall ohne Verzögerung greifen und Ausfallzeiten nachweislich deutlich sinken.

Dell PowerEdge-Plattform und Künstliche Intelligenz.

Mit Blick auf neue Verwaltungsaufgaben wachsen gleichzeitig die Anforderungen an Rechenleistung und Datenschutz. Anwendungen der künstlichen Intelligenz in Fachverfahren erfordern schnelle und sichere Zugriffe auf große Datenmengen. Für diese Szenarien stellt Dell mit seinen PowerEdge-XE9680-Servern eine Plattform bereit, die auf hohe GPU-Dichten und schnelle PCIe-Gen-5-Anbindungen ausgelegt ist. Damit lassen sich komplexe Modelle effizient trainieren und in Echtzeit einsetzen – in Umgebungen, die den strengen Anforderungen an Datensicherheit und Compliance gerecht werden. Parallel beschleunigt KI-gestützte Anomalieerkennung die Früherkennung ungewöhnlicher Muster und trägt dazu bei, Bedrohungen zu stoppen, bevor sie kritische Ausmaße erreichen.

Multi-Cloud und Datenhoheit.

Da Daten zunehmend über verschiedene Clouds und Rechenzentren verteilt sind, benötigen Verwaltungen Transparenz und Kontrolle. Die Multi-Cloud-Datenschutzlösungen von Dell Technologies konsolidieren Datenbestände über Public, Private und Hybrid Clouds hinweg und bieten zentrale Steuerungs- und Auditfunktionen. So wird Schatten-IT vermieden, regulatorische Vorgaben wie DSGVO oder NIS2

werden eingehalten und gleichzeitig bleibt die Flexibilität erhalten, die jeweils passende Plattform für den Anwendungsfall zu wählen.

Langfristige Lebenszyklen.

IT-Investitionen der öffentlichen Hand müssen über Jahre Bestand haben. Dell Technologies setzt deshalb auf langfristige Service- und Update-Programme, die Systeme über ihren gesamten Lebenszyklus hinweg technisch aktuell und sicherheitskonform halten.

Mehr als 2.600 Organisationen weltweit – darunter zahlreiche öffentliche Einrichtungen – nutzen diese Ansätze bereits. Sie zeigen, dass digitale Resilienz kein theoretisches Ziel ist, sondern mit effizienten Speichertechnologien, zentralem Management und erprobten Prozessen verlässlich erreicht werden kann.



Anforderungen an Behörden und die öffentliche Verwaltung werden immer komplexer und vielfältiger.

Weitere Informationen zu den Bechtle Rahmenverträgen über Dell Technologies Lösungen finden Sie unter [bechtle.com/bund](https://www.bechtle.com/bund) sowie beim Beschaffungsamt des BMI (BeschA) unter den Vertragsnummern 22224, 22225 und 22226.

Wie souveräne KI und KI-Governance die Demokratie stärken.

Unsere Demokratie steht in diesen Zeiten sowohl von innen als auch von außen unter erheblichem Druck. Vertrauen in staatliche Institutionen und demokratische Prozesse kann dort wachsen, wo demokratische Prinzipien mit effizientem und transparentem Regierungshandeln verknüpft werden. Der technologische Fortschritt – insbesondere im Bereich der generativen künstlichen Intelligenz (KI) – eröffnet neue Möglichkeiten, um komplexe Herausforderungen wie den Fachkräftemangel zu adressieren. Gleichzeitig erfordert der verantwortungsvolle Einsatz von KI eine klare Regulierung und eine wertebasierte Governance, um Missbrauch zu verhindern und demokratische Grundwerte zu schützen. So kann die Nutzung von KI mit voller Datensouveränität gelingen, ohne einen „Lock-in“ oder die eigene Datenhoheit zu riskieren.

Was das genau für Behörden und die öffentliche Verwaltung bedeutet, darüber haben wir mit Dr. Lisa Precht von IBM gesprochen.

Geopolitische Konflikte, Fachkräftemangel, Bürokratiekrise. Welche Rolle spielt KI, um diese Herausforderungen im öffentlichen Sektor zu bewältigen?

Dr. Precht: Deutschland braucht Effizienz in der öffentlichen Verwaltung, denn Vertrauen entsteht dort, wo demokratische Prinzipien auf wirksames Regierungshandeln treffen. Souveräne künstliche Intelligenz (KI) kann dabei eine Schlüsselrolle spielen. Richtig eingesetzt macht sie staatliches Handeln effizienter, transparenter und widerstandsfähiger – vorausgesetzt, ihre Einführung erfolgt nachvollziehbar, kontrollierbar und mit dem Ziel, menschliche Intelligenz zu ergänzen, nicht zu ersetzen. Studien und Praxisprojekte zeigen bereits das große Potenzial von KI im öffentlichen Sektor. Sie bescheinigen dem KI-Einsatz nicht nur Zeitersparnis mit über 25 Prozent schnelleren Bearbeitungszeiten und 12 Prozent höherer Produktivität, sondern auch eine um 40 Prozent gesteigerte Qualität erledigter Aufgaben.

IBM hat bereits eindruckliche Praxisbeispiele in diesem Zusammenhang umgesetzt, von Sozialhilfe über Gerichte bis zur Bundeswehr. Was war aus Ihrer Sicht der „Game Changer“, der diese Projekte erfolgreich gemacht hat?

Dr. Precht: Drei entscheidende Faktoren tragen aus unserer Sicht wesentlich zu erfolgreichen Projekten bei. Erstens war es entscheidend, sich auf

konkrete, werthaltige Use Cases zu konzentrieren. Indem wir uns auf spezifische Anwendungsfälle fokussierten, konnten wir einzelne Mitarbeitende von lästigen, zeitraubenden Tätigkeiten entlasten. Diese Fokussierung ermöglichte es uns, den Mehrwert des Einsatzes von KI direkt mess- und erfahrbar zu machen. Zweitens war die frühzeitige Einbindung der zukünftigen Nutzer:innen in den Entwurfsprozess von zentraler Bedeutung. Durch ihre Beteiligung konnten wir sicherstellen, dass die entwickelten Lösungen praxisrelevant und benutzerfreundlich sind. Dieser Ansatz half uns, die tatsächlichen Bedürfnisse der Anwender:innen zu verstehen und Lösungen zu entwickeln, die genau auf diese Bedürfnisse zugeschnitten sind. Drittens haben wir uns konsequent an das Vorgehensmodell ‚Ethics by Design‘ gehalten. Dieser Ansatz stellt sicher, dass ethische Überlegungen von Beginn an in den Entwicklungsprozess integriert werden. Durch die Berücksichtigung ethischer Aspekte konnten wir Lösungen entwickeln, die nicht nur effizient, sondern auch transparent sind und damit verantwortungsbewusst eingesetzt werden können.

Im Zusammenhang mit souveräner KI-Nutzung spricht IBM auch über „Agentic AI“, also KI, die eigenständig handelt. Wie lässt sich das mit dem Bedürfnis nach Kontrolle und Nachvollziehbarkeit im Staat vereinbaren?

Dr. Precht: In den letzten Jahren hat KI eine tief greifende Transformation durchlaufen – von starren, vordefinierten Abläufen hin zu hochflexiblen, autonomen KI-Agenten. Regelbasierte

KI, wie klassische KI-Assistenten, automatisiert Aufgaben dann, wenn die einzelnen Schritte dafür zuvor definiert wurden. Das bietet maximale Kontrolle, erfordert aber auch einen hohen Aufwand. Hybride Ansätze, die regelbasierte KI mit generativer KI kombinieren – etwa KI-Assistenten, die Large Language Models (LLMs) nutzen –, ermöglichen eine bessere Skalierbarkeit. Ich gebe hier den Rahmen vor, kann aber gleichzeitig die Vorteile generativer KI nutzen.

Solche Systeme profitieren von optimierter Spracherkennung, flexiblen Dialogen und können Inhalte wie Antworten oder E-Mails dynamisch generieren.

KI-Agenten gehen noch einen Schritt weiter: Sie nutzen LLMs, um selbst zu entscheiden, wie sie ein Ziel erreichen. Ich definiere das Ziel, die KI-Agenten planen und führen die Aufgaben eigenständig aus. Wichtig ist: KI-Agenten unterscheiden sich von hybriden Lösungen – die regelbasierte und generative KI kombinieren – nicht unbedingt in den Ergebnissen, wohl aber grundlegend in ihrem Vorgehen. IBM ermöglicht es, regelbasierte und autonome Technologie in KI-Lösungen zu kombinieren, um von den Stärken beider Ansätze zu profitieren. So behalten Sie maximale Kontrolle, wo notwendig, und profitieren gleichzeitig von den Vorteilen autonomer KI-Agenten. Generative KI setzen wir dabei grundsätzlich in Verbindung mit unserer Governance-Lösung [watsonx.governance](#) ein. Diese ermöglicht es, die Qualität aller eingesetzten KI-Lösungen durch Echtzeitanalysen zu überwachen und Transparenz zu gewährleisten.

Wenn Sie den öffentlichen Sektor heute beraten müssten: Welche drei konkrete Schritte sollten Behörden jetzt gehen, um KI sicher, wirksam und rechtssicher zu etablieren – ohne von Hype oder Unsicherheit ausgebremst zu werden?

Dr. Precht: Für Regierungen und Unternehmen ist es am wichtigsten, Auswahlmöglichkeiten, Kontrolle und Vertrauen in die von ihnen eingesetzten kritischen Technologien zu haben. Für IBM ergibt sich technologische Autonomie aus konkreten Maßnahmen zur Erfüllung dieser Anforderungen wie z. B. 1) Datenhoheit, 2) KI-Lebenszyklus-Governance, 3) Interoperabilität und 4) Offenheit.

Für eine sichere und wirksame Etablierung von KI in öffentlichen Verwaltungen führt der Weg über drei entscheidende Etappen: Der erste Schritt muss ein gemeinsamer Analyseprozess sein. Behörden sollten mit ihren Mitarbeitenden konkret ermitteln, welche Prozesse Optimierungspotenzial bieten und welche Schmerzpunkte durch KI-Unterstützung beseitigt werden können.

Im zweiten Schritt gilt es, eine zukunftssichere technologische Grundlage für KI-Anwendungen zu schaffen. Fragmentierte Insellösungen verursachen langfristig Integrationsprobleme. Im Gegensatz dazu bietet eine offene und flexible KI-Plattform, analog zu einem Werkzeugkasten, die Möglichkeit, fortlaufend beliebige KI-Anwendungen umzusetzen und Open-Source- oder Drittanbieter-Lösungen zu integrieren. Verfügen Behörden oder die öffentliche Verwaltung nur über wenige KI-Expert:innen, empfiehlt sich eine Plattform, die den Einsatz von KI-Lösun-

gen auch ohne Programmieraufwand ermöglicht.

Der dritte Aspekt betrifft die strategische Infrastrukturentscheidung. Behörden sollten sorgfältig abwägen, wie sie ihre KI-Lösungen betreiben wollen. Eine containerbasierte Plattform bietet hier die nötige Flexibilität, um Betriebsmodelle später anzupassen, ohne sich an eine bestimmte Infrastruktur oder einen Anbieter zu binden. So bleibt die Souveränität über sensible Daten gewahrt, während gleichzeitig schrittweise Pilotprojekte mit messbarem Mehrwert umgesetzt werden können.

IMPRESSUM
Herausgeber Bechtle GmbH & Co. KG IT-Systemhaus Bonn, Pennfeldsweg 10, 53177 Bonn, Tel. +49 228 6888-0, E-Mail bonn@bechtle.com **Redaktion** Bechtle Logistik & Service GmbH und Bechtle GmbH & Co. KG IT-Systemhaus Bonn **Verantwortlich** Waldemar Zgrzebski, Geschäftsführer **Layout** Bechtle IT-Systemhaus Rheinland **Fotonachweis** Seite 1: Adobe Stock I [vegefox.com](#), Seite 2: Adobe Stock I [nmann77](#), Adobe Stock I [WavebreakMediaMicro](#), Adobe Stock I [insta_photos](#), Seite 3: Bechtle, Seite 4: DBT/Simone M. Neumann, mit ChatGPT überarbeitet, AV Software Solutions 360°, Adobe Stock I [HockleyMedia24/peopleimages.com](#), Seite 5: Adobe Stock I [Malambo C/peopleimages.com](#), Trend Micro, Bechtle, Seite 6: Adobe Stock I [peopleimages.com](#), Adobe Stock I [KM](#), Seite 7: Adobe Stock I [Deemerwha studio](#), Adobe Stock I [Aevan](#), Seite 9: IBM, Adobe Stock I [imagevision](#)

**bechtle**

Danke!

Für 20 Jahre #zukunftsstark.

Das Bechtle Systemhaus Bonn bedankt sich bei allen Kunden, Partnern und Mitarbeitenden für 20 Jahre Zusammenarbeit, Partnerschaft und Vertrauen. Wir freuen uns darauf, auch in den kommenden Jahren mit Ihnen die digitale Transformation zu gestalten und gemeinsam weiterzuwachsen.

#zukunftsstark verbunden: aus Bonn - für die Region und die öffentliche Verwaltung

Waldemar Zgrzebski
Geschäftsführer

Christian Behma
Geschäftsführer

Thomas Teitge
Mitglied der Geschäftsleitung
Geschäftsbereichsleiter Bundesbehörden

bechtle.com/bonn



IT-Automatisierung in der öffentlichen Verwaltung.

In den vergangenen Monaten zeichnet sich ein klarer Trend in der IT-Landschaft ab: Der Bedarf an Digitalisierung nimmt rasant zu, gleichzeitig wächst die Komplexität der IT-Systeme stetig. Cyber-Angriffe gehören mittlerweile zum Alltag und auch der demografische Wandel sowie der zunehmende Wettbewerb um IT-Fachkräfte stellen die Leistungsfähigkeit der öffentlichen IT vor große Herausforderungen. Wie kann die IT unter diesen Bedingungen ihren Beitrag zur Digitalisierung und zur Erfüllung öffentlicher Aufgaben zukunftssicher gestalten?



Mit Automatisierungen sind Einsparungen in puncto Zeit und Ressourcen möglich.

Die öffentliche Verwaltung steht vor einem tief greifenden Wandel. Themen wie Entbürokratisierung, Planungsbeschleunigung und die Sicherstellung der Handlungsfähigkeit in Krisenzeiten müssen jetzt angegangen werden und nicht erst morgen. Digitalisierung ist dabei ein kritischer Erfolgsfaktor. Die fortschreitende Modernisierung der Verfahrenslandschaft und die zunehmende Verbreitung von Cloud-Technologien sowie hybriden IT-Landschaften bilden das technologische Fundament für die digitale Transformation im öffentlichen Sektor. Gleichzeitig steigt die Nachfrage nach künstlicher Intelligenz rapide an – ein Trend, der nicht zuletzt

durch die demografische Entwicklung und den daraus resultierenden Fachkräftemangel weiter verstärkt wird. „In der Industrie steht das Thema IT-Automatisierung längst ganz oben auf der Agenda“, betont Florian Breger, Vice President für öffentliche Auftraggeber bei IBM Deutschland. Laut einer IBM Studie planen 92 Prozent der Führungskräfte, KI-gestützte Automatisierung gezielt entlang ihren Geschäfts- und IT-Prozessen einzusetzen, mit dem klaren Ziel, der zunehmenden Komplexität der IT erfolgreich zu begegnen. Diese Entwicklung ist dringend notwendig, denn 82 Prozent der Geschäftsführer geben an, dass manuelle und reaktive Tätigkeiten in der IT-Deli-

very den Unternehmenserfolg spürbar hemmen. Gleichzeitig steigt der Druck weiter – laut IDC wird die Zahl der Anwendungen in Unternehmen bis 2028 auf durchschnittlich 1.000 anwachsen.

Ohne Automatisierung der IT keine Digitalisierung.

Digitalisierung ist ohne Automatisierung in der Bereitstellung von IT nicht möglich. Auch die öffentliche IT sollte daher den Einsatz von KI und Automatisierungstechnologien im IT-Betrieb zu ihrem Vorteil nutzen, um nicht der Engpass für den Fortschritt der Digitalisierung der öffentlichen Verwaltung zu werden. Aus Sicht von Florian Breger gibt es zwei

wichtige Ansatzpunkte, die einen zukunftsfähigen IT-Betrieb in der öffentlichen Verwaltung ermöglichen:

Vorhandene IT-Kapazitäten besser nutzen.

Ein erster vielversprechender Ansatz besteht darin, vorhandene IT-Kapazitäten gezielter zu analysieren, zu überwachen und effizienter zu nutzen, ohne dabei die Performance oder Stabilität zu gefährden. Dazu wird die gesamte Anwendungslandschaft mithilfe umfassender Monitoring-Lösungen in Echtzeit über die gesamte IT-Infrastruktur hinweg beobachtet. Ergänzend kommen KI-gestützte Automatisierungsfunktionen zum Einsatz.

Damit lassen sich Erkennung, Überwachung, Fehlerbehebung und Berichterstattung zu Anwendungen und Diensten deutlich effizienter und weitgehend automatisiert abwickeln. Aufwendige manuelle Fehlersuchen entfallen. Systeme können beispielsweise Probleme frühzeitig selbst identifizieren, automatisiert Handlungsempfehlungen geben oder sogar eigenständig Maßnahmen einleiten und so die Leistungsfähigkeit und Effizienz der IT-Umgebung nachhaltig verbessern.

Reduzierung von einfachen, repetitiven Aufgaben über Bereichsgrenzen hinweg.

Laut einer Studie des WEF (World Economy Forum) hat generative KI massive Auswirkungen in Industrien, in denen Informationen, Texte und Sprache eine große Rolle spielen. So gelten bis zu 73 Prozent der Tätigkeiten in der IT-Branche als „Language Tasks“ und können mithilfe von KI vollständig automatisiert oder durch KI-Agenten unterstützt werden. Nehmen wir das Beispiel einer intelligenten Automatisierung des Patch-Managements und die Orchestrierung sicherheitsrelevanter Aktivitäten. Software-Patching bezeichnet das Einspielen von Updates, um kritische Sicherheitslücken und Fehler zu beheben oder Funktionen zu ergänzen. Zum Beispiel verkürzte sich durch Automatisierung dieser Prozess im Application Lifecycle Management von etwa 90 auf nur 20 Minuten pro Applikation bei einem großen deutschen IT-Dienstleister, so Florian Breger. Die enorme Zeitersparnis verschafft IT-Teams neue Freiräume.

Dies zeigt: Jeder Schritt mehr in Richtung Digitalisierung des Verwaltungshandelns erfordert einen Schritt mehr in die Automatisierung der IT-Bereitstellung durch die öffentliche IT. Jede IT hat ihre Optimierungsbereiche, an denen man mit Automatisierung und KI sinnvoll ansetzen kann. Gelingt dies, wird die öffentliche IT zum Motor der Digitalisierung.

Wenn die IT nicht mehr rund läuft – Fehlersuche durch alle Instanzen.

Moderne IT-Umgebungen sind zunehmend komplex und schwer überschaubar. Die Verlagerung in Multi-Cloud-Architekturen, der Einsatz von Micro Services, Containern und Kubernetes-Orchestrierungsplattformen sowie das rapide Datenwachstum treiben diese Entwicklung voran. Für IT-Abteilungen wird es dadurch immer schwieriger, den Überblick zu behalten, insbesondere ohne den Einsatz unterstützender Tools und intelligenter Automatisierung. Kommt es dann noch zu Störungen oder Ausfällen, ist das Risiko groß, dass schnell Unordnung oder gar Stillstand entsteht.

Maximale Transparenz gilt in der IT schon seit Langem als zentraler Meilenstein auf dem Weg der digitalen Transformation. Zu wissen, was funktioniert und was nicht, ist entscheidend. Doch angesichts der Vielzahl an Anwendungen und Systemen, die heute bereits in der öffentlichen Verwaltung im Einsatz sind, ist diese Transparenz schwer zu erreichen. Und die Komplexität nimmt weiter zu. Doch was passiert, wenn plötzlich ein Fehler auftritt? Wenn die IT-Performance nicht den Erwartungen entspricht? Ohne vollständige Transparenz wird die Ursachenanalyse schnell zeit- und ressourcenintensiv.

eAkte – mit hohen Anforderungen an die Performance.

Die elektronische Akte (eAkte) ist deutschlandweit in der Justiz ab 2026 flächendeckend eine der zentralen IT-Anwendungen im Gerichtsalltag. Am

Anfang war die Euphorie groß. Schnellere Prozessabläufe durch übersichtlichere, schnell durchsuchbare digitale Prozessakten statt dicker Papierstapel – das versprach die Einführung der eAkte. Doch Systemausfälle und wiederkehrende Performance-Probleme erschwerten immer wieder die Arbeiten mit der eAkte. Das Problem: Die eingesetzte IT-Umgebung ist sehr komplex, mit heterogenen Serverlandschaften, teilweise container- oder cloudbasiert. Die eAkte wurde in vielen unterschiedlichen Bereichen der Justiz eingeführt wie beispielsweise für die ordentliche Gerichtsbarkeit, die Fachgerichte oder für die Staatsanwaltschaften. Für alle diese Bereiche ist die eAkte organisationskritisch und ihr Funktionieren daher ein Muss.

In einer zunehmend komplexen Systemlandschaft mit zahlreichen Instanzen und Architekturschichten gestaltet

sich die klassische Fehleranalyse äußerst zeitintensiv.

Viele der eingesetzten Analyse- und Monitoring-Tools decken lediglich Teilbereiche ab, da sie meist auf spezifische (Hintergrund-)Systeme ausgelegt sind. Performance-Probleme können jedoch an ganz unterschiedlichen Stellen entstehen – sei es auf der Anwendungsebene oder in einem der zahlreichen Backend-Systeme.

Benötigt wird eine IT-Lösung, die über die Möglichkeiten der bisherigen Analysewerkzeuge deutlich hinausgeht. Sie muss in der Lage sein, ein Gesamtbild der laufenden IT-Prozesse und ihrer Performance über das gesamte IT-System der eAkte hinweg zu liefern. Bis ins kleinste Detail.

Full Stack Observability – dank Agenten alles im Blick.

Die Lösung: Observability-Lösungen

von IBM. Sie integrieren sich mithilfe sogenannter Monitoring-Agenten nahtlos in unterschiedlichste Systeme. Diese Agenten überwachen die Systeme kontinuierlich und führen sämtliche gesammelten Daten zu einem konsolidierten Gesamtbild zusammen. Dazu zählen Informationen aus Anwendungen, Datenbank-Dumps, die Auslastung physischer und virtueller CPUs sowie Daten aus Micro Services, einzelnen Containern oder dem Kubernetes-System als Ganzem.

Das Ergebnis: Ein tief greifender, ganzheitlicher Einblick in die gesamte IT-Landschaft. So lässt sich präzise nachvollziehen, wo und warum Störungen auftreten und welche Anwendungen oder Systeme konkret dafür verantwortlich sind. Dank integrierter KI-Funktionen bauen sie selbstständig ein kontextbezogenes Verständnis der Anwendungen auf und liefern dem IT-Team automatisch relevante Informationen sowie konkrete Lösungsvorschläge.

Schnelle Problemlösung durch ganzheitlichen Blick

In einem konkreten Fall kam es wiederholt zu sogenannten CPU-Steals. Das bedeutet: Die virtuellen CPUs eines Systems mussten auf Rechenzeit der physischen CPUs warten, da diese gerade andere virtuelle Instanzen bedienten. In der Folge stieg die CPU-Last auf den betroffenen Servern stark



Performanceoptimierung sichert auch das Arbeiten zu Hause.

IBM Automation.

IBM Automation ist eine der vier zentralen Plattformen der IBM, die Unternehmen und Behörden unterstützen, die Anforderungen an IT in einer hybriden IT-Landschaft zu bedienen. Die IBM Plattform bietet unter anderem Lösungen für IT-Automatisierung, IT-Security und Technology Business Management. Durch die Übernahmen von Apptio im August 2023 und HashiCorp im

Februar 2025 wurde das Portfolio erweitert und weiter vervollständigt, um den gesamten Lebenszyklus von Geschäftsanwendungen ganzheitlich abzubilden und zu verbessern. Ein besonderer Fokus liegt auf dem Lebenszyklus von Fachanwendungen und IT-Infrastruktur der öffentlichen Hand.

Mehr Infos unter: <https://www.ibm.com/de-de/solutions/automation>

Weitere Informationen zum Bechtle Rahmenvertrag über IBM Lösungen finden Sie unter [bechtle.com/bund](https://www.bechtle.com/bund) sowie beim Beschaffungsamt des BMI (BeschA) unter der Vertragsnummer 22080.



Bechtle@SCCON25. #zukunftsstarke Digitalisierung erleben.

Besuchen Sie uns auf der diesjährigen Smart Country Convention in Berlin. Vom 30. September bis 2. Oktober laden wir Sie zu zahlreichen Fachvorträgen, praxisnahen Tipps und viel Raum für den persönlichen Austausch mit unseren Expert:innen ein. Sprechen Sie mit uns u. a. über die Themen *KI, virtuelle Welten, modernes Arbeiten, Cybersecurity, digitale Bildung, digitale Stadt & Verwaltung, Multi-Cloud und souveräne Infrastrukturen*. Vorbeischauen lohnt sich! **hub27, Stand 401.**



bechtle.com/sccon25