Behörden Spiegel
newsletter
Digitaler Staat und Cyber Security

Nr. 1.329 Berlin und Bonn 11. Februar 2026 ISSN 1867-1993

Mehr als Technik

(BS) Wie sicher Familien und Wohngemeinschaften im digitalen Alltag sind, sei weniger eine rein technische als vielmehr eine organisatorische und soziale Frage. Zu diesem Ergebnis kommt eine neue Studie des Bundesamts für Sicherheit in der Informationstechnik (BSI) mit dem Titel „IT-Sicherheitsmanagement in Haushalten: Risiken, Problemstellungen, Lösungsansätze“.

Foto: BS/ViDi Studio, stock.adobe.com

Die Untersuchung habe erstmals das Ziel verfolgt, grundlegende Prinzipien des Informationssicherheitsmanagements aus dem Unternehmensumfeld auf private Mehrpersonenhaushalte zu übertragen. Diese würden, so die Studie, im Vergleich zu Einzelpersonen vor besonderen Herausforderungen stehen, da digitale Geräte und Anwendungen häufig gemeinsam genutzt würden. Während Unternehmen auf klar definierte Rollen, Zuständigkeiten und Prozesse zurückgreifen könnten, sei die IT-Sicherheit im privaten Zusammenleben oftmals ungeregelt.

Gemeinsam genutzte Geräte ohne Benutzertrennung, geteilte Passwörter für personenbezogene Konten sowie eine ungleiche Verteilung von technischem Wissen unter den Bewohnerinnen und Bewohnern könnten das Sicherheitsrisiko erheblich erhöhen.

Soziale Faktoren entscheidend

Besonders kritisch sei es laut Studie, wenn die Verantwortung für die digitale Sicherheit bei nur einer Person liege. „Die Studie zeigt, dass viele bewährte Sicherheitsmaßnahmen grundsätzlich auf Privathaushalte übertragbar sind, diese jedoch oft an der Komplexität und fehlender Alltagstauglichkeit scheitern. Hinzu kommen soziale Aspekte wie Vertrauen, familiäre Machtverhältnisse und geschlechtsspezifische Rollenbilder", erklärte Caroline Krohn-Atug, Fachbereichsleiterin Digitaler Verbraucherschutz im BSI. Aus den Ergebnissen ließen sich konkrete Empfehlungen auf drei Ebenen ableiten. In Privathaushalten sollten ungleiche Verantwortlichkeiten kritisch hinterfragt und Sicherheitsmaßnahmen als feste Routinen etabliert werden, um sowohl den Kompetenzaufbau zu fördern als auch bestehende Ungleichgewichte abzubauen.

Hersteller digitaler Produkte seien weiterhin in der Pflicht, ihre Angebote konsequent nach den Prinzipien „Security by Design“ und „Security by Default“ zu gestalten. Dabei werde der Aspekt der „Usable Security“ als entscheidender Faktor her-

Fortsetzung auf Seite 2

Inhalt/Themen

KI-Leistungen aus München.....4
Ende der Doppelstrukturen.....8
BfV und BSI warnen vor Phishing.....11

Partnerschaftlich digitalisieren

Ihr Rahmenvertragspartner für IT

Effizienzen heben, Zukunft gestalten

Mehr Informationen per Klick,
Anfragen an public.de@cgi.com

CGI

Fortsetzung von Seite 1

vorgehoben, um Schutzmaßnahmen für Nutzerinnen und Nutzer einfach und sicher anwendbar zu machen. Gleichzeitig bleibe auch der Gesetzgeber gefordert, den Weg hin zu verbindlichen Mindeststandards, transparenten Kennzeichnungen und gezielten Bildungsmaßnahmen fortzuführen. Im Rahmen der Studie sei zudem ein Prototyp für eine Risikoanalyse entwickelt worden, der gezielt auf die Bedürfnisse privater Mehrpersonenhaushalte zugeschnitten sei. Perspektivisch könne daraus ein digitales Tool entstehen, das Nutzerinnen und Nutzer bei der Einschätzung individueller Risiken unterstütze und konkrete Handlungsempfehlungen liefere. Ergänzend verweist das BSI auf sein bestehendes Informationsangebot für Verbraucherinnen und Verbraucher. Dieses umfasse neben Tipps zum digitalen Basisschutz auch Informationen zum sicheren Einsatz von Smarthome-Technologien sowie einen speziellen Wegweiser für Eltern.

Brandenburg steigt im Digital-Index auf

(BS) Brandenburg zählt laut dem aktuellen Deutschland-Index Digitale Verwaltung 2025 des Fraunhofer ÖFIT zu den größten Aufsteigern. Die Studie bescheinigt dem Land einen sehr guten Zugang und eine hohe Benutzerfreundlichkeit digitaler Verwaltungsangebote.

61,4 Prozent der Brandenburgerinnen und Brandenburger gaben an, dass viele Verwaltungsleistungen online beantragt werden können – der dritthöchste Wert bundesweit und zugleich die stärkste Steigerung seit 2023.

Digitalminister Dr. Benjamin Grimm (SPD) erklärte, der Index zeige, dass die Anstrengungen von Land und Kommunen Wirkung entfalten würden: „Immer mehr Bürgerinnen und Bürger erleben, dass Verwaltungsleistungen digital, nutzerfreundlich und verlässlich zur Verfügung stehen. Das ist ein wichtiger Schritt hin zu einer modernen und leistungsfähigen Verwaltung. “Das Vertrauen in die Verwaltung bei der Datenhaltung stieg auf 72,3 Prozent, was dem viertbesten Wert im Ländervergleich entspreche. Brandenburg bot im Mai 2025 204 Online-Dienste nach OZG flächendeckend an. Zwischen Mai 2023 und Mai 2025 seien 77 neue Dienste hinzugekommen.

Digitale Basis noch ausbaufähig

Der Index weist allerdings auch auf Nachholbedarf hin, insbesondere bei digitalen Basiskomponenten wie Online-Bezahlfunktionen, eID, digitalen Bescheiden oder Chatbots, die derzeit unter dem Länderdurchschnitt lägen.

Minister Grimm betonte, dies sei Ansporn, den eingeschlagenen Weg konsequent weiterzugehen, um Verwaltung, Bürgerinnen und Bürger sowie Unternehmen besser zu unterstützen

Das ÖFIT empfiehlt, den Fokus auf die flächendeckende Bereitstellung von Online-Verwaltungsleistungen und den Ausbau der Basiskomponenten zu legen.

Digitale Souveränität: Von Dilemmata zu Handlungsoptionen

Wie lässt sich digitale Souveränität realistisch umsetzen – ohne den Verwaltungsalltag auszubremsen? Im Webinar erklärt Dr. Matthias Zuchowski, Regulatory Affairs & Compliance Manager bei G DATA:

- Was genau ist „digitale Souveränität“?
- Mehr als Datenschutz: Welche Risiken birgt die Abhängigkeit?
- Welche rechtlichen Dilemmata bestehen aktuell?
- Wieso heißt „Rechtssicherheit“ vielleicht, ein Recht brechen zu müssen?
- Welche Handlungsoptionen haben Behörden und Unternehmen?

G DATA CyberDefense

KI soll Hörstest erleichtern

(BS) Das Hessische Ministerium für Digitalisierung und Innovation fördert ein Projekt der Acousticon Hörsysteme GmbH und der Goethe-Universität Frankfurt zur KI-gestützten Hördiagnostik mit fast 500.000 Euro. Ziel sei es, die Hörtests für Menschen mit Schwerhörigkeit effizienter und genauer zu gestalten. Das dreijährige Projekt „Entwicklung und Evaluation einer digitalen automatisierten Hördiagnostik mit interaktiver KI-basierter Antworterkennung“ habe im Januar begonnen.

KI für mehr Lebensqualität

„Gutes Hören ist ein entscheidender Faktor für Lebensqualität und gesellschaftliche Teilhabe. Mit der Förderung des Projekts zur KI-gestützten Hördiagnostik unterstützen wir eine zukunftsweisende Technologie. Hessen bringt Künstliche Intelligenz dorthin, wo sie ganz konkret den Menschen hilft“, sagte Digitalministerin Prof. Dr. Kristina Sinemus. Das Projekt verbinde Forschung mit der Innovationskraft eines hessischen Unternehmens.

Bessere Tests

Zur Beurteilung des Hörvermögens werde üblicherweise ein sogenanntes Tondiagramm erstellt, das die Hörschwelle anhand hoher, tiefer, lauter und leiser Töne ermittle.

Ein Sprachaudiogramm gebe dagegen „viel genaueren Aufschluss über das Hörvermögen“, gehöre aber nicht zu den Standarduntersuchungen, erläuterte Harald Bonsel, Geschäftsführer der Acousticon Hörsysteme GmbH. Bei diesem Test müssten in normaler Lautstärke vorgespielte Worte nachgesprochen werden. „Dies ist der viel aussagekräftigere Test für einen Hörakustiker“, so Bonsel. Da auch diese Berufsgruppe unter Fachkräftemangel leide, solle mit dem Projekt ein Tool geschaffen werden, mit dem die Tests mittels Künstlicher Intelligenz durchgeführt werden könnten. Die Hör-KI könne damit nicht nur die Hörakustiker entlasten und die Tests weniger fehleranfällig machen, sondern diese „zum Beispiel auch in verschiedenen Sprachen durchführen“, was aber erst in einem späteren Schritt der Umsetzung angedacht sei.

Ziel des Projekts sei die Entwicklung eines neuartigen digitalen Audiometrie-Systems, das KI-Erkennung und Multimikrofontechnologie kombiniere. Technische Herausforderungen lägen in der Entwicklung geeigneter Hardware zur Spracherkennung und -verarbeitung sowie in der Gestaltung und dem Training der Algorithmen. Spannend sei, „ob das System Dialekte erkennen könne oder auch undeutliche Aussprachen“, erläuterte Bonsel. Beim Verstehen von Sprache werde viel kognitive Leistung erforderlich, gerade in geräuschstarken Umgebungen. Dieser Lärm könne im Labor dann künstlich erzeugt werden. Wenn das Projekt erfolgreich sei, solle ein als Medizinprodukt zugelassenes Hördiagnostiksystem entstehen.

Verwaltung prämiert

(BS) Deutschland ist beim World Government Summit in Dubai für seinen Einsatz von Künstlicher Intelligenz in der Verwaltung geehrt worden. Ausgezeichnet wurde eine agentische KI, die Planungs- und Genehmigungsverfahren für Infrastrukturprojekte deutlich beschleunigen und Verwaltungsmitarbeitende entlasten könne. Die Lösung wurde vom Bundesministerium für Digitales und Staatsmodernisierung (BMDS) entwickelt und vom Bundesministerium für Wirtschaft und Energie (BMWi) für den Aufbau der Wasserstoff-Infrastruktur initiiert und finanziert.

Die KI analysiere Antragsunterlagen in wenigen Stunden, strukturiere die Inhalte, prüfe erforderliche Nachweise und erstelle fundierte Entscheidungsvorschläge. Die finale Entscheidung verbleibe jedoch bei den zuständigen Mitarbeitenden, sodass rechtliche Verantwortung und Ermessensspielräume weiterhin klar in menschlicher Hand blieben.

Erste Agenten seien bereits in Hamburg im Einsatz; Weitere Module würden aktuell in Nordrhein-Westfalen und beim Fernstraßen-Bundesamt implementiert. BMDS und BMWi planen, die Lösung schrittweise als Open-Source bereitzustellen, sodass sie auch in anderen Behörden genutzt werden könne. Bundesdigitalminister Dr. Karsten Wildberger (CDU) betonte: „Dieser Preis unterstreicht: Deutschland kann bei KI in der Verwaltung in der ersten Liga mitspielen.“

KI-Leistung aus München

Das neue Telekom-Rechenzentrum ist bereits zum Start zu einem Drittel ausgelastet.

Bild: BS/Polina, stock.adobe.com

(BS) Mit der Inbetriebnahme eines großskaligen KI-Rechenzentrums im Münchner Tucherpark erweitert die Deutsche Telekom die verfügbare Hochleistungsinfrastruktur für Anwendungen der künstlichen Intelligenz in Deutschland. Die sogenannte „Industrial AI Cloud“ richtet sich an Unternehmen, Forschungseinrichtungen und öffentliche Organisationen, die für datenintensive Modelle auf leistungsfähige Rechenkapazitäten angewiesen sind. Bereits zum Start ist ein signifikanter Teil der Kapazitäten gebunden, was auf eine hohe Nachfrage nach entsprechender Infrastruktur hindeutet. Technisch basiert die Anlage auf mehreren tausend Hochleistungs-Grafikprozessoren der neuesten Generation und erreicht damit eine Rechenleistung im Exascale-Bereich. Branchenbeobachter sehen darin einen wichtigen Schritt, um die bislang begrenzten KI-Rechenressourcen in Europa auszubauen. Zugleich verdeutlicht das Projekt den wachsenden Wettbewerb um leistungsfähige Datenzentren, die als Voraussetzung für die Entwicklung und den Betrieb komplexer KI-Systeme gelten.

Für die öffentliche Verwaltung eröffnet der Ausbau solcher Infrastruktur neue Handlungsspielräume, wirft jedoch zugleich strategische Fragen auf. Behörden benötigen zunehmend Rechenleistung für datengetriebene Analysen, automatisierte Verfahren oder generative KI-Anwendungen. Gleichzeitig bleiben Anforderungen an Datenschutz, Informationssicherheit und regulatorische Konformität zentrale Rahmenbedingungen. Anbieter reagieren darauf mit dem Versprechen, Daten innerhalb europäischer Rechtsräume zu verarbeiten und technische Architekturen entsprechend auszurichten. Das Münchner Rechenzentrum ist Teil eines breiteren Ansatzes, bei dem Infrastruktur, Plattformdienste und Anwendungsumgebungen stärker verzahnt werden sollen. Ziel ist es, Organisationen nicht nur Kapazität bereitzustellen, sondern auch den Einstieg in produktive KI-Szenarien zu erleichtern. Gerade für öffentliche Einrichtungen könnte dies die Hürde senken, Pilotprojekte in den Regelbetrieb zu überführen – vorausgesetzt, Fragen der Integration in bestehende IT-Landschaften sowie der langfristigen Wirtschaftlichkeit werden frühzeitig adressiert. Parallel gewinnt die Debatte um digitale Souveränität weiter an Bedeutung. Der Aufbau leistungsfähiger Rechenzentren innerhalb Europas wird vielfach als Voraussetzung gesehen, um technologische Abhängigkeiten zu reduzieren und staatliche Gestaltungsspielräume zu sichern. Projekte wie das Münchner Zentrum lassen sich daher auch als infrastrukturelle Antwort auf die zunehmende strategische Relevanz von KI interpretieren.

Auch politisch wird das Projekt als Signal verstanden. Bayerns Wirtschaftsminister Hubert Aiwanger (CSU) spricht von einem „starken Signal für den Wirtschaftsstandort“ und verweist auf die Kombination aus industrieller Basis, Forschung und Vernetzung als ideale Voraussetzung für industrielle KI. Die Industrial AI Cloud ist zudem Teil der Initiative „Made 4 Germany“, die darauf abzielt, Digitalisierung in Wirtschaft und Verwaltung zu beschleunigen.

Welche Rolle leistungsfähige Rechenzentren für staatliche Handlungsfähigkeit und digitale Souveränität künftig spielen werden, ist auch Thema auf dem Kongress „Digitaler Staat“ am 3. und 4. März in Berlin. Am 3. März diskutieren unter anderem Dr. Oliver Heidinger, Präsident von IT.NRW, und Alexander Heinrich, Abteilungsleiter Infrastrukturbetrieb beim ITZBund, im Fachforum „Rückgrat Rechenzentren“ über Perspektiven moderner Rechenzentrumsstrukturen für die öffentliche Verwaltung.

Polizei Rheinland-Pfalz setzt auf KI gegen Deepfakes

KI soll der Polizei Rheinland-Pfalz helfen, digitale Bilddaten zu prüfen.

Bild: BS/Papisut, stock.adobe.com

(BS) Die Polizei Rheinland-Pfalz setzt verstärkt auf Künstliche Intelligenz (KI). Künftig soll ein KI-basierter Deepfake-Detector die Beamtinnen und Beamten bei der Analyse großer Bilddatenbestände unterstützen. „Digitale Manipulationen stellen unsere Ermittlerinnen und Ermittler vor immer größere Herausforderungen", betonte der rheinland-pfälzische Innenminister Michael Ebling (SPD). Genau hier setze der Deepfake-Detector an.

Er sei ein leistungsfähiges Werkzeug, das digitale Ermittlungen effizienter und präziser mache, so Ebling. Entwickelt wurde die neue Anwendung vom Landeskriminalamt (LKA) Rheinland-Pfalz in Kooperation mit dem Polizeipräsidium Einsatz, Logistik und Technik.

Der Deepfake-Detector ist zudem ein Ergebnis der organisatorischen Neuausrichtung des Landeskriminalamtes sowie der Digitalisierungskooperation der Polizei Rheinland-Pfalz (DigiKoRP).

In diesem Rahmen arbeiten Fach- und IT-Expertinnen und -Experten des Landeskriminalamtes (LKA) und des Polizeipräsidiums Einsatz, Logistik und Technik gemeinsam an neuen digitalen Anwendungen für die Polizei.

Einsatz und Funktionsweise

Nach Angaben des Innenministeriums wird der Deepfake-Detector vollständig auf polizeieigener Infrastruktur betrieben. Zudem sei die Anwendung massendatentauglich ausgelegt, wodurch Datenschutz, Datensicherheit und Datenhoheit gewährleistet würden. „Wir setzen bewusst auf eigene Lösungen. So behalten wir die Kontrolle über sensible Daten und können unsere Systeme gezielt an die Anforderungen der Praxis anpassen", erklärte der Innenminister. Ab März soll der Deepfake-Detector zunächst im Rahmen eines Pilotprojekts beim Polizeipräsidium Rheinpfalz getestet werden. Die dabei gewonnenen Erkenntnisse sollen anschließend in die Weiterentwicklung der Anwendung für einen landesweiten Einsatz einfließen.

Advertorial

Prozessmanagement: Hürden erkennen und überwinden

(BS/*Silke Nolopp) Steigende Erwartungen, knappe Budgets, Fachkräftemangel und der drohende Verlust von Wissen stellen Verwaltungen vor enorme Herausforderungen. Gleichzeitig wächst der Druck, Abläufe transparenter, effizienter und digitaltauglicher zu gestalten. Prozessmanagement gilt dabei längst als zentraler Hebel und viele Verwaltungen haben sich bereits auf den Weg gemacht. Doch der Einstieg und vor allem die nachhaltige Etablierung sind anspruchsvoll.

Typische Herausforderungen

Eine der ersten Hürden zeigt sich oft bereits zu Beginn der Prozessmanagement-Reise. Prozesse werden zunächst mit Stift und Papier oder mit allgemeinen Office-Tools visualisiert. Das ist für den Start hilfreich, stößt jedoch rasch an Grenzen.

Mit zunehmender Anzahl und Komplexität der Prozesse wird es unübersichtlich, Auswertungen sind kaum möglich und ein systematisches Weiterarbeiten wird schwierig. An diesem Punkt braucht es spezialisiert Methoden und Werkzeuge, die auf die Anforderungen der öffentlichen Verwaltung zugeschnitten sind. Wenn professionelle Lösungen eingeführt und erste Projekte erfolgreich umgesetzt sind, zeigt sich eine zweite Herausforderung: Prozessmanagement verharrt häufig im Projektmodus.

Einzelne Bereiche arbeiten engagiert, während andere unberührt bleiben. Für den Schritt vom punktuellen Einsatz hin zu einem flächendeckenden, verwaltungsweiten Prozessmanagement braucht es ein klares Zielbild, verbindliche Standards und ein tragfähiges Konzept, das Mitarbeitende und Führungskräfte gleichermaßen mitnimmt.

PICTURE für nachhaltige Prozesse

Genau hier setzt PICTURE an. Mit der intuitiven, bausteinbasierten PICTURE Methode und der PICTURE-Prozessplattform unterstützt PICTURE Verwaltungen dabei, Prozesse verständlich zu erfassen, einheitlich zu steuern und nachhaltig weiterzuentwickeln. Ergänzend hilft die Prozessmanagement Potenzialanalyse PICTURE PROMPT, die individuelle Ausgangslage zu bewerten und ein realistisches Konzept für den langfristigen Einsatz zu entwickeln.

Weitere Informationen finden Sie unter: https://www.picture-gmbh.de/

Besuchen Sie PICTURE auf dem Digitalen Staat 2026!

Wie Verwaltungen diese Hürden konkret überwinden können und worauf es in der Praxis ankommt, zeigt Dr. Lars Algermissen im Vortrag: „Die größten Hürden bei der Einführung von Prozessmanagement und wie man sie erfolgreich überwindet" am 03.03.2026 um 16:15 Uhr auf dem Digitalen Staat.

Nutzen Sie die Chance und gestalten Sie die Zukunft der Verwaltung aktiv mit!

**Dieser Beitrag wurde von Silke Nolopp, Junior Content Managerin bei der PICTURE GmbH, verfasst.*

IT-Dienstleister machen NRWs Kommunen fit

Zur Weiterentwicklung der kommunalen IT in Nordrhein-Westfalen haben OWL-IT und regio iT eine erweiterte Zusammenarbeit vereinbart. *Bild: BS/Jubayer, stock.adobe.com*

(BS) Eine gute Nachricht für die Neuausrichtung der kommunalen IT in Nordrhein-Westfalen: Mit einem Ende Januar geschlossenen Vertrag möchten die Ostwestfalen-Lippe-IT (OWL-IT) und regio iT ihre bestehende Zusammenarbeit stärken. Die regio iT GmbH mit Sitz in Aachen ist als größter kommunaler IT-Dienstleister in NRW Partner für öffentliche Auftraggeber.

Die OWL-IT wiederum versorgt in Form eines kommunalen Zweckverbands rund Neun Millionen Einwohner in mehr als 50 Kommunen mit Technik, Software, Infrastruktur, Services und Innovationen. Dabei steht sie für höchsten Datenschutz sowie bestmögliche Datensicherheit und ist als Rechtsnachfolger des krz der erste kommunale IT-Dienstleister mit der BSI-Zertifizierung ISO 27001 auf Basis von IT-Grundschutz.

Nachdem die beiden bereits in der Vergangenheit erfolgreich in den Bereichen Personalmanagement (P&I LOGA) und Sitzungsmanagement (somacos) kooperiert haben, soll ihr Fokus von nun an vor allem auf Zukunftstechnologien liegen: Künstliche Intelligenz, Automatisierungs- sowie urbane Datenplattformen, Robotic Process Automation (RPA) und Dokumentenmanagement sollen so ihren Weg in die Kommunen finden.

Einen weiteren Schwerpunkt bilden die im Bereich Digitalisierung besonders wichtigen Themen E-Learning sowie Fort- und Weiterbildung. Der Grundstein für innovative Lösungen, die Kommunen und kommunale Unternehmen fit für die digitale Zukunft machen, sei damit gelegt.

Dieter Ludwigs, Vorsitzender der regio iT-Geschäftsführung, ist sich sicher: „Durch unsere Partnerschaft bringen wir KI, Low-Code und Automatisierung schneller in die kommunale Praxis. Das entlastet unsere Kunden und stärkt auch unsere eigene Zukunftsfähigkeit.“ Und Burkhard Schwuchow, Verbandsvorsteher der OWL-IT, bestätigt: „Vor dem Hintergrund der Digitalisierungsoffensive des Bundes und der Konsolidierungsbestrebungen in NRW gestalten wir die Zukunft der kommunalen IT so proaktiv mit.“

Advertorial

Warum Digitalisierung im Betrieb entschieden wird

(BS/*Gerhard Hofweber) Wer von einem „neuen Betriebsmodell für die öffentliche Verwaltung“ spricht, denkt schnell an Staatsreform: andere Organisationen und Kompetenzen, Agilität, KI, Cloud. Diese Debatte ist legitim – sie verfehlt jedoch den eigentlichen Engpass.

Deutschlands Problem ist nicht der Mangel an Strategien oder Technologien, sondern die Annahme, dass föderal organisierte Digitalisierungsprojekte ohne gemeinsame Betriebsverantwortung dauerhaft handlungsfähig werden können.

Digitalisierung scheitern selten am Go-Live

Sie scheitert danach: wenn Leistungen über Haushaltsjahre stabil betrieben, bei Rechtsänderungen angepasst, bei steigender Nutzung skaliert und zwischen Zuständigkeiten koordiniert werden müssen.

Genau dafür ist das bestehende Betriebsmodell nicht ausgelegt – und genau darüber wird zu selten offen gesprochen. Stattdessen entstehen neue Plattformen, Stacks, Cloud-Strategien und Zielbilder.

Sie weisen in die richtige Richtung, lösen das Kernproblem aber nicht. Betrieb bleibt fragmentiert, Verantwortung endet mit Projekten, Standards sind verhandelbar, Wiederverwendung optional. So entstehen formal moderne, faktisch jedoch nicht lieferfähige Lösungen.

Das klassische Verwaltungsmodell ist nicht überholt. Es ist auf Rechtssicherheit, Stabilität und Kontrolle optimiert. Kritisch wird es dort, wo diese Logik unverändert auf digitale Leistungen trifft, die kontinuierliche Weiterentwicklung und Skalierung erfordern.

Ein neues Betriebsmodell bedeutet daher keine große Staatsreform. Es bedeutet, Betrieb als strategische Kernaufgabe zu begreifen: mit klarer Verantwortung über Projektgrenzen hinaus, verbindlichen Standards und einer Betriebslogik, die föderale Autonomie ermöglicht, ohne kollektive Handlungsfähigkeit zu verlieren.

Genau diese verdrängte Frage steht im Mittelpunkt des Forums „Ein neues Betriebsmodell für die öffentliche Verwaltung“ beim Digitalen Staat – und bereits zuvor im begleitenden Online-Live-Talk am 25.02.26 für alle, die Digitalisierung nicht als Projekt, sondern als dauerhafte Betriebsaufgabe verstehen.

Melden Sie sich jetzt an unter
https://webinar260225.fjd.de

Dieser Beitrag wurde von Gerhard Hofweber, Vorstand FJD Information Technologies AG, verfasst.

IT-Sicherheitstag Bayern

4. Februar 2026
München

Schutz schafft Vertrauen

Zwischen Meldepflichten und Datenhoheit wird in Europa bereits über neue Spielräume diskutiert – mit dem Ziel, Datenschutz praxisnäher zu gestalten, ohne den Grundrechtsschutz aus dem Blick zu verlieren. *Foto:BS/Tanja Klement*

(BS) Datenschutz wird häufig als Innovationshemmnis beschrieben – eine Sichtweise, der Prof. Dr. Thomas Petri, Bayerischer Landesbeauftragter für den Datenschutz, entschieden widerspricht. „Datenschutz ist in erster Linie Grundrechtsschutz im digitalen Kontext."

Er sichere digitale Selbstbestimmung, die ermögliche, dass sich „der Mensch frei entfalten kann". Damit wird Datenschutz zur Voraussetzung einer vertrauenswürdigen Digitalisierung, nicht zu ihrem Gegenpol. Petri versteht Datenschutz als Weiterentwicklung von Persönlichkeitsrecht und informationeller Selbstbestimmung. Ziel sei es, den Menschen auch im digitalen Raum als Individuum zu schützen und ihm Kontrolle über die Nutzung seiner Daten zu geben. „Effektiver Grundrechtsschutz und Förderung von Digitalisierung sind zeitgleich möglich und das sollte unser gemeinsames Ziel sein."

Gleichzeitig erkennt er Reformbedarf. Stark zersplitterte rechtliche Voraussetzungen erschweren bislang den Austausch zwischen Behörden. Auf europäischer Ebene wird daher diskutiert, Meldepflichten für Datenschutzpannen stärker auf tatsächlich hohe Risiken zu konzentrieren. Während überbordende Bürokratie reduziert werden müsse, warnt Petri davor, Betroffenenrechte einzuschränken – dies würde Vertrauen bei Bürgerinnen und Bürgern untergraben.

Auch bei der Frage nach zentralen Strukturen plädiert er für Differenzierung: „Es braucht nicht zwingend zentrale Regularien, aber es braucht ein einheitliches Ergebnis." Regionale Behörden gewährleisteten Bürgernähe und könnten insbesondere kleine und mittelständische Unternehmen passgenau betreuen. Tatsächlich hätten lediglich drei Prozent der Unternehmen Interesse an überregionalen Lösungen, während die große Mehrheit von lokal ausgerichteter Beratung profitiere.

Zugleich verweist Petri auf ein Grundprinzip der IT-Sicherheit: Vertrauen allein genügt nicht, denn häufig erweist sich der Mensch als „schwächstes Glied in der Kette". Umso wichtiger sei ein Rahmen, der Freiheit und Schutz zusammendenkt. Datenschutz solle nicht begrenzen, sondern Menschen befähigen, souverän über ihre Daten zu entscheiden – und damit die Grundlage für eine tragfähige digitale Gesellschaft schaffen.

Einen ausführlichen Artikel lesen Sie dazu in der März-Ausgabe des Behörden Spiegel.

Bayerns IT-Fragen

(BS) Digitale Souveränität und IT-Sicherheit bleiben zentrale Herausforderungen für Verwaltung und Politik. Das wurde beim IT-Sicherheitstag München mehr als deutlich.

Florian von Brunn (SPD), Sprecher der SPD-Landtagsfraktion für Energie und Digitales, stellte die aktuelle Debatte um den Einsatz von Microsoft-Produkten in Bayern in den Kontext digitaler Souveränität: „Digitale Souveränität bedeutet für mich, dass wir Dinge, kritische Infrastrukturen und kritische Dienste selbst betreiben können." Er wies darauf hin, dass bestehende Abhängigkeiten von US-Anbietern kritisch zu bewerten seien, insbesondere bei staatlichen Kernaufgaben und sensiblen Daten.

Auch Tobias Beck (Freie Wähler), Mitglied des Ausschusses für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung, betonte die Bedeutung von Datenschutz. Aus seiner Sicht müsse gewährleistet sein, dass Daten in Deutschland verblieben und nicht dem Zugriff ausländischer Staaten unterlägen. Er verwies darauf, dass alternative Systeme, etwa auf Open-Source-Basis, aus seiner Erfahrung heraus verlässlich betrieben werden könnten und für die Verwaltung Vorteile böten.

Michael Rainer sprach sich gegen abrupte Systemwechsel aus. „Transformation muss Schritt für Schritt passieren", betonte der Business Development Manager Public bei Enginsight.

Die Referenten waren sich einig, dass IT-Sicherheit zunehmend auch eine wirtschaftliche Schlüsselfrage sei. Rainer verwies auf konkrete Schäden durch Cyber-Angriffe auf Kommunen. Von Brunn ergänzte, dass Kommunen und kritische Einrichtungen finanziell und strukturell besser unterstützt werden müssten, um Risiken wirksam zu begrenzen.

INNOVATION MIT TAKT UND TEMPO

Der neue Sound für die digitale Verwaltung

Ende der Doppelstrukturen

„Seniorinnen und Senioren sind nicht von der Digitalisierung überfordert – sondern von der Komplexität deutscher Bürokratie", betonte Mehring. *Foto: BS/Bildschön*

(BS) Bayerns Digitalstrategie zielt auf einen grundlegenden Umbau staatlicher Leistungen. Dr. Fabian Mehring, Bayerischer Staatsminister für Digitales, formuliert den Anspruch klar: „Ich möchte aus Bayern nichts geringeres machen als einen modernen Digitalstaat." Digitalisierung sei kein Selbstzweck, sondern müsse das Leben der Menschen konkret verbessern und zugleich wirtschaftliche Innovation ermöglichen.

Ein zentraler Baustein ist das Prinzip „Digital Only", das Bayern erfolgreich in der Digitalministerkonferenz verankert hat. Verwaltungsleistungen sollen künftig primär digital bereitgestellt werden – nicht als bloße Übertragung analoger Verfahren, sondern als neu gedachte Prozesse. Mehring warnt ausdrücklich davor, alte Abläufe einfach ins Internet zu verschieben. Überflüssige Bürokratieschritte müssten entfallen, neue Gesetze idealerweise nur dann verabschiedet werden, wenn sie vollständig digital umsetzbar sind. Der bayerische Digitalcheck setzt deshalb bereits vor parlamentarischen Anhörungen an, um digitale Praxistauglichkeit frühzeitig sicherzustellen.

Treiber dieser Entwicklung ist nicht zuletzt der demografische Wandel. Wenn künftig weniger Fachkräfte zur Verfügung stehen, müsse „so viel automatisiert werden wie irgend möglich". Effizienz wird damit zur Voraussetzung staatlicher Handlungsfähigkeit. Gleichzeitig sieht Mehring in funktionierenden digitalen Verwaltungsleistungen eine Chance, Vertrauen in staatliche Institutionen zu stärken: „Das Image des Staates wird nicht im Fernsehen in Talkshows geformt, sondern auf dem Amt."

Föderale Hindernisse

Als strukturelles Hindernis benennt der Minister föderale Insellösungen. „Der größte Gegner von digitaler Transformation ist die föderale Denke", kritisiert er und fordert schnellere bundesweite Standards. Gemeinsam mit Hessen treibt Bayern deshalb eine nationale Digitalisierungsoffensive voran, die Kommunen schrittweise zur Nutzung zentraler Leistungen befähigen soll.

Entscheidend bleibt jedoch der Abschied vom Parallelbetrieb. „Eine digitale Dividende kann erst dann entstehen, wenn die parallel laufenden analogen Prozesse abgebaut werden." Nur wenn Verwaltung konsequent digital organisiert wird, könne Deutschland zu führenden Digitalstaaten aufschließen und einen messbaren volkswirtschaftlichen Mehrwert erzielen.

Einen ausführlichen Artikel dazu lesen Sie in der März-Ausgabe des Behörden Spiegel.

Datenfluss

(BS) Im Januar 2026 konnte das Nationale Once-Only-Technical-System (NOOTS) einen ersten Erfolg verbuchen: In Baden-Württemberg wurden Daten aus dem Kraftfahrt-Bundesamt für die Beantragung eines Anwohnerparkausweises erstmals erfolgreich abgerufen. Auf dem Zukunftskongress Bayern, organisiert vom Behörden Spiegel, berichteten Expertinnen und Experten von weiteren fortgeschrittenen Pilotprojekten.

Ein nächster Schritt wird derzeit in Nordrhein-Westfalen erprobt: Hier sollen Daten aus dem Handelsregister für die digitale Gewerbeanmeldung über das Nationale Once-Only-Technical-System abgerufen werden. Die zuständige Managerin für Registermodernisierung, Lena Ritterswürden von publicplan, betonte, dass Deutschland vor einer großen Herausforderung stehe: Es existieren rund 13.000 Register, jedes mit eigenen Abläufen, Begrifflichkeiten und Verantwortlichkeiten. Standardisierung sei daher entscheidend, um die unterschiedlichen Strukturen zu vereinheitlichen und die Once-Only-Idee flächendeckend umzusetzen. Auch wenn erste Erfolge wie in Baden-Württemberg zeigen, dass der digitale Datenaustausch funktionieren kann, sei der Weg zu einer wirklich umfassenden Registermodernisierung noch lang.

In Bayern laufen derzeit eigene Erprobungsprojekte in den drei Bereichen Bauwesen, Umwelt und Energie. Simone Baecker-Neuchl, Projektleiterin Registermodernisierung vom Bayerischen Staatsministerium für Digitales, betonte, dass neben der Technik vor allem Kommunikation zwischen den beteiligten Akteuren entscheidend sei, um die NOOTS-Anbindung erfolgreich umzusetzen: „Es braucht überzeugte Stakeholder und intelligente Projektgovernance. Kommunikation ist entscheidend."

IT-Sicherheitstag Bayern

4. Februar 2026 München

VERNETZT UND SICHER

Gemeinsam für eine digitale Zukunft in Bayerns Verwaltung

www.it-sicherheitstag.bayern

ZUKUNFTSKONGRESS BAYERN

5. Februar 2026 | München

www.zukunftskongress.bayern

INNOVATION MIT TAKT UND TEMPO

Der neue Sound für die digitale Verwaltung

Oliver Wolf, Teamleiter Key Account Management Süd/West bei secunet, skizzierte, wie öffentliche Verwaltungen resilienter gestaltet werden können.

Michael Rainer, Business Development Manager Public bei Enginsight, Florian von Brunn (SPD) und Tobias Beck (Freie Wähler), Mitglieder des Bayerischen Landtags, diskutierten wie die Sorgen der IT-Sicherheitscommunity in konkrete politische Maßnahmen übersetzt werden können.

Low Code soll die Zukunft von simplen Fachverfahren bilden. Wie das gelingt, schilderte Sandra Schmitz vom Bayerischen Staatsministerium für Umwelt und Verbraucherschutz.

In den Kaffeepausen nutzten die Teilnehmenden zum regen Austausch über die bestimmenden Themen des Tages.

Dr. Eva-Charlotte Proll, Herausgeberin und Chefredakteurin des Behörden Spiegel, begrüßte Dr. Fabian Mehring, Bayerischer Staatsminister für Digitales, zu seiner Keynote auf dem Zukunftskongress Bayern.

Nadine Weischer aus dem Programmbereich Personalmanagement beim KGSt, erläuterte, wie effektive Förderung und Bindung von IT-Fachkräften aussehen kann.

Markus Jopp, Bereichsleitung für Digitalisierung, führte aus, welche Schritte eingeleitet wurden, um Augsburg zu einer modernen und digitalen Kommune zu machen.

Die OZG-Experten diskutierten über die Erfolgsgeschichte des digitalen Bauantrags und die Rolle des OZG für die Weiterentwicklung des Deutschland Stacks.

Fotos: BS/Bildschön/Tanja Klement

Advertorial

Cyberservices der govdigital

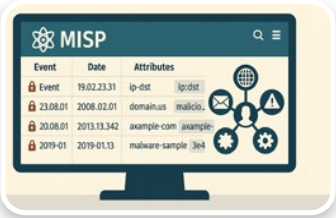
IT-Notfallübungen für Mitglieder und Träger

Die govdigital stellt ihren Mitgliedern sowie deren Trägern den Service „IT-Notfallübungen“ zur Verfügung. Ziel ist, die Handlungsfähigkeit bei Cyberangriffen, Systemausfällen oder Fehlkonfigurationen zu stärken. Denn im Ernstfall entscheidet nicht nur Technik, sondern ob Rollen, Entscheidungswege und Kommunikation funktionieren.

Der Service wird in Form eines Rahmenvertrages von der Firma Deloitte erbracht und unterstützt den gesamten Übungszyklus: Auswahl geeigneter Szenarien, Vorbereitung, moderierte Durchführung und strukturierte Nachbereitung. Inhalte orientieren sich an typischen Lagen wie Ransomware, Ausfall zentraler Infrastruktur- oder Cloud-Services, Störungen von Fachverfahren, Netzwerk-/Identitätsproblemen oder Ausfällen bei Dienstleistern. Je nach Reifegrad sind Tabletop-Übungen, Planspiele oder erweiterte Formate möglich.

Wesentlich ist der Nutzen aus der Übung: Erkenntnisse werden transparent dokumentiert, Lessons Learned abgeleitet und in einen priorisierten Maßnahmenplan überführt, mit konkreten Verbesserungen für Organisation, Technik, Dokumentation und Kommunikation.

Weitere Cyberservices der govdigital



Malware Information Service (MISP): Bedrohungsinformation operationalisieren

- Abwehrmaßnahmen übergreifend ermitteln und teilen
- Angriffserkennung und Angriffsvermeidung
- Effizienzsteigerung durch geteilte Ressourcen
- Hohe Datenqualität und hohe Relevanz

Business Continuity Management (BCM): Vorbereitung auf den Notfall

- 3-tägiges Seminar
- Anwendung des BSI-Standards 200-4 auf kommunale Bedarfe
- Trainiert die verlässliche Absicherung des Verwaltungsbetriebs
- Aufbau eines Business Continuity Management Systems – BCMS für die kommunale Verwaltung

Kontakt
Uwe Schwarz
CISO/Leiter Cybersicherheit
govdigital eG
cybersicherheit@govdigital.de

GOVDIGITAL

Weitere Informationen unter: govdigital.de/themen-leistungen/cybersicherheit

BfV und BSI warnen gemeinsam vor Phishing

Über Messenger-Dienste wie Signal versuchen Angreifende derzeit, auf Konten und Daten von Nutzenden zuzugreifen. *Bild: BS/Gorodenkoff, stock.adobe.com*

(BS) Über die Messenger-Plattform „Signal“ sollen aktuell staatlich gesteuerte Phishing-Angriffe durchgeführt werden. Darauf machen nun das Bundesamt für Verfassungsschutz (BfV) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) gemeinsam aufmerksam. Die Angreifer nutzen laut BfV und BSI legitime Sicherheitsfunktionen der Anwendungen in Kombination mit Social Engineering. Im Fokus stehe somit der „Faktor Mensch“ als vermeintlich schwächstes Glied.

Technische Schwachstellen oder Schadsoftware spielten dagegen keine Rolle. Ziel der Angriffe sei es, unbemerkt Zugriff auf Einzel- und Gruppenchats sowie auf Kontaktlisten der betroffenen Personen zu erlangen. Konkret hätten die beiden Behörden bereits zwei Angriffsvarianten beobachtet. Bei der ersten Variante geben sich die Täter als Support des Messengerdienstes aus oder nutzen die Funktionen der Plattform gezielt aus. Sie kontaktieren ihre Opfer als vermeintlicher „Signal-Support“ und erzeugen durch falsche Sicherheitswarnungen Handlungsdruck.

Durch Herausgabe einer PIN oder eines Verifizierungscodes übernehmen sie das Konto vollständig und können im Namen der Betroffenen Nachrichten versenden. Die zweite Variante missbraucht die Funktion zur Kopplung zusätzlicher Endgeräte. Unter einem glaubwürdigen Vorwand bringen die Angreifer die Zielperson dazu, einen QR-Code zu scannen.

Dadurch wird ein von den Tätern kontrolliertes Gerät mit dem Konto verbunden. Die Betroffenen behalten zwar Zugriff auf ihr Konto, bemerken jedoch häufig nicht, dass ihre Kommunikation überwacht wird.

Laut BfV und BSI liegt der Schwerpunkt der Angriffe auf dem Messenger-Dienst „Signal“.

Vergleichbare Methoden seien jedoch auch über „WhatsApp“ aufgrund ähnlicher Funktionen denkbar. Bei den bisher betroffenen Personen handele es sich um eine „hochkarätige Zielfläche“, weshalb die Behörden von einem staatlich gesteuerten Cyber-Akteur ausgehen.

Schutz durch Achtsamkeit

Nutzerinnen und Nutzer sollten keine Nachrichten von vermeintlichen Support-Konten beantworten, verdächtige Konten blockieren oder melden und ihre Signal-PIN niemals per Nachricht weitergeben, so das BfV und BSI.

QR-Codes sollten nur beim eigenen Gerätewechsel gescannt werden. Unbekannte Gruppeneinladungen seien zudem zu ignorieren, und die Liste der gekoppelten Geräte regelmäßig zu überprüfen. Fremde Geräte sollten umgehend entfernt werden. Ein Angriff sei dann erkennbar, wenn in der Signal-App das eigene Gerät als nicht registriert angezeigt wird und keine Nachrichten mehr versendet oder empfangen werden können.

Hinweise auf Betroffenheit bei Kontakten treten auf, wenn Signal eine geänderte Sicherheitsnummer in Einzel- oder Gruppenchats meldet.

In solchen Fällen sollte über einen anderen Kommunikationskanal überprüft werden, ob die Änderung legitim ist.

Cyber-Abwehr neu denken

Klaus Bürg (Palo Alto Networks), Jeanne Dillschneider (Bündnis 90/Die Grünen), Dr. Uda Bastians (Deutscher Städtetag) und Daniel Grimm (Vitako) diskutieren, wie öffentliche Stellen Cyber-Angriffe besser abwehren können. *Foto: BS/Carla Menzel*

(BS) Cyber-Angriffe treffen öffentliche Stellen inzwischen fast täglich. Beim Parlamentarischen Abend des Behörden Spiegel diskutierten Fachleute, wie Deutschland seine digitale Infrastruktur widerstandsfähiger machen kann. Klassischer Perimeterschutz reiche längst nicht mehr aus, so die Referentinnen und Referenten. Behörden müssten in der Lage sein, Vorfälle zu überstehen und schnell wieder in den Normalbetrieb zu gelangen. Notbetriebspläne, funktionierende Backups und Wiederanlaufkonzepte rückten mehr in den Fokus. „Früher hat man versucht, eine hohe Mauer zu bauen – heute wissen wir: Der Angreifer kommt rein“, betonte Daniel Grimm, Senior Manager Verwaltungsdigitalisierung bei Vitako. Neue Technologien wie Künstliche Intelligenz (KI) verändern zusätzlich die Lage. Johannes Schätzl (SPD), digitalpolitischer Sprecher der SPD-Bundestagsfraktion, sieht in KI einen Effizienzgewinn für Angreifer, die damit bestehende Angriffsmuster schneller und kostengünstiger einsetzen können. Gleichzeitig eröffnet KI auch Behörden Chancen: Sie helfe bei der Analyse großer Datenmengen, der Priorisierung von Vorfällen und der Automatisierung von Prozessen. „KI kann Informationen schnell aggregieren, aber sie kann auch Prozesse und Vorgänge massiv beschleunigen“, erklärte Helmut Reisinger, CEO EMEA & LATAM bei Palo Alto Networks. Entscheidend sei, dies in einem konsequenten Zero-Trust-Ansatz umzusetzen.

Die Umsetzung von Cyber-Sicherheitsmaßnahmen ist für viele kleine Kommunen dennoch herausfordernd, da IT-Ressourcen und Fachpersonal oft begrenzt seien, wie Dr. Uda Bastians, Leiterin des Dezernats Recht und Verwaltung beim Deutschen Städtetag, betonte. Auch Bundestagsabgeordnete Jeanne Dillschneider (Bündnis 90/Die Grünen), Mitglied im Ausschuss für Digitales und Staatsmodernisierung, sieht deutlichen Nachholbedarf: Die NIS-2-Richtlinie sei ein wichtiger Schritt, richte sich jedoch vor allem an Bundesbehörden und zentrale Einrichtungen. Nachgeordnete Behörden und Kommunen sind in der deutschen Umsetzung bislang nicht unmittelbar erfasst – ein Umstand, den sie kritisch bewertete.

Impressum

Herausgeberin und Chefredakteurin von „Behörden Spiegel Newsletter Digitaler Staat und Cyber Security“ und verantwortlich i.S.d.P.: Dr. Eva-Charlotte Proll. Redaktionelle Leitung: Carla Menzel, Frederik Steinhage Redaktion: Julia Grahn, Jonas Brandstetter, Julian Faber, Guido Gehrt, Ann Kathrin Herweg, Mirjam Klinger, Scarlett Fels, Lars Mahnke, Anne Mareile Moschinski, Sven Rudolf. Online-Redaktion: Tanja Klement. Redaktionsassistenz: Kerstin Bauer.

ProPressVerlagsgesellschaft mbH, Friedrich-Ebert-Allee 57, 53113 Bonn, Telefon: 0049-228-970970, E-Mail: redaktion@behoerdenspiegel.de; www.behoerdenspiegel.de. Registergericht: AG Bonn HRB 3815. UST-Ident.-Nr.: DE 122275444 - Geschäftsführer: Dr. Fabian Rusch.

Herausgeber- und Programmbeirat: Dr. h. c. Uwe Proll (Vorsitz). Der Verlag hält auch die Nutzungsrechte für die Inhalte von „Behörden Spiegel Newsletter Digitaler Staat“. Die Rechte an Marken und Warenzeichen liegen bei den genannten Herstellern. Bei direkten oder indirekten Verweisen auf fremde Internetseiten („Links“), die außerhalb des Verantwortungsbereiches des Herausgebers liegen, kann keine Haftung für die Richtigkeit oder Gesetzmäßigkeit der dort publizierten Inhalte gegeben werden.

Behörden Spiegel

NEWSLETTER & PODCASTS

In den aktuellen Ausgaben unserer weiteren Newsletter und Podcasts finden Sie u. a. folgende Themen:

NEWSLETTER

Newsletter „Netzwerk Sicherheit“ – 09. Februar:
- Debatte um Sicherheit im Bahnverkehr
- Grüne fordern effektive Bekämpfung von Finanzkriminalität
- Rheinland-Pfalz betont Sicherheit an Schulen

Newsletter „Rettung. Feuer. Katastrophe“ – 05. Februar:
- Erstmalig: Zentrale Beschaffung für Kommunen
- Administrative Krisenbewältigung ist ausbaufähig
- JUH und Bundeswehr rücken zusammen

Newsletter „Verteidigung. Streitkräfte. Wehrtechnik“ – 10. Februar:
- Vorvertrag für MEKO-Fregatte vergeben
- Hensoldt stattet Kampf- und Schützenpanzern mit Optronik aus
- Worum es im zweiten Space Race geht

Newsletter „Stadt. Land. News.“ – 29. Januar:
- Teilerholung der Bauwirtschaft
- Wenn Fördermittel strangulieren
- Wasser im Wandel

PODCASTS

Podcast „Public Sector Insider“ – 10. Februar:
- Der falschen Erzählung gegenübertreten: Der brandenburgische Innenminister René Wilke erläutert im Interview mit Dr. Eva-Charlotte Proll, warum Reformen im Verfassungsschutz notwendig sind, um Bedrohungen effektiv zu begegnen und Kontrolle zu gewährleisten.

E-JOURNAL

future4public:
- Unsere Städte sind so vielfältig wie die Menschen, die in ihnen leben. Doch was braucht es, damit wirklich alle gut mitgenommen werden?