



Zeitschrift der Bundes-Arbeitsgemeinschaft
der Kommunalen IT-Dienstleister e. V.

VITAKO

vitako.de

AKTUELL

03|2025

CYBERSICHERHEIT

LÜCKEN SCHLIESSEN

**THOMAS JARZOMBK, PST BEIM BUNDESMINISTER
FÜR DIGITALES UND STAATSMODERNISIERUNG**
DEUTSCHLAND-STACK: RÜCKGRAT EINER
MODERNEN VERWALTUNG

**FRIEDERIKE DAHNS, ABTEILUNGSLEITERIN
IM BUNDESMINISTERIUM DES INNERN**
CYBERSICHERHEIT AUF KOMMUNALER EBENE

**DR. DORIT BOSCH, GRÜNDERIN DES
MINDSHIFT FESTIVALS**
DIE KOMMUNEN DÜRFEN IHR MOMENTUM
JETZT NUTZEN

Cybersecurity mit Bechtle

Strategisch denken. Praxisnah handeln.

Bechtle begleitet kommunale IT-Dienstleister und Kommunen von der Entwicklung der IT-Sicherheitsstrategie bis zur Umsetzung – mit konkreten Lösungen, persönlicher Beratung und starker lokaler Präsenz.

Unsere 500 Security-Expertinnen und -Experten übersetzen komplexe Sicherheitsanforderungen in kommunalen Verwaltungen in greifbare Maßnahmen. So wird aus anspruchsvollen Konzepten echte Cybersecurity für Kommunen.

Jetzt weitere Infos anfordern:

provitako.dortmund@bechtle.com | +49 231 725489 17

bechtle.com

LIEBE LESERINNEN UND LESER,

fast 90 Prozent der kommunalen IT-Dienstleister sagen, dass der bürokratische Aufwand rund um das Thema Cybersicherheit zugenommen hat. Ein Grund zur Klage? Nicht unbedingt: Sich um Cybersicherheit zu kümmern heißt auch, die Einhaltung von Sicherheitsregeln zu dokumentieren und sich mit Sicherheitsstandards zu beschäftigen. Themen, die zunächst einmal bürokratischer Natur sind.

Worauf es ankommt: Der Aufwand muss echten Mehrwert in punkto Cybersicherheit bieten. Wir brauchen deutschlandweit geltende Mindeststandards, die auch für kleine Kommunen umsetzbar sind. Zudem sind Bund und Länder gefordert, die Kommunen zu unterstützen. Themen, die auch der VITAKO Vorstandsvorsitzende Sören Kuhn im Leitartikel aufgreift.

Um das Sicherheitsniveau kurzfristig zu heben, ist die interföderale Zusammenarbeit das Gebot der Stunde. In der Reportage schauen wir nach Hessen und Bayern. Dort finden sich hervorragende Beispiele, wie Kooperation auf kommunaler, Landes- sowie auch Bundesebene über das BSI gelingen kann. Weitere Perspektiven finden sich im Gastbeitrag von BMI-Abteilungsleiterin Friederike Dahns, die Unterstützungsmöglichkeiten von Seiten des Bundes aufzeigt, sowie im Interview mit Dr. Tilmann Dittrich und Dr. Michael Littger, die das IT-Sicherheitsniveau in Kommunen untersucht haben.

Cybersicherheit ist eine wesentliche Voraussetzung, damit digitale Verwaltung gelingt. Aber natürlich braucht es mehr. Ich freue mich sehr, dass wir für dieses Heft Thomas Jarzombek, Parlamentarischer Staatssekretär beim Bundesminister für Digitales und Staatsmodernisierung, für einen Gastbeitrag mit Schwerpunkt Deutschland-Stack gewinnen konnten. VITAKO unterstützt das Vorhaben und erarbeitet derzeit konzeptuelle Impulse, um das Projekt erfolgreich in der Fläche umzusetzen. Impulse, die wir mit Ihnen künftig diskutieren wollen.

Anregende Lektüre wünscht

Ihr



**Lars Hoppmann ist
geschäftsführender
Vorstand von
VITAKO.**

SCHWERPUNKT: CYBERSICHERHEIT

6 LEITARTIKEL

KOMMUNEN UNTERSTÜTZEN. JETZT.

Zahlreiche Projekte stärken deutschlandweit bereits die kommunale Cybersicherheit – doch der Schutz reicht längst nicht aus. Im Leitartikel zeigt Sören Kuhn, wo die Bundesregierung dringend nachsteuern muss.

10 GASTBEITRAG

DEUTSCHLAND-STACK: RÜCKGRAT EINER MODERNEN VERWALTUNG

Mit dem neuen Digitalministerium erlangt die digitale Verwaltung endlich die nötige Priorität. Warum der Deutschland-Stack dabei einen entscheidenden Startimpuls liefert, erläutert der Parlamentarische Staatssekretär Thomas Jarzombek in seinem Gastbeitrag.

13 REPORTAGE

KOMMUNEN KÖNNEN SICH HILFE HOLEN

Cyberangriffe auf Kommunen nehmen stetig zu. Doch gerade für kleinere Kommunen sind umfassende Schutzmaßnahmen kaum zu stemmen. Welche Unterstützungsangebote es gibt, zeigen zwei VITAKO Mitglieder und das Bundesamt für Sicherheit in der Informationstechnik (BSI).

19 DIGITALE VERWALTUNG

KOMMUNALE IT-INFRASTRUKTUREN IM WANDEL

Ob Fachkräftemangel, Modernisierungsdruck oder IT-Sicherheit – die kommunale IT steht vor großen Herausforderungen. Der IT-Dienstleister PROSOZ setzt dabei auf Cloud-Dienstleistungen als Innovationsmotor.

20 GASTBEITRAG

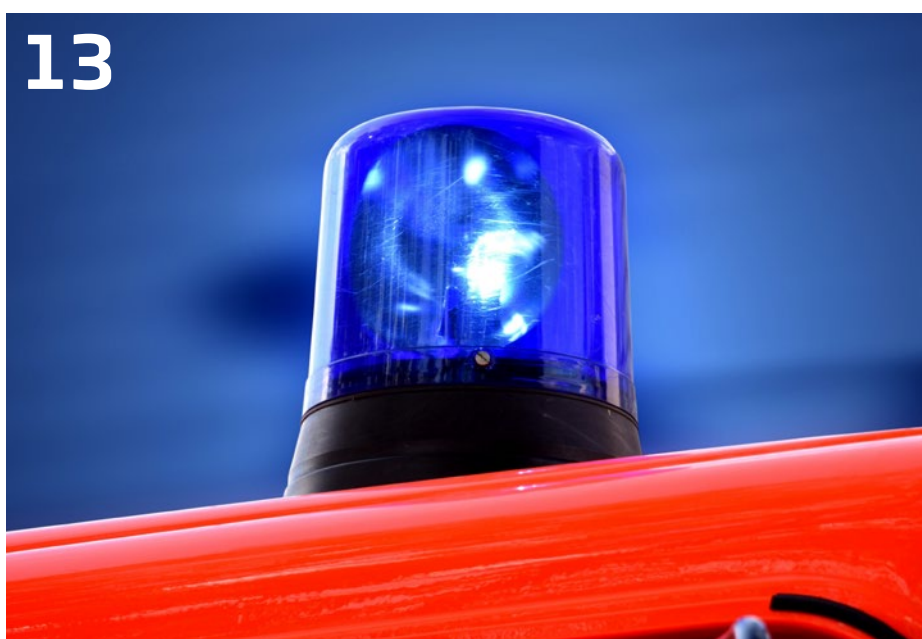
CYBERSICHERHEIT AUF KOMMUNALER EBENE

Das Bundesministerium des Innern (BMI) gewährleistet die Sicherheit im digitalen Raum. Warum das BSI-Gesetz dabei gerade für Kommunen ein zentraler Hebel ist, erläutert Abteilungsleiterin Cyber- und Informationssicherheit Friederike Dahns.

22 INTERVIEW

„CYBERSICHERHEIT MUSS CHEFSACHE SEIN“

Wie gut sind Deutschlands Kommunen in Sachen Cybersicherheit aufgestellt? Das hat das Frankfurter cyberintelligence.institute (CII) in einem Whitepaper untersucht. Die Ergebnisse erläutern Dr. Michael Littger und Dr. Tilmann Dittrich im Interview.



24 GOVDIGITAL

GENAI-PLATTFORM: SICHER, SKALIERBAR, SOUVERÄN

Generative KI bietet enorme Potenziale – doch die sichere und verantwortungsvolle Nutzung stellt Verwaltungen vor eine zentrale Herausforderung. Unterstützung bietet die GenAI-Plattform der govdigital.

26 KOMMUNE DER ZUKUNFT

VERWALTUNGSDIGITALISIERUNG IN EIGENREGIE

Die Herausforderung der digitalen Verwaltung ist groß. Mit der Low-Code-Plattform Axon Ivy befähigt der kommunale IT-Dienstleister OWL-IT Kommunen, einfache digitale Lösungen eigenständig umzusetzen.

28 INTERVIEW

„DIE KOMMUNEN DÜRFEN JETZT IHR MOMENTUM NUTZEN“

Wie können Kommunen und die Menschen, die dort täglich Verantwortung übernehmen, auf Bundesebene endlich sichtbarer werden? Das diskutieren Verwaltungsjuristin Dr. Dorit Bosch und Katrin Giebel, stellvertretende Geschäftsführerin von VITAKO, im Interview.

30 PROVITAKO

BESCHAFFUNG NOCH STRATEGISCHER PLANEN

Die ProVitako bündelt die Beschaffungsbedarfe ihrer Mitglieder. Mit dem neuen Portfolio-Management setzt die Genossenschaft einen neuen Meilenstein.

31 SPOTLIGHTS

Politischer Abend 2025

32 UMFRAGE

Die Gefahr von Cyberangriffen wächst – insbesondere für kleine Kommunen. Wie VITAKO Mitglieder die Lage bewerten, zeigt die aktuelle Umfrage.

34 TERMINE





KOMMUNEN UNTERSTÜTZEN. JETZT.

Quer durch Deutschland gibt es großartige Projekte, in denen Kommunen ihre Cybersicherheit stärken – das ist gut! Allerdings herrscht mancherorts eine gewisse Überforderung, auch vor dem Hintergrund personeller und finanzieller Ressourcen. Und ein bundesweit einheitlicher Sicherheitsstandard, wie es ihn für Autos, Spielplätze oder Dixi-Klos gibt? Fehlanzeige! In Sachen Cybersicherheit der kommunalen Verwaltung müssen wir flächendeckend ein höheres Level erreichen. Und zwar jetzt.

Die Zahlen sind eindeutig. In den vergangenen zwei Jahren ist die Anzahl der öffentlich bekannt gewordenen IT-Sicherheitsvorfälle bei Kommunen deutlich angestiegen. Das BSI warnt vor schwerwiegenden Cyberattacken auf Städte und Gemeinden, insbesondere aufgrund der geopolitischen Entwicklungen. Das treibt uns als kommunale IT-Dienstleister um. Ungern erinnere ich mich an die schweren Folgen der Cyberattacken gegen den Landkreis Anhalt-Bitterfeld. Oder an das Ausmaß des Angriffs auf den Dienstleister Südwestfalen-IT. Der Angriff wirkte sich auf 72 nordrhein-westfälische IT-Kommunen aus, die 2023 über Wochen keine Fahrzeuge zulassen, Geburten registrieren oder Pässe ausstellen konnten.

SENSIBILITÄT SCHÄRFEN

Gleichwohl scheint mir, dass die Gefahrensituation mitunter unterschätzt wird. So gibt laut Umfrage des Deutschen Städte- und Gemeindebundes (DStGB) etwa die Hälfte der Kommunen mit bis zu 100.000 Einwohnerinnen und Einwohnern an, dass sie auf Cyberangriffe gut vorbereitet seien und angemessen reagieren könnten. Aber spiegelt diese Einschätzung tatsächlich die Realität gerade in kleinen Verwaltungseinheiten wider? So schätzen fast 80 Prozent der kommunalen IT-Dienstleister – die wie kein zweiter Einblick in die Verwaltungspraxis haben – dass Kommunen mit bis zu 10.000 Einwohnerinnen und Einwohnern „viel zu schlecht“ im Bereich Cybersicherheit ausgestattet sind, für Städte zwischen 10.000 und 100.000 liegt der Anteil auch noch bei

30 Prozent. Zudem sagen 65 Prozent unserer Mitglieder, dass die politischen Entscheiderinnen und Entscheider auf kommunaler Ebene die Cybergefahren noch immer unterschätzen.

95 %

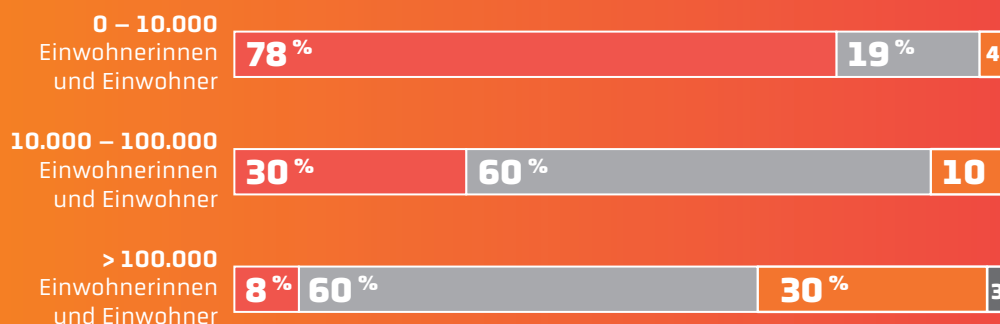
Laut 95 % der VITAKO Mitglieder hat das Risiko von IT-Sicherheitsvorfällen in den letzten fünf Jahren deutlich zugenommen.

BUND UND LÄNDER IN DIE VERANTWORTUNG NEHMEN

Dennoch bin ich weit davon entfernt, kleine Kommunen an den Pranger zu stellen. Die finanzielle Situation ist mitunter dramatisch. Und es wäre realitätsfremd, von Gemeinden mit vielleicht zwei oder drei Dutzend hauptamtlichen Verwaltungsmitarbeitenden zu erwarten, dass sie die Grundschutz-Zertifizierung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) auch nur ansatzweise stemmen könnten. Denn klar ist: Cybersicherheit umfassend zu garantieren ist mehr als das einmalige Einrichten einer Firewall. Es handelt sich zum Teil um hochkomplexe Aufgaben, deren Erfüllung dauerhaft zu gewährleisten ist – und viele Kommunen verständlicherweise überfordert.



■ Viel zu schlecht
 ■ Etwas zu schlecht
 ■ Genügend
 ■ Etwas zu gut



Kleinere Kommunen besonders gefährdet

„Wie sind die Kommunalverwaltungen im Bereich Cybersicherheit personell und finanziell ausgestattet?“

Quelle: VITAKO Umfrage unter den Mitgliedern, April 2025

Umso wichtiger, dass Bund und Länder ihrer Verantwortung gerecht werden und Städte und Gemeinden unterstützen. Konkret:

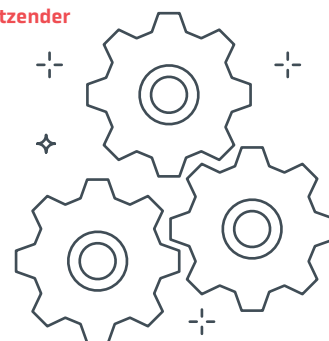
- **BSI-Support ermöglichen:** Das BSI ist in den vergangenen Jahren auf über 1.600 Mitarbeitende ausgebaut worden. Keine andere Behörde verfügt über ein ähnliches Know-how zu Cybersicherheit. Nach geltender Rechtslage darf es Kommunen in Krisenfällen aber nur kurzfristig unterstützen und muss ihnen sogar wichtige Sicherheitstools vorenthalten. Die Bundesregierung ist aufgefordert, die Behörde entsprechend des Koalitionsvertrages zur Zentralstelle auszubauen, so dass sie die Kommunen – die 80 Prozent der Verwaltungsleistungen stemmen – endlich angemessen unterstützen kann. Wenn das eine Grundgesetzänderung braucht, dann sollte man das dennoch ohne zu zögern angehen.
- **Interföderale Vernetzungs- und Unterstützungsstrukturen intensivieren:** Es gibt hervorragende Beispiele, wie einzelne Bundesländer ihren Kommunen konkrete Unterstützung bieten. Es entstehen Computer Emergency Response Teams (CERTS), Förderprogramme werden initiiert, zentrale Anlaufstellen auf Landesebene gegründet. Bundesländer, die bislang noch zurückhaltend sind, finden hier genug Best Practice Beispiele als Vorbilder – und müssen sie angehen.
- **Netz des Bundes leistungsfähiger machen:** Das Netz des Bundes (NdB) ist auf einzigartige Weise gegen Hackerangriffe gesichert. Hierüber werden hochsensible Daten zwischen den Bundesministerien ausgetauscht, und auch die Kommunen sind für vereinzelte Verfahren wie Kfz-Zulassung, Einbürgerung und Waffenregister angeschlossen. Es gilt, diese Infrastruktur für weitere Anwendungsfälle zu öffnen und gleichzeitig das hohe Sicherheitsniveau des NdB nicht zu gefährden.

- **Mindeststandards verbindlich einführen:** Es ist überfällig, dass für deutsche Kommunen einheitliche Mindeststandards verbindlich gelten. Ansatzpunkte für Kommunalverwaltungen gibt es vom BSI-Projekt „Weg in die Basis-Absicherung“ (WiBA) über das Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“ bis hin zu ISIS/CISIS12 zuhauf. VITAKO initiiert derzeit eine Arbeitsgruppe aus kommunalen Praktikern, die die vorhandenen Standards prüft und definiert, welche – gegebenenfalls differenziert nach Größe und IT-Arbeitsleistung der jeweiligen Kommune – zwingend eingehalten werden sollten. Wir gehen damit in Vorleistung und benötigen nach der Veröffentlichung politische Unterstützung auf allen Ebenen.

VITAKO treibt das Thema voran. Parallel arbeiten unsere Mitglieder daran, Kommunen noch besser auszurüsten, zu beraten und Mitarbeitende zu schulen – das Portfolio ist umfassend. Gemeinsam mit Politik und Verwaltung müssen wir alles daransetzen, Cybersicherheit der Verwaltungen zu stärken. Denn einen wirklich schweren Cyberangriff, der leicht das Ausmaß erreichen könnte, unser demokratisches Zusammenleben zu erschüttern, will wirklich niemand erleben.



**Sören Kuhn ist
Vorstandsvorsitzender
bei VITAKO.**



The Fortinet logo, featuring the word "FORTINET" in a bold, sans-serif font. The letter "O" is stylized with a red and white grid pattern.The Computacenter logo, consisting of a stylized circular icon with two dots inside, followed by the word "Computacenter" in a sans-serif font.

Menschen, Geräte und Daten schützen – überall.

Schwachstellen erkannt – und jetzt? Computacenter unterstützt gemeinsam mit Fortinet den öffentlichen Sektor dabei, Netzwerke, Cloud-Umgebungen, Endgeräte und Fachanwendungen gegen digitale Bedrohungen abzusichern.

Nutzen Sie den ProVitako-Rahmenvertrag und profitieren Sie von attraktiven Konditionen für die Fortinet-Produktpalette und umfassende Beratungsleistungen.

Wir sind gerne für Sie da:
kommunen.nrw@computacenter.com

DIGITALE BILDUNG BRAUCHT MODERNE IT – OHNE HÜRDEN.

Im Gespräch mit Frank Schöneberg, Vice President Sales Public & Healthcare bei CHG-MERIDIAN.

Herr Schöneberg, Sie sprechen regelmäßig mit Schulträgern und kommunalen IT-Dienstleistern. Was hören Sie aktuell am häufigsten?

Ich erlebe eine gewisse Ambivalenz: Der Wille zur Digitalisierung ist groß, aber viele Kommunen stehen unter Druck. Ressourcen sind knapp, Ausschreibungen aufwendig und oft müssen engagierte Lehrkräfte die IT nebenbei organisieren. Gesucht werden Lösungen, die im laufenden Schulbetrieb einfach funktionieren – und nicht nur auf dem Papier.

Was genau macht CHG-MERIDIAN – und warum ist Leasing für den öffentlichen Bereich so relevant?

Wir sind seit über 45 Jahren Finanzierungspartner für IT. Unsere Stärke im öffentlichen Sektor liegt vor allem in Bildung und Verwaltung. Ziel ist es, wirtschaftlich tragfähige Modelle für planbare, aktualisierbare IT so bereitzustellen, dass sie den Alltag der Nutzer:innen erleichtern. Die Geräte sind dabei nur Mittel zum Zweck: Es geht um funktionierende Strukturen, Standards und Lerninhalte im Bildungssektor – und darum, dass Schulträger handlungsfähig bleiben. Leasing ermöglicht moderne Technik ohne hohe Anfangsinvestitionen – wie in der freien Wirtschaft längst üblich.

Und wie funktioniert die Kooperation mit ProVitako?

Über den herstellerunabhängigen Rahmenvertrag können ProVitako-Mitglieder direkt auf unsere Leasingmodelle zugreifen – ohne eigene Ausschreibung.

Das vereinfacht die IT-Beschaffung erheblich, spart Zeit und reduziert den administrativen Aufwand. Gleichzeitig profitieren die Mitglieder von einem geprüften und verlässlichen Vertragswerk. ProVitako ist für uns ein strategischer Partner und ein Enabler für moderne kommunale Beschaffung.

Gibt es dafür Praxisbeispiele?

Absolut. Wir begleiten seit vielen Jahren Projekte im kommunalen Umfeld und sehen dabei immer wieder, wie viel Wirkung Leasing entfalten kann – besonders im Schulbereich. Ob bei wechselnden Klassenstärken oder beim Aktualisieren von Geräten: Früher wurde auf Vorrat gekauft oder teuer nachbeschafft. Heute können wir gemeinsam mit Schulträgern Geräte flexibel hinzufügen oder zurücknehmen – genau dann, wenn es gebraucht wird, ohne großen Verwaltungsaufwand.

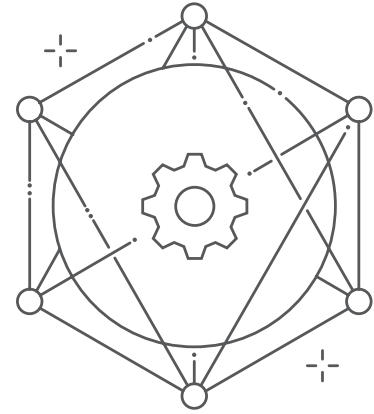
Was treibt Sie in Ihrer Arbeit an?

Ich finde es spannend, gemeinsam mit öffentlichen Auftraggebern praxistaugliche Lösungen zu finden; gerade dann, wenn es scheinbar kompliziert wird. Digitale Bildung braucht moderne IT – ohne Hürden. Wenn wir es schaffen, dass sich Kommunen stärker auf ihre eigentlichen Aufgaben konzentrieren können, haben wir einen guten Job gemacht.



Frank Schöneberg ist Vice President Sales Public & Healthcare bei CHG-MERIDIAN. Er begleitet öffentliche Auftraggeber seit über 30 Jahren.





DEUTSCHLAND-STACK: RÜCKGRAT EINER MODERNEN VERWALTUNG

Mit dem neuen Ministerium für Digitales und Staatsmodernisierung (BMDS) hat Digitalpolitik einen festen Umsetzungswillen bekommen: Digitalisierung, Staatsmodernisierung und Bürokratierückbau haben nun eine gebündelte, starke Stimme in der Bundesregierung. Als Parlamentarischer Staatssekretär beim Bundesminister für Digitales und Staatsmodernisierung, Karsten Wildberger, setze ich mich dafür ein, die Digitalisierung in Deutschland effektiver, schneller und bürgerfreundlicher umzusetzen. Dabei verfolge ich pragmatische Ansätze und bin bereit, den einen oder anderen „Häuserkampf“ zu führen. Mein Ziel ist es, durch die Wiederverwendbarkeit von Lösungen auf breiter Basis zu überzeugen.

Lassen Sie mich die Notwendigkeit mit Zahlen des Statistischen Bundesamtes verdeutlichen: In der Privatwirtschaft wird zu 98 Prozent digital kommuniziert, im öffentlichen Sektor jedoch erfolgt 58 Prozent der Kommunikation nach wie vor auf Papier.

Der Ausbau digitaler Infrastrukturen und die Reduzierung von Bürokratie durch schlanke Prozesse nach dem „Once-Only-Prinzip“ bilden die Grundlage für eine stärkere digitale Verwaltung. Dabei ist es entscheidend, Komplexität zu verringern und den richtigen Rahmen für die digitale Transformation zu setzen. Es braucht Lösungen, die auf verschiedenen Systemen funktionieren, damit Daten medienbruchfrei und digital ausgetauscht werden können.

DEUTSCHLAND-STACK ALS MEILENSTEIN

Mit dem Deutschland-Stack werden wir im BMDS ein Regal voller Standards und Softwarelösungen schaffen, die mehrfach verwendet werden, so dass eine gemeinsame IT-Architektur für die Verwaltung entsteht. Der Deutschland-Stack wird eine nationale souveräne Technologie-Plattform und damit Chancen eröffnen, digitale Infrastruktur auszubauen und Wachstum zu fördern. Dafür arbeiten wir an pragmatischen Digitalisierungsprozessen zum Nutzen für Bürger und Wirtschaft.

Konkret besteht der Deutschland-Stack aus

- einer einheitlichen Betriebs-Infrastruktur,
- aus Mechanismen zur standardisierten Bereitstellung und Pflege,
- aus Plattformen und Anwendungen mit nachnutzbarer Basis-IT sowie
- aus Schnittstellen und Integrations-Komponenten zur Realisierung der digitalpolitischen Vorhaben in Deutschland.

Der Deutschland-Stack wird Bund, Länder und Kommunen unterstützen, ihre Verwaltungsprozesse zu digitalisieren und effizienter zu gestalten. Durch die Bereitstellung standardisierter Bausteine können Kommunen ihre eigenen digitalen Lösungen schneller und kostengünstiger entwickeln. Dies fördert die Interoperabilität und Zusammenarbeit zwischen verschiedenen Verwaltungsebenen.

SCHRITTWEISE EINFÜHRUNG

Obwohl der Deutschland-Stack noch in der Entwicklung ist, zeigen unsere Zeitpläne eine klare Richtung. Wir setzen auf eine schrittweise Einführung bis 2028, um eine nachhaltige und effiziente digitale Verwaltung zu erreichen. Die Grundlage dafür ist die einheitliche Betriebsinfrastruktur sowie die standardisierte Bereitstellung und Pflege.

Wir werden Plattformen und Anwendungen auf dieser Infrastruktur betreiben, um vor allem die Nachnutzbarkeit durch die IT- und Digitalwirtschaft zu ermöglichen. Darüber hinaus schaffen wir Raum für neue Ideen und Geschäftsmodelle in der digitalen Transformation. Wir wollen nicht die bestehende Bürokratie digitalisieren, sondern neue, vorausschauende Lösungen für Städte und Kommunen schaffen – antragslos und effizient.

Der bestehende Dschungel an individuellen Schnittstellen muss reduziert werden. Wir werden bestehende Datenaustausch- und Kommunikationsstrukturen stärken. Dabei setzen wir auf die



„In Deutschland müssen wir das Rad nicht ständig neu erfinden, nicht jedes Ministerium oder jede Behörde muss seine eigenen Lösungen bauen. Mit dem Deutschland-Stack wollen wir Softwarelösungen für eine digitale Verwaltung bereitstellen, die auch von Ländern und Kommunen genutzt werden können, so dass eine gemeinsame IT-Architektur entsteht.“

Thomas Jarzombek, Parlamentarischer Staatssekretär
beim Bundesminister für Digitales und Staatsmodernisierung

Kompetenz der internen Dienstleister der öffentlichen Verwaltung, die technisches Fachwissen in die Praxis übersetzen.

KOMMUNEN ALS AUSGANGSPUNKT

Liebe Leserinnen und Leser, ich gehe davon aus, dass wir uns darüber einig sind, dass die meisten Dienstleistungen in den Kommunen erbracht werden. Daher ist es entscheidend, die Leistungsfähigkeit vor Ort zu erhöhen – nur was wirklich beim Bürger und in der Wirtschaft ankommt, ist echte Digitalisierung und schafft Vertrauen in den Staat.

Das Onlinezugangsgesetz war und ist ein erster Schritt. Aber wir stehen noch nicht da, wo wir sein wollen – auch da sind wir uns vermutlich einig. Derzeit erarbeiten wir mit den Bundesressorts, Onlinedienste gebündelt bereitzustellen. Hier greifen wir die Dresdner Forderungen und die Empfehlungen der Initiative für einen handlungsfähigen Staat auf.

Wir werden deshalb auch eine KI-Offensive starten. Auch in den Ländern werden bereits verschiedene KI-Initiativen vorangetrieben. Hier ist es entscheidend, dass wir unsere Strukturen so denken, dass wir bestmöglich Lösungen nachnutzen können.

Zentrales KI-Vorhaben der Bundesverwaltung ist die KI-Plattform des ITZBund (kurz: „KIPITZ“) als Basisplattform für LLMs und KI-Anwendungen. In der Weiterentwicklung soll im Rahmen des 100-Tage-Programms eine zentrale Bereitstellung ei-

ner KI-Plattform erfolgen, damit nach dem EfA-Prinzip alle Behörden über die gleichen KI-Anwendungen verfügen und diese leicht beziehen können.

KI: POTENZIALE HEBEN

KI hat das Potenzial, als transformative Technologie Prozesse neu zu gestalten. Deswegen haben wir im Koalitionsvertrag festgeschrieben, dass wir mit dem Staat als KI-Ankerkunden den KI-Standort Deutschland sowie Europa insgesamt stärken wollen.

Dabei setzen wir auf digital first, KI-unterstützte und automatisierte Prozesse. Mit einfachen, intuitiven und pragmatischen Lösungen wird das Vertrauen der Gesellschaft und Wirtschaft in einen digitalen Staat und digitale Prozesse erreicht werden.

Benötigte Unterlagen und Willenserklärungen müssen digital vorgelegt werden können. Wir wollen ein EUDI-Wallet-Ökosystem für Bürgerinnen und Bürger und Unternehmen schaffen, mit der Identifikation, Authentifizierung und Zahlungen ermöglicht werden. Dies werden wir bis Ende 2026 umsetzen. Dann werden wir unser Portemonnaie als digitalen Zwilling mitnehmen können – alles in einer App.

WENN DATEN ZUR BEUTE WERDEN: KOMMUNEN IM FADENKREUZ

Jede siebte Kommune in Deutschland war im vergangenen Jahr von Cyberattacken betroffen. Angesichts veralteter IT-Systeme und knapper Budgets sind Städte und Gemeinden oft leichte Beute für Cyberkriminelle. Von der Cloud-Migration bis zum 24/7-Sicherheitsmonitoring stellt die AKDB sicher, dass Kommunen der Bedrohung durch Cyberangriffe proaktiv begegnen können.

Die zunehmende Komplexität und Dynamik der Bedrohungslage für kommunale IT-Infrastrukturen stellt Städte und Gemeinden vor erhebliche Herausforderungen. Angriffe wie Ransomware, Phishing und Social Engineering sind an der Tagesordnung und gefährden die reibungslose Funktion der öffentlichen Verwaltung. Der Vorfall bei Südwestfalen-IT im Jahr 2023 verdeutlicht, wie schwerwiegend die Auswirkungen von Cyberangriffen sein können. Der Betrieb von 72 kommunalen Verwaltungen in Nordrhein-Westfalen kam teilweise wochenlang zum Erliegen, was massive Folgen für Bürger und Unternehmen nach sich zog.

ENDPOINT SECURITY VERSTÄRKEN

Kommunen sind aus Sicht von Cyberkriminellen attraktive Ziele. Um sich zu schützen, müssen Kommunen dringend ihre Cyberresilienz erhöhen. Schulungen zur Sensibilisierung für Phishing sowie die Entwicklung von Notfallplänen sind essenziell. Auch die Erstellung eines Informationssicherheitskonzepts oder das Schwachstellenmanagement sind wichtig. Zudem sollten Sicherheitsmechanismen wie Endpoint Security und aktuelle Virens Scanner implementiert werden.

FACHVERFAHREN IN DIE CLOUD

Um Kommunen beim Aufbau einer robusten Sicherheitsarchitektur zu unterstützen, bietet die AKDB umfassende Services. Durch die Migration in die AKDB Cloud kann kommunale Software effizienter gemanagt und geschützt werden. LivingData, eine Tochter der AKDB, übernimmt als Managed Security Service Provider außerdem die Verantwortung für Sicherheitspatches, Updates und das Monitoring von Cybergefahren. Das rund um

die Uhr besetzte Security Operations Center entlastet die IT-Admins in den Kommunen erheblich und trägt zur Erhöhung der Cyberresilienz bei.

IT-BETRIEB OUTSOURCEN ALS LÖSUNG

Der Freistaat Bayern umfasst viele kleinere Kommunen, die mit begrenzten Ressourcen umgehen müssen. Hier setzt die AKDB an und bietet Dienstleistungen wie Notfallmanagement und IT-Outsourcing. Besonders das Outsourcing-Angebot NextGO wird zunehmend gefragt, denn Kommunen erkennen, dass die Verantwortung für Cybersicherheit keine Option, sondern eine Notwendigkeit ist. Die AKDB-Gruppe hat ihr Portfolio entsprechend aufgestellt, um Kommunen für die wachsenden Herausforderungen der Cybersicherheit zu wappnen.



MEHR DAZU UNTER

www.akdb.de/loesungen/cloud-services



CYBERANGRIFFE

KOMMUNEN KÖNNEN SICH HILFE HOLEN



„Kommunen machen Daseinsfürsorge. Fallen ihre Services aus, untergräbt das letztlich das Vertrauen in den Staat – das können wir uns nicht leisten.“

Stefanie Euler, BSI

Kommunen müssen sich gegen Cyberangriffe schützen. Ihre Verantwortung beim Thema ist enorm, denn sie verwalten Millionen teils hochsensibler Daten, ihre Services sind mitunter lebensnotwendig. Gerade für kleinere und finanzschwache Kommunen ist IT-Sicherheit auf hohem Niveau aber oft kaum leistbar. Welche Hilfen und Anlaufstellen es gibt, berichten Marco Dörfler und Philipp Schneider von den kommunalen IT-Dienstleistern AKDB und ekom21 sowie Stefanie Euler vom Bundesamt für Sicherheit in der Informationstechnik (BSI).

2021: Anhalt Bitterfeld; 2022: Rhein-Pfalz-Kreis; 2023: gut 72 Kommunen in Nordrhein-Westfalen. Cyberangriffe mit massiven Folgen für Kommunen sind bittere Realität. Das BSI geht von durchschnittlich zwei erfolgreichen Attacken im Monat aus. Die genaue Zahl: unbekannt. Denn ein einheitliches Lagebild gibt es bis dato nicht. Kommunen sind nicht verpflichtet, Angriffe zentral zu melden. „Wir können daher nur auf Grundlage öffentlich verfügbarer Informationen schätzen. Die Dunkelziffer liegt

vermutlich höher“, sagt Stefanie Euler. Die Expertin arbeitet seit 20 Jahren beim BSI und ist dort seit 2020 als Referatsleiterin für die Beratung von Ländern und Kommunen zuständig.

Sie spricht von einer steigenden Gefährdungslage. Kommunen seien attraktive Ziele für internationale Cyberkriminelle, die Angriffe würden ausgefeilter, KI eröffne den Tätern neue Möglichkeiten. Hinzu kämen geopolitische Risiken. Zugleich sei die Ressourcenlage in vielen Kommu-

nen immer noch zu schlecht, „auch wenn ich wahrnehme, dass das Bewusstsein wächst.“ Sie bemängelt vor allem das heterogene Bild. Auf der einen Seite gäbe es gut aufgestellte Kommunen mit BSI-IT-Grundschutz-Zertifizierung, auf der anderen Seite aber auch solche, die gerade mal einen Virenschutz installiert haben. „Das ist gefährlich“, sagt sie. „Kommunen machen Daseinsfürsorge. Fallen ihre IT-Systeme aus, können Anträge nicht beantragt, wichtige Sozialleistungen nicht ausgezahlt werden. Das untergräbt letztlich das Vertrauen in den Staat – das können wir uns gerade in den aktuellen Zeiten nicht leisten.“

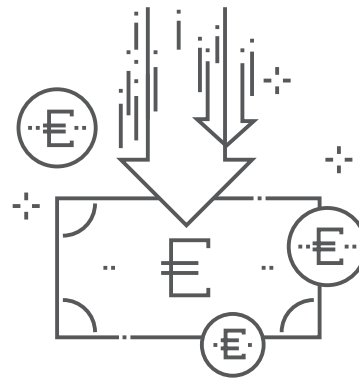
KOMMUNALE IT-DIENSTLEISTER HELFEN

Marco Dörfler kennt die Sorgen und Nöte vor Ort gut. Er ist beim bayerischen IT-Dienstleister AKDB für IT-Sicherheit zuständig. „Das Thema ist in den Verwaltungen auf jeden Fall präsent. Aber gerade den kleineren Kommunen fehlen Fachkräfte und Geld“, sagt er. „Cybersicherheit ist ja auch nichts, was man

einmal macht, und dann passt es. Im Gegenteil.“ Kommunen müssten laufend nachjustieren und sich auf neue Bedrohungen einstellen, Mitarbeitende nachschulen, mehrmals im Jahr Übungen abhalten. Es sei viel Aufwand, ständig auf dem Laufenden zu bleiben.

Dabei fehlt es den Kommunen in Deutschland zunehmend an Geld. Im Jahr 2024 haben sie ein neues Rekorddefizit von mehr als 24 Milliarden Euro eingefahren – gut 18 Milliarden mehr als im Jahr zuvor. Die Ursachen sind struktureller Art: steigende Sozialausgaben etwa durch die Erhöhung der Regelsätze bei Sozialhilfe und Bürgergeld, explodierende Kosten für die Kinder- und Jugendhilfe sowie wachsende Personalkosten. Bei mehr oder weniger stagnierenden Einnahmen. Zugleich müssen die Kommunen investieren, in Infrastruktur, in Kitas und Schulen, in die Digitalisierung ihrer Verwaltungstätigkeit – und natürlich in Cybersicherheit als einem wesentlichen Teil davon.

Kommunale IT-Dienstleister wie die AKDB können Kommunen hier zumindest teilweise entlasten. Marco Dörfler: „Wir bündeln Know-how, schaffen Synergien und nehmen den Kommunen damit konkret Arbeit ab.“ So übernimmt die AKDB etwa das IT-



-24 Mrd. €

**2024 HABEN KOMMUNEN
EIN NEUES REKORDDEFIZIT
EINGEFAHREN**

Outsourcing und ermöglicht seinen Kunden eine moderne, kosteneffiziente Infrastruktur. Die Fachleute setzen technologische Sicherheits-Basics um und sensibilisieren die Mitarbeitenden. „Die meisten Attacken kommen über Phishing, also gefälschte E-Mails scheinbar vertrauenswürdiger Absender. Wir schulen Mitarbeiterinnen und Mitarbeiter darin, Fälschungen zu erkennen und zu melden.“



Prosoz-Formularlösungen

**Realisieren Sie Online-Services mit
digitalem Mehrwert für Ihre Verwaltung.**

- Schlüsselfertige Online-Formulare für zahlreiche Antragsanlässe
- Umfassendes Formularmanagement bis zu individueller Formularerstellung und -hosting
- Datenübernahme aus Online-Anträgen in die Prosoz-Fachverfahren inkl. begleitender Dokumente

Besuchen Sie uns auf der SCON

30.09. - 02.10. | hub27 | 406 | VITAKO Gemeinschaftsstand



prosoz.de/
ende-zu-ende-digitalisierung

Prosoz

Digitale Transformation.
Einfach machen.



„Eine Kommune kann noch so gut abgesichert sein, eine 100-prozentige Garantie gibt es leider nicht.“

Philipp Schneider, ekom21

UNTERSTÜTZUNG AUF LANDESEBENE

Kommunen sowie auch die AKDB holen sich dabei Unterstützung von externen Dienstleistern, die auf Forensik oder eine 24/7-Überwachung der IT-Systeme spezialisiert sind. Eine weitere Anlaufstelle ist das Landesamt für Sicherheit in der Informationstechnik (LSI). Das LSI unterstützt bayerische Kommunen beim Thema IT-Sicherheit und wurde 2017 als bundesweit erste Einrichtung dieser Art gegründet. Angebote wie Infoveranstaltungen, Beratungen oder E-Learning-Kurse stehen Kommunen kostenfrei zur Verfügung. Marco Dörfler: „Wir kooperieren mit dem LSI vor allem beim Thema Monitoring von Schwachstellen und stehen regelmäßig im Austausch, etwa zu Verdachtsfällen.“

Sprung von Bayern nach Hessen. Beim kommunalen IT-Dienstleister ekom21 leitet Philipp Schneider das Team KDLZ-CS. Die komplizierte Abkürzung steht für Kommunales Dienstleistungszentrum für Cybersicherheit. Die Besonderheit: Das Zentrum wurde 2016 mit Fördermitteln des Landes Hessen gegründet. Mit jährlich 1,5 Millionen Euro unterstützt das Land im Rahmen des „Aktionsprogramms Kommunale Cybersicherheit“ Kommunen dabei, ihre IT-Sicherheit zu stärken. Die Umsetzung übernimmt die ekom21. Philipp Schneider: „Das Angebot ist deutschlandweit einzigartig. Andere Bundesländer unterstützen Kommunen punktuell, aber so eine umfangreiche Hilfe gibt es sonst nirgends.“

Die Angebote des KDLZ-CS sind vielfältig. Das Team checkt etwa den Zustand der IT-Sicherheit in Kommunen gemäß BSI Grundschutz-Profil, empfiehlt darauf aufbauend Maßnahmen und berät zur konkreten Umsetzung. „Wir wollen in erster Linie ein Vertrauensverhältnis aufbauen und gemeinsam schauen, wo sich eine Kommune noch verbessern kann.“ Nach einem Jahr werden die Resultate überprüft, etwa im Rahmen von Penetrationstests, die eine Cyberattacke simulieren. Flankiert wird das Angebot von E-Learning-Kursen sowie Live-Veranstaltungen zur Mitarbeitersensibilisierung. Alles komplett kostenfrei für die Kommunen.

GEWAPPNET FÜR DEN ERNSTFALL

Hat eine Kommune das Programm durchlaufen und ihr Sicherheitsniveau verbessert, kann sie an einem kostenfreien BCM-Workshop teilnehmen. BCM – ausgeschrieben: Business Continuity Management – bereitet Kommunen auf den Ernstfall vor. Philipp Schneider: „Eine Kommune kann noch so gut abgesichert sein, eine 100-prozentige Garantie gibt es leider nicht. Dann ist es entscheidend, ob eine Verwaltung auch hier ihre Hausaufgaben gemacht hat.“ Notfallpläne erstellen, Verantwortlichkeiten festlegen, analoge Listen mit Kontaktnummern hinterlegen, separate Kommunikationswege vordenken, die wichtigsten Dienstleistungen über Nachbarkommunen abdecken – viel zu tun, aber machbar, so Philipp Schneider. Besonderes Plus: Kommunen, die Maßnahmen konkret umgesetzt haben, können im Krisenfall fünf Tage lang kostenlos einen externen Incident Response Service in Anspruch nehmen. Der Dienstleister hilft dann, befallene Systeme wieder sicher zu machen und Prozesse wiederherzustellen.

„Die ekom21 ist bislang der einzige kommunale Dienstleister in Deutschland, der so eine umfangreiche Vorbereitung auf den Notfall und eine Krisenhilfe abdecken kann“, sagt Philipp Schneider. „Dank der Fördermittel war es möglich, das in den letzten drei Jahren intern aufzubauen und den Kommunen zur Verfügung zu stellen.“ Das Interesse ist groß: Von den über 420 Gemeinden, Städten und 21 Landkreisen in Hessen haben bereits gut 300 Kommunen geförderte Leistungen in Anspruch genommen.

Das Interesse wundert nicht. Mehrere Angriffe auf Kommunen haben gezeigt, wie wichtig Prävention und Vorbereitung sind. Und welche Konsequenzen drohen, wenn die Gefahren ignoriert werden. So musste 2021 der Landkreis Anhalt-Bitterfeld aufgrund eines Ransomware-Angriffs den Katastrophenfall ausrufen, persönliche Daten von Kreistagsmitgliedern landeten im Darknet, die Verwaltung war über Monaten lahmgelegt, Kostenpunkt rund zwei Millionen Euro. Ein Jahr später fand sich die Landeshauptstadt Potsdam auf der Liste einer internationalen Hacker-Bande wieder. Vorsorglich schaltete die Stadt ihre Systeme ab, holte Mitarbeitende aus dem Urlaub, engagierte ein global aufgestelltes Forensik-Unternehmen, das die IT-Systeme prüfte. An-

ders als Anhalt-Bitterfeld hatte Potsdam zuvor Vorkehrungen getroffen. Eine Priorisierungsliste der wichtigsten Bürgerservices, ein Bypass bei der Sparkasse für die Auszahlung von Geldern und Kooperationen mit Nachbargemeinden verhinderten einen Komplettausfall, nach einigen Wochen lief alles wieder. Dennoch: 2,3 Millionen Euro an Kosten für Forensiker und neue Sicherheitsmaßnahmen.



2,3 Mio. €

**KOSTEN FÜR FORENSIKER
UND NEUE SICHERHEITS-
MASSNAHMEN IN POTSDAM**

KEEP GOING!

SMART COUNTRY CONVENTION

hub27, Stand 603
Besuchen Sie uns!

Treffpunkt Berlin

Neue Lösungen rund um E-Government, Smart City und nachhaltige Mobilität: Dieses Jahr präsentieren wir Ihnen eine souveräne Chatplattform auf LLM-Basis, MobilityGPT, Energiemonitoring sowie smarte Apps und Touchpoints für Ihre Serviceportale. Sehen wir uns in Berlin?



MEHR ERFAHREN

vertrieb@regioit.de www.regioit.de



nextgov IT

regio IT

**„Das Thema
IT-Sicherheit bleibt
permanent wichtig.
Man muss immer
wieder eine Schippe
drauflegen.“**

Marco Dörfler, AKDB



Allen Betroffenen ist gemein: Nach einem Vorfall wird das Thema endlich ernst genommen. Kommunale IT-Dienstleister sind dann ideale Partner. Auch Stefanie Euler vom BSI unterstreicht die Bedeutung: „Gerade für kleinere oder finanzschwache Kommunen ist das Know-how der Dienstleister wertvoll. Man muss ja nicht 11.000 Mal das Rad neu erfinden, sondern kann auf vorhandene Strukturen und Ressourcen zurückgreifen.“ In ihrer Rolle beim BSI organisiert sie Informationsveranstaltungen, erstellt Handreichungen und berät bei Fragen. Ihrer Arbeit sind allerdings Grenzen gesetzt, rein rechtlich. „Die Kommunen sind Ländersache. Als Bundesbehörde dürfen wir daher nur sehr punktuell tätig werden.“ Vieles laufe daher in Kooperation mit den Bundesländern. Jüngst etwa eine Online-Roadshow für Kommunen: Das Land lädt ein und gemeinsam wird die Agenda erstellt. Themen sind etwa der Einstieg in die IT-Sicherheit oder Krisenmanagement. Stefanie Euler hält es für besonders wichtig, dass die Länder ihr Engagement ausbauen. Siehe das KDLZ-CS in Hessen. Siehe das LSI in Bayern.

LUFT NACH OBEN

Eines ist klar: Im Thema ist Bewegung. Immer mehr Länder schaffen Angebote für Kommunen, das Bewusstsein in den Verwaltungen wächst, und auch die kommunalen IT-Dienstleister rüsten weiter auf. So will die AKDB in Bayern perspektivisch auch im Ernstfall noch mehr Unterstützung bieten durch das AKDB 360 Grad Lösungskonzept für die digitale Verwaltung. Marco Dörfler: „Die Nachfrage ist da und steigt. Dazu trägt auch der Fachkräftemangel bei. Viele Kommunen haben gar nicht mehr das Personal, IT-Sicherheit inhouse abzudecken.“ Die Angebote von Dienstleistern wie der AKDB oder ekom21 bündeln Ressourcen und schaffen dringend notwendige Synergien.

Aber es ist noch Luft nach oben, darin sind sich die Fachleute einig. „IT-Sicherheit ist teuer, aber es ist nicht allein eine Frage des Geldes“, so Philipp Schneider von der ekom21. „Man muss auch die Prioritäten richtig setzen. Sicherheit muss zur Chefsache werden.“ Stefanie Euler fügt an: „Nach wie vor fehlt eine gesetzliche Vorgabe, dass Kommunen IT-Sicherheit umsetzen müssen. In der EU-Richtlinie NIS2 wäre die Chance dazu dagewesen, aber die Kommunen wurden letztlich rausgenommen. Wir finden das sehr bedauerlich.“

Sie verweist zudem auf das Thema Standards. Deutschlandweit seien Tausende Fachverfahren im Einsatz, Schnittstellen sind oft nicht einheitlich geregelt, ebenso wenig Sicherheitsvorgaben. „Gemeinsame Standards würden das Sicherheitsniveau insgesamt erhöhen und wären für die Kommunen eine erhebliche Erleichterung“, so die BSI-Expertin. „Bei dem Thema sind wir derzeit sehr aktiv und sprechen regelmäßig mit Multiplikatoren, etwa VITAKO oder auch govdigital.“ Auch Marco Dörfler und Philipp Schneider betonen die Bedeutung von Netzwerken wie govdigital. Die Genossenschaft bündelt Angebote von IT-Dienstleistern und stellt sie deutschlandweit zur Verfügung. So können die BCM-Schulungen der ekom21 über den Marktplatz von govdigital von IT-Dienstleistern und Kommunen aus ganz Deutschland erworben werden – Wissenstransfer at its best.

„Das Thema Informationssicherheit bleibt permanent wichtig“, konstatiert Marco Dörfler. „Man muss immer wieder eine Schippe drauflegen.“ Das sei für ihn aber auch das Faszinierende daran – und die Herausforderung, die ihn jeden Tag von neuem antreibt. „Wir sind stolz darauf, an diesem Thema aktiv arbeiten zu dürfen. Im Fokus steht die Vermeidung von Sicherheitsvorfällen.“

KOMMUNALE IT – INFRASTRUKTUREN IM WANDEL

Die kommunale IT steht vor großen Herausforderungen. Der Mangel an IT-Fachkräften verschärft sich weiter: Bis 2030 könnten im öffentlichen Dienst rund 140.000 IT-Spezialistinnen und -Spezialisten fehlen – besonders in Kommunen, wo die Lücke laut Schätzungen bis zu 26 Prozent betragen kann. Dadurch wird es für Kommunen immer schwieriger, ihre IT-Systeme eigenständig zu betreiben und weiterzuentwickeln.

Gleichzeitig steigt der Digitalisierungsdruck. Bürgerinnen und Bürger sowie Unternehmen erwarten digitale Verwaltungsdienstleistungen. Moderne Fachverfahren und digitale Prozesse sind zunehmend unerlässlich. Besonders wichtig ist die Registermodernisierung – etwa durch das Once-Only-Prinzip, bei dem Daten nur einmal erfasst und verwaltungsübergreifend genutzt werden.

INNOVATIONSMOTOR CLOUD

Vor diesem Hintergrund gewinnen zentrale Cloud-Lösungen und Software-as-

140 Tsd.
IT-Spezialistinnen
und -Spezialisten
fehlen bis 2030

a-Service (SaaS) an Bedeutung. Mit dem Start der Deutschen Verwaltungswolke (DVC) 2025 entsteht eine zentrale Plattform für digitale Verwaltungsdienste, die standardisierte Cloud-Services für Bund, Länder und Kommunen bereitstellt. Die Vorteile: Kosteneinsparungen, Skalierbarkeit, automatische Updates und höhere

IT-Sicherheit. Gleichzeitig entlastet das Modell den öffentlichen Dienst personell – Betrieb und Wartung werden ausgelagert, wodurch der Fachkräftemangel gezielt abgefedert werden kann.

ZUSAMMENARBEIT STÄRKEN

Die Modernisierung gelingt nur in enger Zusammenarbeit mit Bund und Ländern. Der Bund unterstützt bei der Umsetzung der DVC, der Registermodernisierung und der Standardisierung von Fachverfahren. Eine enge Abstimmung ist essenziell, um eine einheitliche, sichere und zukunftsfähige IT-Infrastruktur zu schaffen. Ein besonderer Fokus liegt dabei auf der IT-Sicherheit. Während Kommunen bei der IT-Selbstverwaltung eigenständig für Schutz, Updates und Compliance verantwortlich sind, übernehmen dies im SaaS-Modell die Anbieter. Vorteile sind die Reduzierung von Risiken durch moderne Sicherheitsinfrastrukturen, regelmäßige Wartung, schnelle Reaktion auf Bedrohungen und zertifizierte Rechenzentren. Letztere müssen Standards wie ISO 27001 oder den BSI IT-Grundschutz sowie rechtliche Anforderungen wie die DSGVO erfüllen.

FIT FÜR DIE ZUKUNFT

Die kommunale IT steht vor einer tiefgreifenden Transformation. Der Druck durch Fachkräftemangel und Digitalisierung führt zu einem Wandel hin zu zentralen, cloudbasierten Lösungen. Mit Unterstützung des Bundes und Nutzung von SaaS-Modellen sind die Weichen für eine leistungsfähige, resiliente und sichere Verwaltung der Zukunft gestellt.



Oskar Rzepinski ist
Leiter IT-Betrieb
Software-as-a-Service
(SaaS) bei PROSOZ
Herten GmbH.



Tobias Kippert ist
Informationssicher-
heitsbeauftragter bei
PROSOZ Herten GmbH.

CYBERSICHERHEIT AUF KOMMUNALER EBENE – UNVERZICHTBAR FÜR DAS ZUSAMMENLEBEN IN DEUTSCHLAND

Die Digitalisierung eröffnet enorme Chancen für Wachstum, Fortschritt und Teilhabe. Zugleich wächst die Verletzlichkeit unserer Gesellschaft, die Abhängigkeit von technischen Systemen und Prozessen nimmt zu, und neue Angriffsflächen entstehen. Neue Technologien spielen diesen Angreifern in die Hände. Cyberkriminalität ist mittlerweile ein Geschäftsmodell, in dem arbeitsteilige Vorgehensweisen durch spezialisierte Tätergruppen fest etabliert sind. Zudem verschwimmen die Grenzen zwischen staatlichen und nicht-staatlichen Akteuren. Angesichts der angespannten geopolitischen Lage sind der Erfolg der Digitalisierung und unsere nationale Sicherheit untrennbar miteinander verbunden. Cybersicherheit ist daher eine unverzichtbare Voraussetzung für das Zusammenleben und -arbeiten in unserem Land.

KOMMUNEN BESONDERS GEFORDERT

Dies gilt auch und gerade für die Digitalisierung der Verwaltung. Den Kommunen als erste und vorrangige Anlaufstelle des Bürgers, in denen ein Großteil der Verwaltungsvorgänge abgewickelt werden, kommt hierbei eine entscheidende Rolle zu. Gerade die Kommunen stehen vor besonderen Herausforderungen angesichts knapper finanzieller, personeller und fachlicher Ressourcen.

Aufgabe des Bundesministeriums des Innern ist es, die Sicherheit im digitalen Raum nicht dem Zufall zu überlassen. Hierzu zählt, für angemessene Rahmenbedingungen zu sorgen, die die Gewährleistung von Cybersicherheit ermöglichen. Insbesondere das BSI-Gesetz bietet einen effizienten Rechtsrahmen, der, wo

nötig, Anforderungen klar festlegt, Rechtssicherheit schafft und Anreize, Verfahren und Hilfestellungen für die Gewährleistung von Cybersicherheit bietet.

BSI ALS ZENTRALER AKTEUR

Mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) besteht auf Bundesebene ein starker zentraler Akteur für die Cybersicherheit, der neben der Sicherheit der Behörden des Bundes Kritische Infrastrukturen und einen – mit der anstehen-

den NIS-2-Richtlinien-Umsetzung dann noch signifikant vergrößerten – Kreis wichtiger Unternehmen speziell in den Blick nimmt. Auch kommunale Einrichtungen können hiervon erfasst werden. Mit Zuständigkeiten im Bereich der Akkreditierung und Produktsicherheit sowie der Information und Warnung erreicht das BSI ferner einen breiten Kreis von Nutzern aus Staat, Wirtschaft und Gesellschaft.

Unsere föderale Struktur bildet sich auch im Bereich der Cybersicherheit ab. Der Zusammenarbeit zwischen Bund und Ländern sind verfassungsrechtliche Grenzen gesetzt. Gleichwohl werden wir die Zusammenarbeit von Bund und Ländern im Rahmen des Möglichen weiter vertiefen. Der Spielraum des Bundes zur Unterstützung der Kommunen bleibt aber eingeschränkt, grundsätzlich liegt die

Zuständigkeit bei den Ländern. Innerhalb des durch das Grundgesetz vorgegebenen Rahmens kann der Bund – auch mittelbar und gemeinsam mit den Ländern – zur Unterstützung der Kommunen im Bereich Cybersicherheit beitragen. Wo dies möglich ist, geschieht dies auch.

„Innerhalb des durch das Grundgesetz vorgegebenen Rahmens kann der Bund – auch mittelbar und gemeinsam mit den Ländern – zur Unterstützung der Kommunen im Bereich Cybersicherheit beitragen. Wo dies möglich ist, geschieht dies auch.“

Friederike Dahns



Im BSI wurden die Zusammenarbeitsstrukturen mit den Zielgruppen Länder und Kommunen in den letzten Jahren bereits ausgebaut. Dabei wird die Zusammenarbeit des BSI mit den Ländern durch bilaterale Kooperationsvereinbarungen jeweils näher strukturiert. In diesem Rahmen finden jeweils auf verschiedenen Ebenen – zum Beispiel mit Multiplikatoren, in Gremien und durch zielgruppenspezifische regionale Formate – Umsetzungsberatungen, Wissenschaftstransfer und Austausch statt.

UNTERSTÜTZUNG FÜR KOMMUNEN

Kommunen bietet das BSI zudem zahlreiche Hilfestellungen, die praxisnah und skalierbar aufeinander aufbauen und ineinandergreifen, zum Beispiel:

- Um den Start in die IT-Sicherheit zu erleichtern, hat das BSI das Projekt „Weg in die Basis-Absicherung“ als niedrigschwelligen Einstieg in den IT-Grundschutz initiiert. Damit werden insbesondere kleinere Kommunen adressiert, bei denen nötige Ressourcen und Know-how für eine Umsetzung von IT-Sicherheitsmaßnahmen knapp sind. Themenspezifische Checklisten und ergänzende Informationen führen durch die für die Cybersicherheit relevanten Bereiche, wie beispielsweise die Erstellung von Back-ups, mobiles Arbeiten, Serverräume und -systeme oder die Vorbereitung auf Sicherheitsvorfälle.
- Speziell für Kommunen wurden IT-Grundschutzprofile zu konkreten Anwendungsfällen erstellt, die das BSI begleitet hat und auf den eigenen Webseiten zur Verfügung stellt. Hierzu zählt auch das IT-Grundschutz-Profil „Basisabsicherung Kommunalverwaltung“, das generelle Schutzmaßnahmen für zentrale Objekte der Kommunalverwaltung adressiert und mit Vertretern der kommunalen Ebene erarbeitet wurde. Ziel ist es, das Sicherheitsniveau in der Breite anzuheben. Adressaten sind Kommunen, die systematisch Vorkehrungen zur IT-Sicherheit treffen möchten. Weitere Maßnahmen, dann orientiert am Stand der Technik, können auf die Basisabsicherung aufsetzen.

Darüber hinaus stellt das BSI eine Reihe weiterer, auch niedrigschwelliger Arbeitshilfen, Handlungsempfehlungen und Vorlagen online abrufbar bereit, die im kommunalen Bereich genutzt werden können. Als zentralen Anlaufpunkt für Fragen und Anregungen zu Informationssicherheit und Arbeitshilfen hat das BSI hierfür ein spezielles Funktionspostfach eingerichtet.

Um der übergreifenden Gefährdungslage effektiv begegnen zu können, werden Bund und Länder auch weiterhin – und zukünftig eher noch stärker – darauf setzen, auf Augenhöhe und eng verzahnt miteinander zu agieren. Dies schließt die Cybersicherheit auf Ebene der Kommunen zwingend mit ein.



Friederike Dahns
ist Abteilungsleiterin
Cyber- und Informations-
sicherheit im
Bundesministerium
des Innern.

Mehr Informationen unter:
bit.ly/va03-25-bsi



„CYBERSICHERHEIT MUSS CHEFSACHE SEIN“

Das Frankfurter cyberintelligence.institute (CII) hat das IT-Sicherheitsniveau in Kommunen auf den Prüfstand gestellt – und bescheinigt erheblichen Verbesserungsbedarf. Dr. Michael Littger, Strategiedirektor des Instituts, und Dr. Tilmann Dittrich, Rechtsanwalt und Co-Autor der Studie, sehen die Kommunen in der Verantwortung, Maßnahmen zu ergreifen.

Was hat Sie dazu gebracht, die Studie durchzuführen?

Dr. Tilmann Dittrich: Wir haben einfach die Brisanz der Lage in den Kommunen gesehen. Laut BSI sind jeden Monat durchschnittlich zwei Kommunen von Ransomware-Angriffen betroffen – das ist zu viel. Kommunen sind heute eines der Hauptangriffsziele internationaler Cybergruppierungen, da haben wir keine Zeit zu verlieren.

Sie sehen eine hohe kommunale Eigenverantwortung. Weshalb?

Dr. Michael Littger: Es geht uns darum, die Kommunen zu unterstützen. Bei den strukturellen Problemen sehen wir auch den Bund in einer Bringschuld. Hier geht es um Geschwindigkeit. Kommunen können nicht auf langwierige Prozesse warten. Und es gibt viele Maßnahmen, die Kommunen schnell und relativ unkompliziert umsetzen können.

Können Sie Beispiele nennen?

Littger: Erstens: Cybersicherheit zur Chefsache machen. Die Leitungsebene muss die Ernsthaftigkeit des Themas erkennen, Strategien entwickeln und Mittel bereitstellen. Es würde auch niemand auf die Idee kommen, die Finanzverantwortung der Buchhaltung zu überlassen. Zweitens: Jede Kommune braucht einen kommunalen Chief Information Security Officer (CISO). Die Leitungsebene kann das Thema weder fachlich noch zeitlich allein stemmen. Ein CISO bündelt Know-how, berät die Führungsebene und setzt Impulse – etwa durch Schulungen oder eLearning-Programme für Mitarbeitende.

„Die Leitungsebene muss die Ernsthaftigkeit des Themas erkennen.“

Dr. Michael Littger

Dittrich: Was uns zu einem dritten Punkt führt: Kommunen müssen sich auf den Ernstfall vorbereiten. Notfallkonzepte dürfen nicht erst dann entwickelt werden, wenn es schon zu spät ist, sondern müssen im Vorfeld stehen. Und dann heißt es: Üben. Alle Mitarbeitenden sollten im Ernstfall wissen: Was sind die ersten Schritte bei einem Angriff? Wer muss informiert werden? Was wird kommuniziert? Cybersicherheit muss so selbstver-

ständlich geübt werden wie der Feueralarm in der Schule. Diese Vorbereitung hat übrigens auch einen wichtigen psychologischen Effekt: Wenn Mitarbeitende sich nicht hilflos fühlen, steigt ihr Interesse am Thema. Das erzeugt eine positive Lernspirale.

Welche Rolle spielt dabei die kommunale IT?

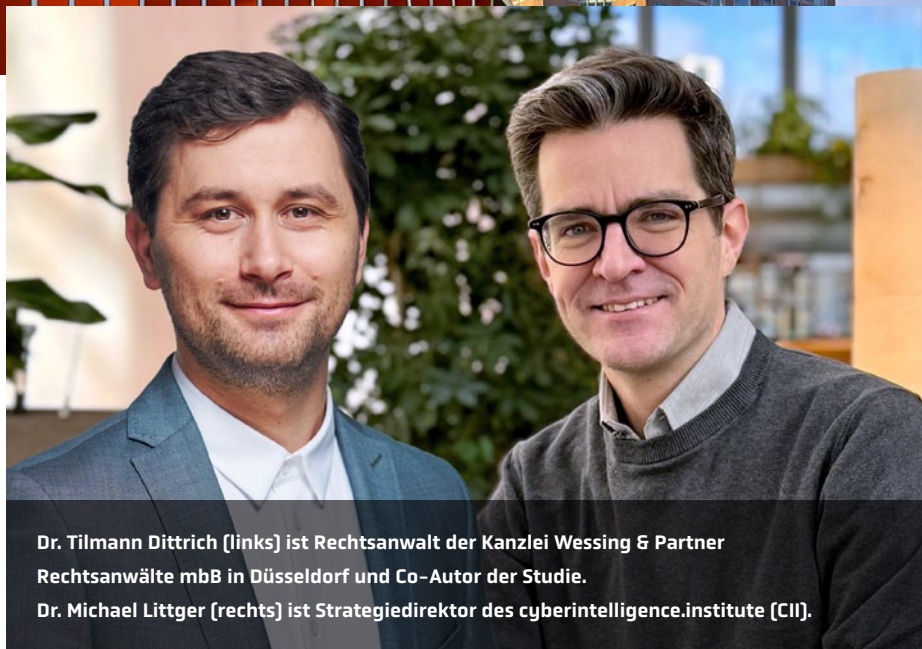
Dittrich: Eine sehr wichtige. Die IT-Dienstleister verfügen über einen breiten Wissens- und Erfahrungsschatz. Sie kennen die aktuelle Gefahrenlage, aber auch

die Situation vor Ort in den Städten und Gemeinden. Sie begleiten regelmäßig Angriffe und wissen um typische Schwachstellen und adäquate Reaktionen. Dadurch bieten sie ein höheres Sicherheitsniveau als eine Kommune selbst es je leisten könnte. Aber natürlich sind auch die IT-Dienstleister nicht vor Angriffen gefeit. Absolute Sicherheit gibt es leider nicht.

Was fordern Sie von der Politik?

Littger: Wir brauchen klare Zuständigkeiten und weniger Regelungswirrwarr. Derzeit haben wir einen Flickenteppich: Die DSGVO regelt den Datenschutz, das BSI-Gesetz gilt für Kritische Infrastrukturen und das Onlinezugangsgesetz (OZG) betrifft einzelne Verwaltungsleistungen. Eine einheitliche Cybersicherheitsstrategie gibt es nicht. Hinzu kommt, dass Kommunen bei vielen Regelungen durch das Raster fallen. Das BSI-Gesetz etwa bezieht sie bislang kaum ein. Einige Länder wie Bayern oder Hessen haben deshalb eigene Gesetze erlassen und Landes-CISOs etabliert – aber das ist bei weitem nicht überall der Fall.

Dittrich: Deshalb muss man auch klar sagen: Ohne eine solide Finanzierung bleibt jede Strategie ein Papiertiger. Es kann nicht sein, dass nur wohlhabende Kommunen ihre digitale Infrastruktur schützen können – die Daten der Bürgerinnen und Bürger in Hagen sind genauso schützenswert wie in Wolfsburg. Hier sind Bund und Länder gefragt, für einen Ausgleich zu sorgen.



Dr. Tilmann Dittrich (links) ist Rechtsanwalt der Kanzlei Wessing & Partner Rechtsanwälte mbB in Düsseldorf und Co-Autor der Studie.

Dr. Michael Littger (rechts) ist Strategiedirektor des cyberintelligence.institute (CII).

Wie bewerten Sie die Vorhaben der neuen Bundesregierung?

Dittrich: Insgesamt positiv. Mit dem neuen Digitalministerium und der nun wohl zeitlich straffen Umsetzung von NIS-2 hat die Regierung in ihren ersten Tagen im Amt gezeigt, dass sie Tempo aufnehmen will. Leider aber werden Kommunen bei NIS-II erneut außenvorgelesen – das ist ein Versäumnis.

Littger: Auch der angekündigte Deutschland-Stack ist eine Chance für Cybersicherheit und ermöglicht einen Neustart in Sachen Digitale Souveränität. Vor fau-

len Kompromissen können wir nur warnen, sonst scheitert die neue Regierung sehr schnell am Anspruch, einen echten Orientierungsanker für übergreifende Sicherheitsstandards zu schaffen. Hier bleibt spannend, welches Signal das Bundesministerium in den nächsten 100 Tagen setzen wird. Wichtig ist jetzt, dass auch die Kommunikation nach außen stimmt. Denn was viele unterschätzen: Gut erklärte Cybersicherheit kann ein sehr starkes Signal an Bürgerinnen und Bürger senden. Das stärkt das Vertrauen in den Staat und seine Leistungsfähigkeit – derzeit ein unbezahlbarer Wert!

WEITERE INFOS

Mehr Informationen finden sich im Whitepaper „Kommunale Cybersicherheit auf dem Prüfstand“ des cyberintelligence.institute (CII): bit.ly/va03-2025-whitepaper

GENAI-PLATTFORM : SICHER, SKALIERBAR, SOUVERÄN

Der Einsatz von generativer KI (GenAI) hat enorme Innovationspotenziale für digitale Services der Behörden. Viele IT-Dienstleister arbeiten an entsprechenden Angeboten. Die Herausforderungen dabei sind groß: Auswahl der Technik, Nutzung von Behördendaten, Berücksichtigung von Souveränität, Datenschutz und IT-Compliance.

govdigital begegnet diesen Herausforderungen mit einer speziell für öffentliche IT-Dienstleister und ihre Kunden konzipierten GenAI-Plattform. Die Plattform stellt eine langfristige Grundlage für das GenAI-Engagement der govdigital-Mitglieder dar. Sie ermöglicht es, KI-Anwendungen datenschutzkonform, flexibel und wirtschaftlich zu entwickeln und zu betreiben – in deutschen Rechenzentren sowie inhouse durch öffentliche IT-Dienstleister. Dabei stehen Sicherheit, Souveränität und Skalierbarkeit im Mittelpunkt.

DURCHGÄNGIGE COMPLIANCE-ARCHITEKTUR

Die Plattform bietet eine durchgängige Compliance-Architektur: Sie stellt sicher, dass nur KI-Modelle und -Dienste zum Einsatz kommen, die den regulatorischen Anforderungen des öffentlichen Sektors genügen. Zugleich gewährleistet ein mandantenfähiges System eine strikte Trennung der Daten- und Anwendungsbereiche unterschiedlicher Verwaltungen – für maximale Vertraulichkeit und Kontrolle. Der Einsatz von Open-Source-

Software schafft Transparenz, fördert Flexibilität und schützt vor Anbieterabhängigkeiten.

Ein integrierter App-Store erlaubt die einfache Übernahme, Anpassung und Wiederverwendung praxiserprobter Lösungen – von intelligenten Chatbots über Dokumentenassistenten bis hin zu KI-unterstützten Fachverfahren. Diese Anwendungen lassen sich sofort produktiv einsetzen oder flexibel auf individuelle Anforderungen zuschneiden.

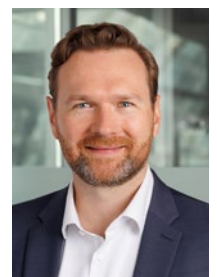
„UNSERE PLATTFORM SPRICHT VERWALTUNG.“

Kommunen, Länder und Bundesbehörden können von einem deutlich reduzierten Entwicklungsaufwand, niedrigeren Betriebskosten und einer höheren Interoperabilität durch standardisierte Schnittstellen profitieren. Die Plattform kann Mitarbeitende entlasten und das digitale Serviceniveau nachhaltig anheben. Erste Funktionalitäten der Plattform werden Ende 2025 bereitstehen, der vollständige Ausbau ist bis Mitte 2026 geplant.

Mit der GenAI-Plattform macht sich govdigital auf den Weg, gemeinsam mit Mitgliedern und Partnern KI für die Verwaltung nicht nur verfügbar, sondern verantwortungsvoll, effizient und zukunftssicher nutzbar zu machen. Wir entwickeln eine Lösung, die genau auf die Anforderungen und Regularien öffentlicher Verwaltungen zugeschnitten ist.



**Thomas Schmitt ist
IT-Architekt bei
govdigital eG.**



**Maximilian Brunn ist
Geschäftsbereichsleiter
KI bei govdigital eG.**



**SMART
COUNTRY
CONVENTION**
#nextgermany

Viel mehr als Software!

Sie setzen Kurs auf eine zukunftsorientierte, digitale Verwaltung – wir machen sie möglich! Ob sicherer IT-Betrieb, vollständig digitale Verwaltungsprozesse, servicestarke Ämter oder klimaresiliente Städte und Gemeinden: Die AKDB-Gruppe bietet Ihnen Lösungen, nicht nur Software. Für ein funktionierendes Gemeinwesen. Für einen modernen Staat. Für uns alle!

www.akdb.de/sccon

AKDB

Wir haben die Lösung

SERIE KOMMUNE DER ZUKUNFT



Der Weg zur vollständig digitalen Kommunalverwaltung ist lang. Umso wichtiger ist es, dass Kommunen in die Lage versetzt werden, Prozesse eigenständig zu digitalisieren. Eine wichtige Unterstützung bietet dabei die Low-Code-Plattform Axon Ivy des kommunalen IT-Dienstleisters OWL-IT. Wie das funktioniert, erklären der Projektleiter Dhany Ballgobind und der Bereichsleiter Softwareentwicklung Christian Beermann.

TEIL 14
STRATEGIEWERKSTATT
FÜR KOMMUNEN

TEIL 15
EIN CHATBOT FÜR
JEDEN BESCHIED

TEIL 16
GREMIENSITZUNGEN
WERDEN HYBRID

TEIL 17
VERWALTUNGSDIGITALISIERUNG
IN EIGENREGIE

VERWALTUNGSDIGITALISIERUNG IN EIGENREGIE

Bislang sind Kommunen bei der Digitalisierung fast vollständig auf die Unterstützung ihrer Fachverfahrenshersteller angewiesen. Für jede neue Lösung ist in der Regel eine öffentliche Ausschreibung notwendig. „Vom ersten Angebot bis zur Umsetzung können teils Monate ins Land ziehen“, so Christian Beermann. Selbst kleinere Medienbrüche zu schließen, wird dabei zum langwierigen Vorhaben. Die Low-Code-Plattform Axon Ivy befähigt kommunale IT-Abteilungen, digitale Lösungen auch in Eigenregie zu entwickeln.

LEICHTER EINSTIEG

Die Bedienung der Plattform ist intuitiv. Dhany Ballgobind: „Um mit Axon Ivy zu arbeiten, braucht es kein Informatikstudium.“ Schon einfache Programmierkenntnisse reichen aus. Entwicklungsschritte – die sonst in komplexem Code dargestellt sind – werden auf der Plattform grafisch visualisiert. Per Drag-and-Drop-Menü wählen Nutzerinnen und Nutzer zwischen verschiedenen Bausteinen aus und müssen nur noch an wenigen Stellen selbst Code einfügen. Über eine integrierte Toolbox lassen sich zu-

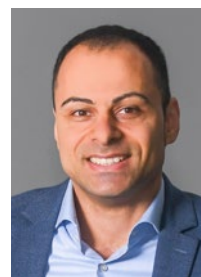
dem Vorlagen bereits entwickelter Lösungen auf eigene Bedarfe anpassen.

Seit Anfang 2025 steht das Angebot allen Kunden offen – wahlweise zur eigenständigen Nutzung mit optionaler Beratung oder als Full-Service durch OWL-IT. Erste Kunden setzen bereits eigene Pilot-Projekte um: Der Kreis Herford etwa nutzt Axon Ivy, um eine Schnittstelle im öffentlichen Gesundheitsdienst zu schließen. Der Kreis Paderborn entwickelt eine Lösung für das städtische Geoinformationssystem.

COMMUNITY ALS HILFESTELLUNG

Begleitend baut OWL-IT zudem eine digitale Low-Code-Community mit den beteiligten Kommunen auf. Das Ziel: Erfahrungen austauschen, gegenseitig Hilfestellung leisten und sich im besten Fall sogar auf gemeinsame Standards und Ziele verständigen. „Die Zusammenarbeit ist enorm produktiv – wir kommen wirklich gemeinsam ins Entwickeln“, so Dhany Ballgobind. „So verstehen wir als IT-Dienstleister die Bedarfe der Kommunen noch besser und können gezielt unterstützen.“

Seit Anfang 2025 arbeitet OWL-IT zudem daran, Robotic Process Automation (RPA) und Künstliche Intelligenz (KI) in die Plattform zu integrieren. Einfache, wiederkehrende Aufgaben lassen sich so künftig noch leichter automatisieren. Christian Beermann: „Damit geben wir den Kommunen ein Werkzeug an die Hand, um noch effizienter zu werden. Das ist ein wichtiger Schritt in Richtung kommunale Selbstermächtigung!“



Dhany Ballgobind
ist Projektleiter
bei OWL-IT.



Christian Beermann
ist Bereichsleiter
Softwareentwicklung
bei OWL-IT.

ELEKTRONISCHE SIEGEL UND SIGNATUREN ZUKUNFTSSICHER UND FLEXIBEL INTEGRIEREN

Der Weg zur Digitalisierung in der öffentlichen Verwaltung ist bereits eingeschlagen – das Herumreichen von Unterschriftenmappen gehört der Vergangenheit an. Damit steigen jedoch die Anforderungen an rechtssichere und medienbruchfreie Prozesse. Elektronische Signaturen und Siegel sind dabei unverzichtbare Bausteine, um effiziente Arbeitsabläufe zu gewährleisten. Governikus DATA Sign bietet hier eine praktische Lösung, die sich nahtlos in bestehende Prozesse integriert.

Obwohl viele Arbeitsabläufe heute digital sind, erfolgt das Unterschreiben von Dokumenten oft noch immer analog – ein Bruch im Prozess, der Risiken birgt und Ressourcen bindet. Mit Governikus DATA Sign ändert sich das: Es handelt sich um eine webbasierte Plattform für qualifizierte elektronische Signaturen und Siegel, die den kompletten Prozess abdeckt. Sie erfüllt alle Anforderungen der eIDAS-Verordnung und sorgt für Transparenz und Sicherheit.

Ein zentrales Ziel ist es, papierbasierte Verfahren vollständig zu ersetzen. Der medienbruchfreie Ablauf spart Zeit, senkt Kosten, verringert Fehlerquellen und sorgt für eine bessere Nachvollziehbarkeit.

DEMOZUGANG ERHÄLTICH

Alle Test- und Integrationsmöglichkeiten können Interessierte jetzt 30 Tage lang kostenlos in einer praxisnahen Umgebung testen. Dabei können sie qualifizierte elektronische Signaturen und Siegel einrichten, ohne eigene technische Infrastruktur aufbauen zu müssen. Außerdem steht eine gesicherte API-Testumgebung bereit, in der Signaturprozesse der Vertrauensdiensteanbieter – wie qVDA, Bank-Verlag und D-Trust der Bundesdruckerei – getestet werden können. So lassen sich Integrationen vorbereiten, ohne eigene Referenzzugänge beantragen zu müssen.

ZUKUNFTSSICHER UND FLEXIBEL

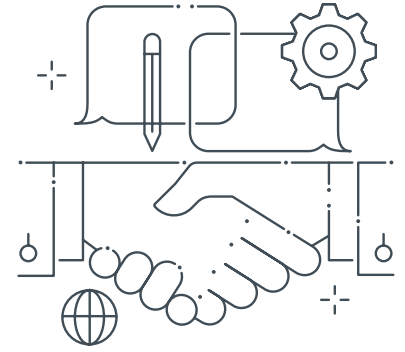
DATA Sign ist so entwickelt, dass es sich problemlos in bestehende Dokumentenmanagement- oder eAkten-Systeme integrieren lässt. Die Plattform ist skalierbar und bietet flexible Schnittstellen, während die Webversion zusätzlich mit einer benutzerfreundlichen Oberfläche daherkommt. Unternehmen können auf eine Auswahl verschiedener Vertrauensdiensteanbieter zugreifen. In Zukunft wird das Angebot weiter ausgebaut und an neue regulatorische Anforderungen angepasst.

Als Teil der Anwendung, die als ein zentrales Produkt des IT-Planungsrates durch Governikus bereitgestellt wird, setzt DATA Sign neue Maßstäbe in der Dokumentenverarbeitung. Es hilft Unternehmen, ihre Prozesse effizienter zu gestalten und gleichzeitig rechtlich auf der sicheren Seite zu bleiben.



MEHR DAZU UNTER

www.governikus.de/demo-governikus-data-sign/



„DIE KOMMUNEN DÜRFEN JETZT IHR MOMENTUM NUTZEN“

Die neue Bundesregierung hat die digitale Verwaltung weit oben auf die Agenda gesetzt. Doch wie lassen sich alte Fehler vermeiden? Und wie können die Kommunen – und die Menschen, die dort täglich Verantwortung übernehmen – sichtbarer werden? Dr. Dorit Bosch, Verwaltungsjuristin, Business Coach und Gründerin des Mindshift Festivals, im Gespräch mit Katrin Giebel, stellvertretende Geschäftsführerin von VITAKO, über einen Kulturwandel in der Verwaltung und warum jeder einzelne Beitrag zählt.

Katrin Giebel: Dorit, was können die Kolleginnen und Kollegen im Bund unter der neuen Regierung besser machen?

Dr. Dorit Bosch: Das zentrale Problem ist: Wir entwickeln immer noch zu viele Lösungen aus dem Elfenbeinturm, ohne echten Dialog mit denen, die es später umsetzen sollen. Da wurden oft neue Lösungen mit viel Tempo vorangetrieben, die dann im Zweifel viel Geld kosten, aber an den tatsächlichen Bedarfen – insbesondere der Kommunen – vorbeigingen. Ein gutes Beispiel ist auch die Corona-Warn-App: Eigentlich eine tolle Idee. Aber nicht alltagstauglich für viele Kollegen in der Verwaltung, wenn die Gesundheitsämter nicht im ersten Schritt schon mitgedacht werden.

Da bin ich absolut bei Dir. Aber viele würden jetzt sagen: Der Föderalismus steht dem im Weg...

Das ist mir zu einfach. Ja, wir haben ein föderales System. Aber nirgendwo steht geschrieben, dass man nicht zusammenarbeiten darf. Frankreich zum Beispiel ist hochzentralisiert, und trotzdem muss die Regierung die Realität der 86 Départements berücksichtigen. Genau darum geht es: zu verstehen, was Menschen wie Lisa und Felix in einer Kommunalverwaltung tatsächlich leisten, was sie brauchen, was sie stemmen können. Nur so entsteht ein tragfähiges System. Und dafür braucht es Räume zum Mitdenken und Mitreden – für echte Perspektiven aus der Praxis.

„Es braucht Räume für echte Perspektiven aus der Praxis.“

Dr. Dorit Bosch

Du selbst kommst aus der Bundesverwaltung. Ist das immer leicht umzusetzen?

Natürlich nicht – das habe ich am eigenen Leib erfahren. Ich habe von Anfang an darauf hingewiesen, dass die Kommunen mit an den Tisch müssen und wurde nicht immer gehört. Umso schöner zu sehen, dass sich gerade in den letzten Jahren spürbar etwas bewegt hat. Die Kommunen haben gerade ihr großes Momentum. Der demographische Wandel, aber auch zunehmende Cyberangriffe machen immer deutlicher: Ohne die

Kompetenz und Kreativität in den Kommunen geht es nicht. Ihre Lösungen sind überlebensnotwendig – und verdienen die Anerkennung, die ihnen zusteht. Die Kommunen sind der Maschinenraum der Demokratie, hat Jürgen Beck, Leiter des Amts für öffentliche Ordnung der Stadt Pforzheim, in meinem Podcast Let's Staat gesagt. Und so ist es!

Genau dieses Momentum nutzen wir bei VITAKO, um uns einzubringen und mitzugestalten. Was rätst du uns?

Ihr habt schon sehr viel angestoßen, Katrin. Ihr geht raus, führt Gespräche, knüpft Netzwerke – genau das ist der richtige Ansatz. Im Coaching sage ich oft: Warte nicht auf perfekte Strukturen. Fang an, wo du gerade bist! Viele wünschen sich gleich das ganze Paket – Mitsprache an allen Tischen, Einfluss auf Gesetzgebungen. Aber die wichtigste Frage ist nicht: Was wäre ideal? Sondern: Was kannst du jetzt realistisch bewegen?



Katrin Giebel (links) ist stellvertretende Geschäftsführerin von VITAKO.

Dorit Bosch (rechts) ist promovierte Verwaltungsjuristin, Business Coach und Gründerin des Mindshift Festivals.

Was können Mitarbeitende in den Behörden konkret tun?

In meinen Coachings sind immer wieder drei Punkte wichtig. Erstens: Kenne deine Stärken. Was willst und kannst du zusammen mit deinem Team erreichen? Nimm dir für diese Frage in einer Teambesprechung Zeit. Zweitens: Vernetze dich. Wer unterstützt das Thema noch? Geh raus und baue eine Community in deiner Behörde und darüber hinaus auf. Und drittens: Werde sichtbar! Wo werden diese Themen entschieden und wie kannst du Kontakt zu Entscheidungsträgern aufbauen? Diese Art zu arbeiten gibt Kraft und stärkt uns von innen. Denn: Jeder einzelne Schritt, jede Stimme zählt.

Gibt es auch Beispiele, wo eine Zusammenarbeit schon gut funktioniert hat?

Auf jeden Fall! Ein starkes Beispiel ist die Föderale Digitalstrategie. Sie ist ein echter Meilenstein für eine neue Form der Zusammenarbeit: Bund, Länder und kommunale Spitzenverbände haben – koordiniert vom IT-Planungsrat – mit vereinten Kräften ein Zielbild für eine gemeinsame digitale Zukunft erarbeitet. Damit haben sie eine wichtige Grundlage geschaffen, endlich verbindliche

Standards und einheitliche Schnittstellen über alle Ebenen hinweg umzusetzen. Ein gutes Beispiel dafür, was möglich ist, wenn man aufeinander hört.

Oft herrscht in der Gesetzgebung ein großer Zeitdruck. Ist es da überhaupt möglich, alle Perspektiven einzubeziehen?

Wir kommen aus einer Kultur, in der die Einstellung weit verbreitet ist: „Allein und geradlinig geht es schneller.“ Das ist ein Irrglaube. Denn es sind doch gerade diese Schnellschüsse, mit denen wir hinten raus Probleme schaffen. Und die Folgen müssen dann oft diejenigen auffangen, die im Alltag die Gesetze umsetzen – also die Menschen in den Kommunen. Es ist aufwändig, ein Gesetz zu machen – aber es ist noch viel aufwändiger, es zu-

rückzunehmen, wenn es nicht funktioniert hat. Deshalb braucht es kluge und kraftvolle Stimmen wie eure – frühzeitig.

Auf dem Mindshift Festival bringst du viele hochmotivierte Menschen zusammen!

Das stimmt. Das Festival bietet denjenigen, die wirklich etwas erreichen und anpacken wollen, einen Resonanzraum: Es ist ein Ort zum Ideen spinnen, Erfahrungen austauschen und Netzwerken. Außerdem können sich Menschen dort Rückhalt zu suchen – denn mutig zu sein in alten Strukturen kostet enorm viel Kraft. Umso mehr freut es mich, dass ihr euch mit VITAKO einbringt und den Kommunen eine so starke Stimme verleiht. Genau da liegt der Schlüssel für den Wandel.

DAS MINDSHIFT FESTIVAL

Das Festival bringt Pionierinnen und Pioniere aus Verwaltung, Politik und Zivilgesellschaft zusammen – mit dem Ziel, innovative Lösungsansätze zu fördern, neue Netzwerke zu knüpfen und den Wandel in Behörden konkret voranzutreiben. Am 2. Oktober 2025 findet es erstmalig in Wien statt. Mehr Informationen unter: www.drdoritbosch.de



Jürgen Abelshäuser
ist Vorstandsvor-
sitzender & CEO
der ProVitako e.G.

PROVITAKO: BESCHAFFUNGEN NOCH STRATEGISCHER PLANEN

Wir erkennen die Beschaffungsinteressen unserer Mitglieder frühzeitig, erarbeiten daraus europaweite Ausschreibungen und erzielen gute Konditionen über großvolumige Rahmenverträge. Mit dem Portfolio-Management unterstützen wir diesen Anspruch und bauen derzeit eine Treiberrolle bei der ProVitako auf.

Erstmals vorgestellt wurde das Portfolio-Management auf der „Hausmesse meets Beschaffungskonferenz“ Anfang Mai in Bremen. Die Idee: Handlungsfelder identifizieren, die aufgrund von Marktreife, Nachfragepotenzial und Innovationsgrad eine hohe strategische Relevanz für die ProVitako-Community besitzen. Dabei stehen Themen wie Backup-Lösungen, Härtung von IT-Umgebungen oder auch Robotic Process Automation – für die es derzeit noch keine gemeinsamen Beschaffungsinitiativen gibt – ganz oben auf der Agenda.

PROVITAKO BEWEGT MILLIARDEN

4 Mrd. €

Bestand der Rahmenverträge des ITK-Portfolios der ProVitako zum Jahresende 2025

PORTFOLIO-STRATEGIE-KREIS ALS INHALTLICHER GESTALTER

Der Portfolio-Strategie-Kreis, der sich aus Portfolio-Verantwortlichen der Mitglieder zusammensetzt, wird das Herzstück für die Innovationsbeschaffungen der ProVitako-Community. Dieses Beteiligungsformat wird das kommunale ITK-Portfolio in Deutschland wesentlich weiterentwickeln. Die erste Kick-Off-Veranstaltung ist noch für das laufende Jahr geplant, die Vorfreude ist bei uns in Siegburg und unseren Mitgliedern mit Händen zu greifen.

BESCHAFFUNGSVORHABEN IM AUFWIND

Anzahl der von ProVitako durchgeführten Beschaffungsvorhaben

2021: **5** 2025: **22**

BESCHAFFUNGSKONFERENZEN ALS GEMEINSAMES PLANUNGSINSTRUMENT

Die inhaltlichen Impulse aus dem Portfolio-Strategie-Kreis werden gezielt in die ProVitako-Beschaffungskonferenz einfließen. Die Plattform ist ideal, um sich über strategische Handlungsfelder und konkrete Beschaffungsvorgänge innerhalb und mit der Mitgliedschaft auszutauschen. Sie hat sich als zentrales Planungsinstrument der ProVitako-Community für deutschlandweit gebündelte Beschaffungsvorhaben etabliert.

KONTAKT

Michael Schnepfer

Kundenmanagement

Tel.: +49 2241 999 1170

kundenmanagement@provitako.de

Stefan Pauly

Portfolio Management

Tel. +49 151 58438028

stefan.pauly@provitako.de

SAVE THE DATE

Die nächste Beschaffungskonferenz findet am 11. und 12. November 2025 in München statt.

Politischer Abend am 9. Juli 2025

DIGITALE VERWALTUNG JETZT!

Die Verwaltungsdigitalisierung nimmt unter der neuen Bundesregierung spürbar an Fahrt auf – siehe etwa das neue Digitalministerium oder die geplante Umsetzung von NIS-2. Nun gilt es, die Vorhaben entschlossen umzusetzen. Doch welche Prioritäten müssen gesetzt werden? Was braucht es für die gelingende Umsetzung aus Sicht der Kommunen? Und wie kann die interföderale Zusammenarbeit noch stärker forciert werden? Diese Fragen standen bei unserem Politischen Abend im Mittelpunkt.



Thomas Jarzombek, Parlamentarischer Staatssekretär im neuen Digitalministerium, stellte in seiner Keynote den Deutschland-Stack als gemeinsame bundesweite Plattform vor.



Es diskutierten (v.l.n.r.): Parsa Marvi (MdB SPD); Kerstin Pliquett (Geschäftsleiterin KDN und Vorstandsmitglied VITAKO); Sören Kuhn (Vorstandsvorsitzender VITAKO); Alexander Handschuh (Sprecher DStGB); Ralph Brinkhaus (MdB CDU/CSU); Katrin Giebel (stellv. Geschäftsführerin VITAKO); Lars Hoppmann (geschäftsführender Vorstand VITAKO); Bernd Schlömer (CIO Sachsen-Anhalt); Dr. Johann Bizer (Vorstandsvorsitzender Dataport und Vorstandsmitglied VITAKO)

Ostwestfalen-Lippe-IT

OWL!t



Ihr Partner für die digitale Transformation

Dynamische Zusammenarbeit,
aufregende Innovationen,
erstklassige IT-Lösungen
und viel Expertise.

Das ist die Ostwestfalen-Lippe-IT.

www.owl-it.de



95 %

Die Gefahr steigt

Laut 95 % der IT-Dienstleister hat das Risiko von IT-Cybersicherheitsvorfällen in Kommunen deutlich zugenommen.

CYBERSICHERHEIT: NACHHOLBEDARF INSBESONDERE BEI KLEINEN KOMMUNEN

Wie schätzen kommunale IT-Dienstleister die Cybersicherheitslage in den Kommunen ein?

Die aktuelle Umfrage gibt einen Überblick.

Um sich vor Cyberangriffen zu schützen, müssen Kommunen erhebliche finanzielle und personelle Ressourcen aufbringen. Doch genau daran mangelt es vielerorts – insbesondere in kleinen Kommunen. Rund 80 Prozent der befragten IT-Dienstleister beklagen, die Ausstattung für IT-Sicherheit sei bei Kommunen mit weniger als 10.000 Einwohnerinnen und Einwohnern viel zu schlecht. In mittelgroßen und großen Kommunen zeigt sich ein etwas positiveres Bild, dennoch hält auch hier ein Großteil der Befragten die Ausstattung für viel oder etwas zu schlecht.

Eine mögliche Ursache: Zwei Drittel der kommunalen Entscheidungsträger unterschätzen nach Aussage der IT-Dienstleister weiterhin die Dringlichkeit des Themas. Der Wert ist im Vergleich zum Vorjahr sogar noch gestiegen. Und das, obwohl sich die Gefahrenlage weiter zuspitzt. So sehen 95 Prozent der IT-Dienstleister einen massiven Anstieg der Cybergefahr in den letzten fünf Jahren.

Befragt nach der wichtigsten Maßnahme zum Schutz vor Angriffen nennen gut ein Viertel der Befragten die gezielte Weiterbildung von Mitarbeitenden. Dicht

gefolgt von einer engeren Zusammenarbeit zwischen Kommunen sowie mit Bund und Ländern. Denn klar ist auch: Die Kommunen allein können die wachsenden Anforderungen nicht stemmen. Schon heute stellen fast 90 Prozent der befragten IT-Dienstleister einen steigenden bürokratischen Aufwand für Cybersicherheit fest – angesichts der begrenzten Ressourcen in den Kommunen ein Warnsignal.

AUSSTATTUNG BEI KLEINEN KOMMUNEN MANGELHAFT

Wie sind die Kommunalverwaltungen im Bereich Cybersicherheit personell und finanziell ausgestattet?

Kommunen < 10.000 Einwohnerinnen und Einwohner

77,8 %

18,5 %

3,7 %

Kommunen 10.000 – 100.000 Einwohnerinnen und Einwohner

30,0 %

60,0 %

10,0 %

Kommunen > 100.000 Einwohnerinnen und Einwohner

8,1 %

59,5 %

29,7 %

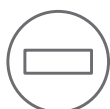
2,7 %

■ Viel zu schlecht

■ Etwas zu schlecht

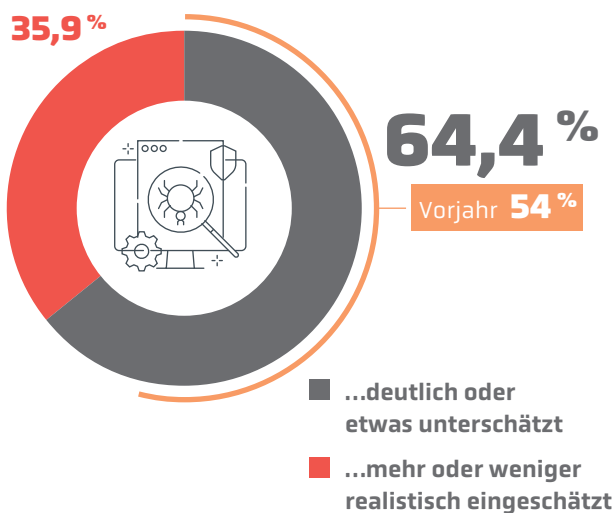
■ Genügend

■ Etwas zu gut



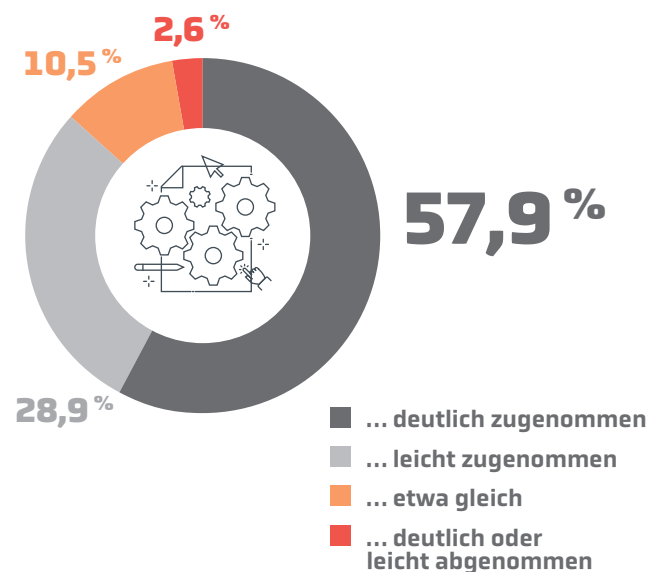
CYBERGEFAHREN WERDEN NACH WIE VOR UNTERSCHÄTZT

Wie realistisch schätzen die kommunalen Entscheider Cybergefahren ein?



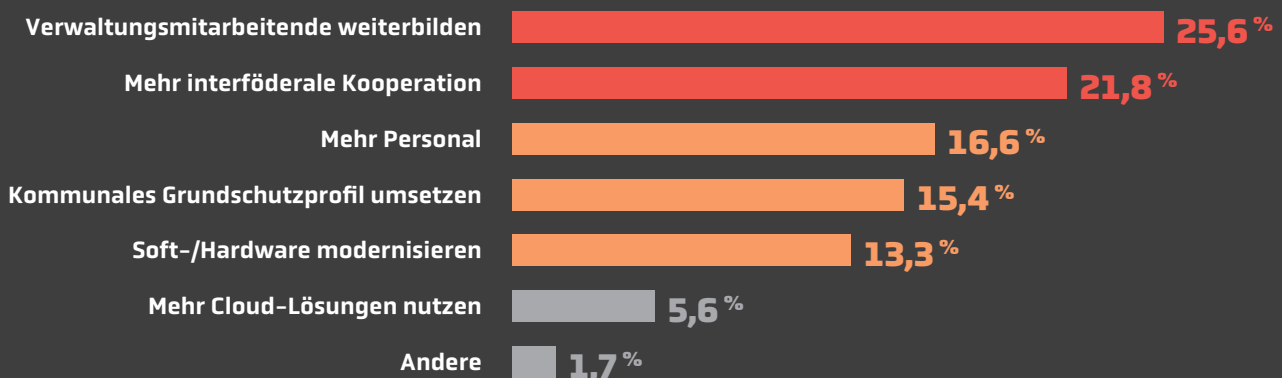
BÜROKRATISCHER AUFWAND NIMMT ZU

In den vergangenen 5 Jahren hat der bürokratische Aufwand rund um das Thema Cybersicherheit in Kommunen ...



WEITERBILDUNG UND KOOPERATION IM FOKUS

Mit welcher der folgenden Maßnahmen können sich Kommunen am besten gegen Cyberattacken wappnen?



Die Umfrage wurde vom Marktforschungsunternehmen Hiestermann & Frömchen GmbH durchgeführt.



Herausgeber:

Bundes-Arbeitsgemeinschaft der
Kommunalen IT-Dienstleister e. V.
Charlottenstr. 65
10117 Berlin
Tel. 030/20 63 15 60
E-Mail: aktuell@vitako.de
www.vitako.de

V. i. S. d. P.: Lars Hoppmann,
geschäftsführender Vorstand von VITAKO

Redaktion, Gestaltung: Köster Kommunikation

Die Redaktion behält sich vor, eingesandte Berichte auch ohne vorherige Absprache zu kürzen. Der Inhalt der Beiträge gibt nicht in jedem Fall die Meinung des Herausgebers wieder. Alle Rechte vorbehalten. Nachdruck oder elektronische Verbreitung nur mit Zustimmung des Herausgebers.

Druck: triggermedien, Berlin

Erscheinungsweise: 4 Ausgaben/Jahr, Auflage: 5.000

Autoren und Mitwirkende dieser Ausgabe:

Jürgen Abelhauser, ProVitako; Dhany Ballgobind, OWL-IT; Christian Beermann, OWL-IT; Maximilian Brunn, govdigital; Dr. Dorit Bosch, Bundesministerium für Digitales und Staatsmodernisierung; Friederike Dahns, BMI; Dr. Tillmann Dittrich, Kanzlei Wessing & Partner; Marco Dörfler, AKDB; Stefanie Euler, BSI; Katrin Giebel, VITAKO; Lutz Hiester mann, Hiester mann & Frömchen; Lars Hoppmann, VITAKO; Thomas Jarzombek, Bundesministerium für Digitales und Staatsmodernisierung; Tobias Kippert, PROSOZ; Sören Kuhn, VITAKO; Dr. Michael Littger, CII; Aboli Lion, VITAKO; Oskar Rzepinski, PROSOZ; Thomas Schmitt, govdigital; Philipp Schneider, ekom21; Michael Schnepfer, ProVitako

Bildnachweise:

S. 3: dirk hasskarl/fotografie; S. 4: folgt; S. 7: dirk hasskarl/fotografie; S. 11: Kurc/VITAKO; S. 29: Coco Spenger für das Mindshift-Festival; S. 30: atelier-fotogreif@t-online.de; S. 31: Kurc/VITAKO

Hinweis:

VITAKO aktuell erscheint zusätzlich mit zwei Regionalausgaben: OWL-IT, Lecos. Der Vertrieb erfolgt durch das jeweilige VITAKO Mitglied.

ISSN 2194-1165

Wird innerhalb der Zeitschrift auf fremde Links oder externe Informationsangebote hingewiesen, so macht sich VITAKO diese Inhalte nicht zu eigen und kann für sie keine Haftung übernehmen.

TERMINE

30. September – 02. Oktober 2025, Berlin

SMART COUNTRY CONVENTION (SCCON)

hub27, Standnummer 406, Messegelände Berlin
www.smartcountry.berlin

06. November 2025, Berlin

VITAKO JUBILÄUM 20 JAHRE

www.vitako.de

**DIE NÄCHSTE „VITAKO AKTUELL“
ERSCHEINT IM DEZEMBER 2025.**



Für sichere, innovative und bürgernahe Kommunen

Wir gestalten die digitale Zukunft vor Ort.
www.dataport-kommunal.de

KOMMUNALE VERWALTUNG AUS EINER HAND

Cloud-Lösungen,
IT-Infrastruktur,
Cybersicherheit.

Komm.ONE – Ihre
Partnerin für die
digitale Zukunft.

Sie finden uns auf der SCCON.
30. Sept. bis 02. Okt. 2025
hub27, Stand 405



Sie wollen mehr über uns erfahren:
komm.one/mitglieder magazin

