IT-Architektur

Digitalisierung dauerhaft sicher gestalten

[12.11.2026] Offene Schnittstellen, neue Technologien und steigende Sicherheitsanforderungen stellen Kommunen vor Herausforderungen. Modulare Plattformarchitekturen schaffen die Grundlage für eine sichere und zukunftsfähige Verwaltungs-IT.

Kommunen sollen digitale Verwaltungsleistungen zügig bereitstellen, bestehende Fachverfahren vernetzen und gleichzeitig neue Technologien wie Künstliche Intelligenz integrieren. Parallel dazu steigen die Anforderungen an Datenschutz, Informationssicherheit und Resilienz kontinuierlich. Für viele Verwaltungen entsteht daraus der Eindruck eines Zielkonflikts: Je offener eine IT-Landschaft für neue Anwendungen gestaltet wird, desto größer scheint das Sicherheitsrisiko. Doch es gibt Lösungen.

Die meisten Kommunen arbeiten heute nicht mit einer einzigen Verwaltungsplattform, sondern mit einer Vielzahl spezialisierter Anwendungen unterschiedlicher Hersteller. Denn Anforderungen an kommunale Verwaltungen und ihre Digitalisierung haben sich in den vergangenen Jahren grundlegend verändert. Während früher häufig einzelne Fachverfahren digitalisiert wurden, stehen heute durchgängige digitale Prozesse im Mittelpunkt. Bürgerinnen und Bürger erwarten Verwaltungsleistungen, die unabhängig von Öffnungszeiten oder Zuständigkeiten verfügbar sind.

Hinzu kommen gesetzliche Vorgaben wie das Onlinezugangsgesetz, die Registermodernisierung oder Anforderungen an interoperable Verwaltungsprozesse: Bürgerinnen und Bürger geben ihre Daten heute idealerweise nur noch einmal an. Damit Anträge medienbruchfrei bearbeitet werden können, müssen Fachverfahren, Register, Dokumentenmanagementsysteme, Identitätsdienste und weitere Anwendungen Informationen automatisiert austauschen. Moderne Plattformen verfügen deshalb über standardisierte Schnittstellen. Ebenso lassen sich externe Dienste wie BundID oder Unternehmenskonto integrieren. Diese Vernetzung ermöglicht durchgängige digitale Verwaltungsprozesse und verhindert eine doppelte Datenerfassung oder manuelle Zwischenschritte.

Sicherheit beginnt nicht bei der Firewall

Das Problem: Sobald Anwendungen Daten austauschen und Prozesse über Systemgrenzen hinweg ablaufen, entstehen Angriffsflächen. Und die Bedrohung durch Cyber-Angriffe wächst: Kommunale Verwaltungen gehören inzwischen regelmäßig zu den Zielen professioneller Angreifer. Die Absicherung einzelner Systeme reicht nicht mehr, Sicherheit muss auf Plattformebene gedacht werden. Die Systeme müssen sicher, nachvollziehbar und dauerhaft miteinander arbeiten können. Das erfordert Architekturen, die Identitäten, Zugriffe, Datenflüsse und Schnittstellen zentral absichern und überwachen. Firewalls, Virenschutz oder Verschlüsselung bleiben unverzichtbarer Teil des Sicherheitskonzepts und werden von anderen Elementen ergänzt.

Eins dieser Elemente ist die zentrale Benutzerverwaltung: Sie vereinfacht nicht nur die Administration, sondern ermöglicht auch eine konsistente Vergabe von Berechtigungen. Gerade bei Personalwechseln oder organisatorischen Veränderungen reduziert das Sicherheitsrisiken erheblich. Hier schließt ein durchgängiges Identity Management an: Benutzerinnen und Benutzer benötigen eindeutige Identitäten, über die sämtliche Zugriffe gesteuert werden. Ergänzend sorgen Rollen- und Rechtekonzepte dafür, dass

Mitarbeitende ausschließlich auf diejenigen Informationen und Funktionen zugreifen können, die sie für ihre Aufgaben tatsächlich benötigen.

Für kommunale Plattformen spielt außerdem die Mandantenfähigkeit eine wesentliche Rolle: Verschiedene Organisationseinheiten oder angeschlossene Einrichtungen können auf einer gemeinsamen Plattform arbeiten, ohne dass Daten oder Berechtigungen vermischt werden. Ein weiterer Baustein ist die vollständige Nachvollziehbarkeit der Aktivitäten. Protokollierung und revisionssichere Dokumentation schaffen Transparenz und ermöglichen die Kontrolle sicherheitsrelevanter Vorgänge.

Sicherheit entsteht damit nicht erst durch technische Schutzmechanismen am Rande eines Netzwerks. Sie ist das Ergebnis klar definierter Prozesse, eindeutiger Zuständigkeiten und einer Architektur, die den kontrollierten Umgang mit Daten und Zugriffsrechten gewährleistet.

Offenheit bedeutet Integrationsfähigkeit

Sicherheit ist aber nur ein Teil des Ganzen. Die Offenheit der Systeme ist der andere: Denn dies bedeutet Integrationsfähigkeit und schafft Investitionssicherheit. Neue Anwendungen können dann ergänzt werden, ohne bestehende Strukturen ersetzen zu müssen. Damit bleiben Investitionen, die in Fachverfahren geflossen sind, erhalten. Eine integrationsfähige Plattform reduziert außerdem den Aufwand bei künftigen Digitalisierungsprojekten: Neue gesetzliche Anforderungen oder zusätzliche Online-Services können schneller umgesetzt werden, wenn die technische Grundlage auf standardisierte Anbindungen ausgelegt ist.

Offenheit schafft die Voraussetzungen dafür, dass sich kommunale IT-Landschaften weiterentwickeln können, ohne bei jeder Erweiterung grundlegend neu aufgebaut werden zu müssen.

Cloud ist nicht gleich Cloud

Die Cloud ist auch für Kommunen ein Thema, allerdings wird die Diskussion über Cloud-Lösungen oft verkürzt geführt. Denn weniger die Technologie selbst ist entscheidend als vielmehr das zugrunde liegende Betriebsmodell und dessen Eignung. Verwaltungen müssen zahlreiche rechtliche und organisatorische Rahmenbedingungen berücksichtigen: Datenschutz nach DSGVO, Anforderungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) sowie hohe Erwartungen an Verfügbarkeit und Betriebssicherheit. Ebenso wichtig ist die Wahl geeigneter Rechenzentrumsstandorte. Hier sind Kommunen auf deutsche oder europäische Rechenzentren angewiesen, um rechtliche Vorgaben und die Anforderungen an Datensouveränität zu erfüllen.

Cloudbasierte Betriebsmodelle bieten Vorteile hinsichtlich Skalierbarkeit, automatisierter Updates, Hochverfügbarkeit und standardisierter Betriebsprozesse. Aber auch hybride Modelle mit einer Mischung aus Cloud-Services und lokalen Servern können sinnvoll sein: Dabei verbleiben besonders sensible Anwendungen oder Daten in kommunalen Infrastrukturen, während andere Dienste flexibel aus einer Cloud-Umgebung bezogen werden.

Modular statt monolithisch

Ein Hindernis für die Zukunftsfähigkeit kommunaler IT sind monolithische Systeme. Aufgrund ihrer Abgeschlossenheit erschweren sie Anpassungen und führen zu hohen Modernisierungskosten. Modulare

Plattformen verfolgen einen zeitgemäßeren Ansatz. Einzelne Komponenten übernehmen klar definierte Aufgaben und können unabhängig voneinander weiterentwickelt oder ersetzt werden. Dadurch lassen sich neue Funktionen schrittweise ergänzen, ohne das Gesamtsystem grundlegend verändern zu müssen.

Für Kommunen bietet dieses Architekturprinzip erhebliche Vorteile. Einzelne Prozesse können modernisiert werden, während andere Bereiche unverändert weiterlaufen. Diese Flexibilität gewinnt auch angesichts ständig neuer gesetzlicher Anforderungen an Bedeutung. Verwaltungsplattformen müssen dauerhaft anpassungsfähig bleiben, ohne umfangreiche Neuentwicklungen erforderlich zu machen.

Sicherheit darf Innovation nicht verhindern

Chatbots unterstützen bei Standardanfragen, Voicebots verbessern die telefonische Erreichbarkeit und KI-Anwendungen können Mitarbeitende bei Recherche, Dokumentenanalyse oder der Bearbeitung wiederkehrender Aufgaben entlasten: Digitale Tools eröffnen Kommunen neue Möglichkeiten, Verwaltungsleistungen effizienter und bürgerfreundlicher zu gestalten.

Der Einsatz dieser Technologien wirft jedoch Fragen hinsichtlich des Datenschutzes, der Informationssicherheit und Compliance auf. Erforderlich sind hier klare Leitplanken. Neue Anwendungen müssen sich in Sicherheits- und Governance-Strukturen einfügen. Zugriffsrechte, Protokollierung, Datenklassifizierung und Freigabeprozesse sorgen dafür, dass sich zum Beispiel KI-gestützte Anwendungen ohne Sicherheitseinbußen integrieren lassen.

Fazit

Kommunale IT wird niemals einen Endzustand erreichen. Gesetzliche Vorgaben verändern sich, technologische Entwicklungen schreiten voran und die Erwartungen von Bürgerinnen und Bürgern steigen. Digitalisierung ist deshalb ein fortlaufender Entwicklungsprozess. Um diesen Wandel erfolgreich zu gestalten, benötigen Verwaltungen Plattformen, die Sicherheit, Offenheit und Erweiterbarkeit unterstützen. Sie müssen Standards integrieren, neue Technologien aufnehmen und Investitionen langfristig absichern. Der Gegensatz besteht daher nicht zwischen Sicherheit und Offenheit, sondern zwischen starren, monolithischen Systemen und modernen Plattformarchitekturen. Eine durchdachte Architektur schafft die Voraussetzung dafür, dass Kommunen ihre Digitalisierung dauerhaft sicher, flexibel und zukunftsfähig gestalten können.

()

www.optigov.de

Stichwörter: IT-Infrastruktur, Cloud-Lösung, IT-Sicherheit