Cyber-Sicherheit

KI ist Segen und Fluch

[06.08.2026] Für Verwaltungen ist KI Segen und Fluch zugleich. Einerseits soll sie den Fachkräftemangel kompensieren und Bürgerservices beschleunigen, andererseits wird sie für Cyber-Angriffe genutzt. Oft fehlt eine IT-Infrastruktur, die KI und Cyber-Abwehr verbindet.

Ransomware-Angriffe auf Kommunalverwaltungen sind keine Ausnahme mehr. Allein in Bayern wurden 2024 laut Landeskriminalamt mehr als 48.000 Fälle von Cyber-Kriminalität registriert. Die Folgen solcher Angriffe sind oft gravierend: wochenlange Ausfälle von Bürgerservices, Verlust sensibler Melde-, Sozial- und Finanzdaten, erschüttertes Vertrauen in die digitale Verwaltung. Unterdessen hinkt das Risikobewusstsein der Realität hinterher: Während 80 Prozent der Befragten auf Landes- und Bundesebene die Bedrohungslage als sehr hoch einstufen, sind es auf kommunaler Ebene nur 58 Prozent. Zu diesem Ergebnis kommt eine repräsentative Umfrage von Civey aus dem November des vergangenen Jahres. Diese Diskrepanz zwischen Gefährdung und wahrgenommenem Risiko offenbart ein strukturelles Problem. Kommunen verfügen selten über dedizierte IT-Sicherheitsteams. Die vorhandenen Fachkräfte sind mit dem Tagesbetrieb ausgelastet. Gerade hier könnte KI durch automatisierte Anomalieerkennung, Echtzeitkorrelation von Sicherheitsereignissen oder die Entlastung von Sachbearbeitern bei Routinevorgängen den wirksamsten Hebel ansetzen.

Medizin ist zugleich das Gift

Was Kommunen als Verteidigungsinstrument dringend benötigen, setzen Angreifer längst systematisch ein. KI wird immer häufiger für täuschend echte Phishing-Mails, automatisierte Schwachstellen-Scans und die Skalierung ganzer Angriffskampagnen genutzt. Kurz gesagt: Dieselbe Technologie, die den Bürgerservice beschleunigen soll, vergrößert gleichzeitig die Angriffsfläche.

Hinzu kommt der wachsende Druck vonseiten des Gesetzgebers. Mit der Umsetzung der NIS2-Richtlinie in deutsches Recht verschärfen sich die Anforderungen an die Cyber-Sicherheit auch für kommunale Einrichtungen und deren Dienstleister erheblich. BSI-Grundschutz, die Basis-Absicherung Kommunalverwaltung und zunehmend auch BSI-C5-Testate entwickeln sich zum verbindlichen Standard. Parallel dazu müssen KI-Anwendungen in der Verwaltung den Vorgaben des EU AI Acts entsprechen – einem Regelwerk, das Transparenz, Risikoklassifizierung und menschliche Aufsicht vorschreibt. Kommunen geraten damit in eine doppelte Compliance-Herausforderung: Sie müssen sowohl ihre Sicherheitsarchitektur als auch ihre KI-Governance aufrüsten. Und das mit begrenzten Budgets und ohne ausreichendes Fachpersonal. Wer hier nicht rechtzeitig die Weichen stellt, riskiert nicht nur Sicherheitslücken, sondern auch regulatorische Konsequenzen.

Wo ein Wille ist nicht immer ein Weg

Doch selbst dort, wo der politische Wille vorhanden ist, scheitert die KI-Modernisierung häufig an einer einfachen Hürde: der fehlenden Infrastruktur. Viele Kommunen betreiben ihre IT noch in hauseigenen Serverräumen oder bei kleinen regionalen Dienstleistern. Diese sind jedoch weder für GPU-intensive KI-Workloads noch für professionelles Security-Monitoring ausgelegt. Für Chatbots, KI-gestützte

Antragsverarbeitung oder automatisierte Bescheiderstellung sind dagegen leistungsfähige, hochverfügbare und datenschutzkonforme Rechenumgebungen erforderlich.

Ein Ausweg sind spezialisierte, zertifizierte Infrastrukturen, die Kommunen Zugang zu professioneller Rechenleistung ermöglichen, ohne dass sie selbst ein Rechenzentrum aufbauen müssen. Dabei ist nicht allein die Leistungsfähigkeit der gewählten Plattform entscheidend, sondern auch ihre Datensouveränität. Bürgerdaten, Registerdaten und Fachverfahren unterliegen besonderen Schutzanforderungen und dürfen den europäischen Rechtsraum nicht verlassen. Das ist insbesondere vor dem Hintergrund des US CLOUD Act von Bedeutung, da dieser amerikanischen Behörden einen extraterritorialen Zugriff auf Daten bei US-Anbietern einräumt – selbst dann, wenn diese auf europäischen Servern liegen. Anbieter wie noris network setzen deshalb konsequent auf das Prinzip der digitalen Souveränität und betreiben ihre Cloud-Plattformen ausschließlich in deutschen Hochsicherheitsrechenzentren, ohne von US-amerikanischen Hyperscalern abhängig zu sein.

Kompetenzen auslagern

Ebenso entscheidend ist die Frage, wie Kommunen ihre wachsende Angriffsfläche professionell überwachen lassen können. Ein Security Operations Center, das IT-Umgebungen rund um die Uhr analysiert, Sicherheitsereignisse mittels KI-gestützter Verfahren korreliert und im Ernstfall eine professionelle Incident Response sicherstellt, übersteigt die Kapazitäten der meisten kommunalen IT-Abteilungen. Diese Lücke können Managed-Security-Dienste schließen, indem sie Ransomware-Schutz, Intrusion Detection und forensische Kompetenz als Service bereitstellen, statt diese Leistungen selbst erbringen zu müssen.

Neben der Sicherheitsfrage stellt sich für Kommunen, die KI-Anwendungen produktiv betreiben wollen, auch die Frage nach der Rechenleistung. Dedizierte GPU-Cluster und Private-AI-Plattformen ermöglichen die datensouveräne Nutzung großer Sprachmodelle über standardisierte API-Endpunkte, ohne dass Bürgerdaten oder Verwaltungsinformationen an internationale Anbieter fließen. Die Verarbeitung findet in deutschen Rechenzentren statt, unterliegt deutschem Recht und ermöglicht eine vollständige Kontrolle über die eingesetzten Modelle sowie die zugrunde liegenden Daten. Klar ist: Die Herausforderungen, vor denen kommunale Verwaltungen stehen, lassen sich nicht isoliert voneinander lösen. Sie erfordern ein integriertes Konzept, das sichere Infrastruktur, professionelle Cyber-Abwehr und souveräne KI-Kapazitäten verbindet.

()

www.noris.de

Dieser Beitrag ist in der Ausgabe August 2026 von Kommune21 erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit, Cyber-Kriminalität, künstliche Intelligenz, NIS2, noris network