Große Bedeutung für Kommunen:

Technologische Souveränität und Cybersicherheit im KI-Zeitalter

Technologische Souveränität wird oft als Angelegenheit großer Unternehmen oder nationaler Regierungen dargestellt. Tatsächlich beginnt ihr Einfluss viel näher an den Bürgerinnen und Bürgern: in den Kommunen, die täglich unverzichtbare öffentliche Dienstleistungen erbringen.

Ein Beitrag von
Roberto Viola

Kommunen verwalten Daten und Infrastrukturen, die für das tägliche Leben von zentraler Bedeutung sind: öffentliche Verwaltung, Mobilität, soziale Dienstleistungen, Energie, Wasser, Schulen und Notfallkoordination. Wenn diese Systeme durch einen Cyberangriff gestört werden, sind die Folgen unmittelbar und unübersehbar. Im Jahr 2025 identifizierte die EU-Agentur für Cybersicherheit (ENISA) die öffentliche Verwaltung als den am stärksten angegriffenen Sektor in der EU. Kommunen sind oft attraktive Ziele, weil sie sensible Daten speichern, bürgerorientierte Systeme betreiben und Dienstleistungen erbringen, die nicht ohne Weiteres unterbrochen werden können.

Die Möglichkeit, sich bei kritischen digitalen Funktionen auf vertrauenswürdige Technologien, sichere Infrastruktur und widerstandsfähige Lieferketten verlassen zu können, steht im Mittelpunkt der europäischen Vision für technologische Souveränität. Konkret bedeutet dies, dass öffentliche Verwaltungen in der Lage sein sollten, sichere digitale Lösungen zu wählen und neue Abhängigkeiten in Bereichen zu vermeiden, die für unsere Sicherheit zunehmend an Bedeutung gewinnen.

Das im Juni 2026 verabschiedete **Paket zur technologischen Souveränität** der Europäischen Kommission spiegelt dieses Bestreben wider. Mit dem vorgeschlagenen Gesetz zur Entwicklung von Cloud- und KI-Technologien sowie der EU-Open-Source-Strategie soll sichergestellt werden, dass Europa die Technologien entwickeln, einsetzen und ihnen vertrauen kann, von denen seine Wirtschaft, seine öffentlichen Dienste und seine Demokratie zunehmend abhängen.

Foto: Berlin IckLiebeDir / flickr.com

Kommunen bieten viele Dienstleistungen digital an – das macht sie gegenüber Cyberangriffen verwundbar

KI verändert die Bedrohungslage – für Angreifer und Verteidiger

Im Zentrum der technologischen Souveränität Europas steht heute die künstliche Intelligenz (KI). Bei der KI geht es jedoch nicht nur um technologischen Wettbewerb, sondern um die Sicherheit unserer Union insgesamt.

Künstliche Intelligenz verändert die Cybersicherheit auf beiden Seiten. Fortschrittliche KI-Modelle können kleinen IT-Teams dabei helfen, Bedrohungen schneller zu erkennen, Schwachstellen zu analysieren und die Reaktion auf Vorfälle zu koordinieren. Dies ist ein echter Vorteil für Kommunen, in denen die Ressourcen begrenzt sind und die Zahl der digitalen Dienste stetig wächst.

Doch dieselben Möglichkeiten stehen auch böswilligen Akteuren zur Verfügung. KI ermöglicht es Angreifern, Schwachstellen

Zum Autor:

Roberto Viola ist Generaldirektor der Generaldirektion Kommunikation, Netze, Inhalte und Technologien (GD CONNECT) bei der Europäischen Kommission.

schneller zu identifizieren, Angriffe zu automatisieren und deren Raffinesse zu steigern. Das Zeitfenster zwischen der Entdeckung einer Schwachstelle und ihrer Ausnutzung wird immer kleiner. Für Kommunen bedeutet dies, dass langsame Patch-Zyklen, veraltete Software und unzureichend geschultes Personal keine akzeptablen Risiken mehr darstellen.

Was die EU dagegen unternimmt

Europa hat in den vergangenen Jahren eine solide rechtliche Grundlage geschaffen. Die **NIS2-Richtlinie** verpflichtet Betreiber kritischer Infrastrukturen, darunter Trinkwasserversorgung, Abwasserentsorgung, Verkehr, Energie und öffentliche Verwaltung, über ein robustes Cybersicherheits-Risikomanagement zu verfügen. Behörden der regionalen Ebene, wie sie von den Mitgliedstaaten gemäß nationalem Recht definiert werden und die Dienste erbringen, deren Störung erhebliche Auswirkungen auf kritische gesellschaftliche oder wirtschaftliche Aktivitäten haben könnte, fallen in den Anwendungsbereich der Richtlinie. Die Mitgliedstaaten können zudem vorsehen, dass die NIS2-Vorschriften auch für Behörden der lokalen Ebene gelten. Der **Cyber Resilience Act** schreibt „Security-by-Design" für Software- und Hardwareprodukte vor, die auf den europäischen Markt gebracht werden. Und das KI-Gesetz bietet den weltweit ersten rechtsverbindlichen Rahmen für den Umgang mit Risiken durch fortschrittliche KI-Systeme.

Auf dieser Grundlage hat die Europäische Kommission im Juli 2026 einen **Aktionsplan für Cybersicherheit und künstliche Intelligenz** verabschiedet. Er gliedert sich in drei miteinander verknüpfte Ziele, die gemeinsam die zentrale Herausforderung angehen: Wie können europäische Organisationen, einschließlich Kommunen, von fortschrittlicher KI im Bereich der Cybersicherheit profitieren, ohne neue Abhängigkeiten zu schaffen?

Foto: Europäische Union, 2026 / Roméo Boetzlé

Henna Virkkunen, Exekutiv-Vizepräsidentin der Europäischen Kommission, präsentierte bei einer Pressekonferenz im Juli 2026 den Aktionsplan zu Cybersicherheit und KI

Sicherstellen, dass fortschrittliche KI vertrauenswürdig ist

Das erste Ziel besteht darin, sicherzustellen, dass KI-Tools, die in sensiblen Umgebungen eingesetzt werden, wirklich sicher sind und unabhängig bewertet wurden.

Eine neue europäische Bewertungskapazität für KI-Modelle wird unabhängige Bewertungen der KI-Fähigkeiten und der entsprechenden Maßnahmen zur Risikominderung ermöglichen. Dies ist für Kommunen, andere öffentliche Verwaltungen und die Gesellschaft insgesamt von Bedeutung: Fundierte Sicherheitsbewertungen, die vom Anbieter

Fünf Prioritäten für europäische Kommunen

Der politische Rahmen ist wichtig, aber er zeigt nur dann Wirkung, wenn Kommunen entsprechend handeln. Fünf Prioritäten sind dabei von besonderer Bedeutung:

1. Behandeln Sie Cybersicherheit als eine strukturelle Führungsaufgabe, nicht nur als technische Angelegenheit. Bürgermeisterinnen, Bürgermeister und leitendes Verwaltungspersonal sollten wissen, welche wesentlichen Dienste von digitalen Systemen abhängen, wo die Hauptrisiken liegen und wer im Ernstfall verantwortlich ist.
2. Sorgen Sie für solide Grundlagen. Patches, Backups, Zugriffskontrolle, Sensibilisierung des Personals und die Planung der Reaktion auf Vorfälle bleiben die erste Verteidigungslinie. KI-gestützte Bedrohungen machen diese Grundlagen noch dringlicher, nicht weniger wichtig.
3. Erfassen Sie Ihre Abhängigkeiten. Ermitteln Sie, welche Software, Cloud-Dienste, Open-Source-Komponenten und externen Anbieter für Ihre Dienste unverzichtbar sind. Technologische Souveränität beginnt damit, zu verstehen, wovon Sie abhängig sind, und was passiert, wenn diese Zugänge entzogen werden.
4. Setzen Sie KI-Tools mit Sicherheitsvorkehrungen ein. KI kann die Cybersicherheit unterstützen, muss jedoch sorgfältig eingesetzt werden. Setzen Sie auf erprobte Lösungen, bewährte Leitlinien und klare Beschaffungsanforderungen statt auf unkontrollierte Experimente in sensiblen Systemen.
5. Kooperieren Sie mit anderen und investieren Sie in Menschen. Keine Kommune kann KI-gestützte Bedrohungen allein bewältigen. Die Zusammenarbeit mit nationalen Cybersicherheitsbehörden, der ENISA und anderen Kommunen ist unerlässlich. Technologie allein reicht nicht aus – es braucht geschulte Fachkräfte. Deshalb sind die Bemühungen der EU um Cyberkompetenzen für die Kommunalverwaltung von unmittelbarer Bedeutung.

durchgeführt werden, tragen zur Minderung systemischer Risiken durch KI-Modelle bei, auch im Cyberspace.

Ein europäischer Fahrplan für den strukturierten Zugang zu fortschrittlicher KI wird klare Kriterien definieren, nach denen europäische Organisationen zeitnah Zugang zu fortschrittlichen KI-Modellen erhalten können, einschließlich Notfallmaßnahmen für den Fall, dass der Zugang eingeschränkt oder entzogen wird, sei es durch einen Anbieter oder eine ausländische Behörde. Dies ist eine direkte Reaktion auf das oben beschriebene Abhängigkeitsrisiko: Europa benötigt einen Plan für den Fall, dass der Zugang zu einem kritischen KI-Tool plötzlich unterbrochen wird.

Schließlich wird eine sichere Testplattform, einschließlich Cyber-Ranges, die Umgebungen kritischer Infrastrukturen simuliert, es Organisationen ermöglichen, KI-Tools unter realistischen Bedingungen zu testen, ohne echte Systeme einem Risiko auszusetzen. Dies kann wichtige Erkenntnisse darüber liefern, wie KI zur Stärkung der Cyber-Resilienz eingesetzt werden sollte. Diese Erkenntnisse können Kommunen, die den Einsatz von KI-gestützten Tools zur Bedrohungserkennung oder zur Reaktion auf Vorfälle in Betracht ziehen, anschließend anwenden.

Unterstützung bei der Abwehr KI-gestützter Angriffe

Das zweite Ziel ist für kommunale IT-Teams von unmittelbarer Relevanz. Es konzentriert sich darauf, die Lücke zwischen der Geschwindigkeit, mit der Angreifer heute Schwachstellen ausnutzen können, und der Geschwindigkeit, mit der Organisationen reagieren können, zu schließen.

Die vollständige Umsetzung der NIS2-Richtlinie ist hierfür der Ausgangspunkt. Kommunen, die in ihren Geltungsbereich fallen, sollten die Einhaltung der Vorschriften nicht als bürokratische Aufgabe, sondern als operative Grundvoraussetzung betrachten. Dies beinhaltet dokumentierte Risikomanagementprozesse, getestete Pläne zur Reaktion auf Vorfälle und klare Zuständigkeiten auf Führungsebene.

Ebenso dringend ist die Beschleunigung des Patch-Managements. Die ENISA wird Leitlinien und bewährte Verfahren veröffentlichen, die speziell auf kleinere Organisationen mit begrenzten Ressourcen zugeschnitten sind. Sie sollen dabei helfen, Prioritäten zu setzen, also festzulegen, welche Schwachstellen zuerst behoben werden müssen und wie dies effizient geschehen kann. Das Ziel ist es, das Zeitfenster zu verkürzen, in dem Angreifer – zunehmend unterstützt durch KI – bekannte Schwachstellen ausnutzen können.

Der Aktionsplan sieht zudem den Start einer Kampagne zur Stärkung der Widerstandsfähigkeit kritischer Open-Source-Systeme vor. Dies ist von Bedeutung, da die Codebasen kritischer Infrastrukturen – einschließlich derer, die von Kommunen genutzt werden – im Durchschnitt einen hohen Anteil an ungepatchten Open-Source-Schwachstellen enthalten. Die Ressourcen sollen hier darauf konzentriert werden, zunächst die kritischsten Probleme zu beheben. Ein freiwilliges Sponsoring-Programm wird Open-Source-Projekte mit Organisationen zusammenbringen, die bereit sind, deren Wartung und Sicherheit zu unterstützen, und so ein nachhaltigeres Modell für die Open-Source-Komponenten schaffen, auf die öffentliche Dienste im Hintergrund angewiesen sind.

Aufbau eigener europäischer KI-Kapazitäten

Das dritte Ziel ist weiter in die Zukunft gerichtet. Europa muss eigene Spitzenkapazitäten entwickeln. Dies bedeutet Investitionen in eine souveräne Recheninfrastruktur, insbesondere durch bestehende KI-Fabriken und künftige KI-Gigafabriken, um die Grundlage für die Entwicklung, Erprobung und den großangelegten Einsatz europäischer KI-Modelle zu schaffen.

Für Kommunen ist die unmittelbare Auswirkung dieses Ziels die Personalentwicklung. Fortschrittliche Tools sind nur dann nützlich, wenn die Menschen, die sie bedienen, verstehen, was sie tun. Im Rahmen der EU-Akademie für Cybersicherheitskompetenzen werden spezielle Schulungsmodule entwickelt, mit dem ausdrücklichen Ziel, sicherzustellen, dass Fachleute für Cybersicherheit in ganz Europa, einschließlich der Kommunalverwaltungen, effektiv mit KI-gestützten Werkzeugen arbeiten können. Kommunen sollten diese Entwicklung im Auge behalten, um sicherzustellen, dass ihr Personal Zugang zu entsprechenden Schulungen erhält, sobald diese verfügbar sind.

Technologische Souveränität entsteht nicht zentral. Sie entsteht in jedem Rathaus, jedem Kontrollraum eines Wasserwerks und jeder kommunalen IT-Abteilung, die Cybersicherheit ernst nimmt. Im Zeitalter der KI ist dies eine Aufgabe für die gesamte Gesellschaft und Kommunen sind für deren Erfolg unverzichtbar. ■

Infos

Paket zur technologischen Souveränität Europas:
https://ec.europa.eu/commission/presscorner/detail/de/ip_26_1187

NIS-2-Richtlinie:
https://digital-strategy.ec.europa.eu/de/policies/nis2-directive

Aktionsplan für Cybersicherheit und künstliche Intelligenz:
https://digital-strategy.ec.europa.eu/de/library/eu-action-plan-cybersecurity-and-artificial-intelligence