DEUTSCHER LANDKREISTAG

Kommunale Informationssicherheit nachhaltig und übergreifend stärken

Eine leistungsfähige Verwaltung bildet den Grundpfeiler für die Funktionsfähigkeit und Legitimation des Staates. Die Landkreise übernehmen wesentliche Vollzugsaufgaben und spielen eine zentrale Rolle bei der Gewährleistung sozialer Sicherheit oder in der Bewältigung von Krisenlagen wie Pandemien und Naturkatastrophen. Die Kommunen stellen dabei den zentralen Berührungspunkt zwischen dem Staat sowie den Bürgern und Unternehmen dar. Die Funktionsfähigkeit des Staates prägt sich somit in der Außenwirkung über leistungsfähige Kommunen. Durch die fortschreitende Digitalisierung ist diese unmittelbar mit einer funktionsfähigen IT gekoppelt. Die Ereignisse zu den bekannten Cyberangriffen auf öffentliche IT-Dienstleister, Landkreise, Städte und Gemeinden sowie die daraus resultierende eingeschränkte Handlungsfähigkeit, Folgekosten und Vertrauensverluste gegenüber der Öffentlichkeit verdeutlichen die Bedeutung der Informationssicherheit in den Kommunen.

Dennoch bleibt das Thema Informationssicherheit in der politischen Debatte bislang unterrepräsentiert. Es fehlt an einem klaren, gesamtstaatlichen Ansatz, der die Kommunen als tragende Säule des Verwaltungsvollzugs und der Daseinsvorsorge in den Blick nimmt. Angesichts der zunehmenden Digitalisierung und den Anforderungen, die sich durch das Onlinezugangsgesetz, die Registermodernisierung sowie Smarte Landkreise ergeben, ist die Bedeutung einer robusten Informationssicherheit auf kommunaler Ebene kaum zu überschätzen.

Zur nachhaltigen Stärkung der kommunale Informationssicherheit bedarf es deshalb gezielter bundesländerübergreifender Unterstützungsmaßnahmen, die die Kommunen in ihrer Arbeit wirksam entlasten und stärken.

1. IT-Grundschutz vereinfachen

Der Schlüssel zur Informationssicherheit ist ein übergreifendes und systematisches Managementsystem für Informationssicherheit (ISMS). Um ein solches System aufzubauen, stellt das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit dem IT-Grundschutz eine etablierte und übertragbare Methodik zur Verfügung. Der IT-Grundschutz gilt dabei als bürokratisch und gerade für kleine Organisationen als äußerst herausfordernd in der Umsetzung (ca. 1.100 Maßnahmen, umfassende Dokumentationspflichten). Hier muss gegengesteuert werden. Es bedarf einer gezielten und kompetenten Unterstützung der Kommunen beim Aufbau des IT-Grundschutzes. Dazu gehören niedrigschwellige Einstiegshilfen wie Wege in die Basisabsicherung und die Verknüpfung mit bestehenden Konzepten der Länder (z. B. Sicherheit für Kommunen in Schleswig-Holstein), welche anschließend den Weg in die Standardabsicherung ebnen müssen. Dieser seit wenigen Jahren eingeschlagene Weg ist unbedingt weiter zu intensivieren und finanziell zu unterlegen. Über kostenfreie Testate oder Zertifikate müssen dabei Zwischenerfolge ausweisbar sein. Arbeitsbeispiele des BSI (z. B. das fiktive Unternehmen Recplast GmbH) müssen um kommunale Beispiele ergänzt werden.

2. ISMS-Tool als Open-Source-Software entwickeln

Das ISMS der öffentlichen Verwaltung für eine digitalisierte und informationssichere Verwaltung basiert auf hundertseitenlangen PDF-Dokumenten. Diese Grundlagen müssen grundsätzlich neu gedacht werden. Ein ISMS-Tool auf Open-Source-Basis, entwickelt oder weiterentwickelt durch das BSI, könnte die Umsetzung der Informationssicherheit auf kommunaler Ebene

erleichtern. Dieses Tool sollte durch die Integration von Künstlicher Intelligenz (KI) die Informationssicherheitsbeauftragten der Kommunen bei der schrittweisen Einführung eines ISMS nach IT-Grundschutz unterstützen und durch intelligente Vorlagen, Zeitpläne, die Integration von Grundschutzprofilen sowie Handlungsempfehlungen die Umsetzung vereinfachen und optimieren. Dabei muss von Beginn an die kommunale Perspektive mitgedacht werden. Ein solches Vorhaben könnte in enger Kooperation mit dem Zentrum für digitale Souveränität (ZenDiS) auf eine nachhaltige Grundlage gestellt werden, um ein starkes Open-Source-Ökosystem für die Informationssicherheit in der öffentlichen Verwaltung zu schaffen.

3. Verbindliche Standards schaffen

Die Benennung von Informationssicherheitsbeauftragten, die Definition von Meldewegen und Mindeststandards an ein ISMS sollten gesetzlich vorgegeben werden. Dazu gehört eine angemessene kommunale Finanzausstattung. Unterschiedliche Regelungen von verschiedenen Rechtsakten sind zu vermeiden und eine Harmonisierung von Anforderungen anzustreben (EU-Zahlstelle, iKfz etc.). Das BSI sollte zukünftig obligatorisch bei der Definition von Anforderungen der Bundesbehörden gegenüber den Kommunen eingebunden werden.

Informationssicherheit muss außerdem zukünftig von Beginn an bei der Konzeption von Gesetzen und Programmen als Mittel der Umsetzung mitgedacht werden. Eine nachträgliche Definition von Anforderungen, wie dies bei dem OZG geschehen ist, ist unbedingt zu vermeiden. Der IT-Planungsrat sollte zukünftig klar definieren, welche Anforderungen ebenenübergreifende Verfahren zu erfüllen haben. Die Kommunen müssen auf die Sicherheit der zentralen Verfahren bei einer für die Ende-zu-Ende notwendigen Verzahnung mit den eigenen IT-Infrastrukturen vertrauen können.

4. IT-Sicherheitsanalysen anbieten

Im Rahmen von IT-Sicherheitsanalysen werden Kommunen gemäß eines standardisierten Fragenkataloges und technischer Stichproben (Netzwerk, Firewalls, Verzeichnisdienste etc.) beurteilt. Teil der Prüfung sind auch die Sichtungen von Dienstanweisungen, Richtlinien oder Dokumentationen. Anhand von Vorgesprächen, vor Ort-Terminen und einer individuellen Ergebnisaufbereitung sind umfassende Handlungsempfehlungen für die Kommunen möglich. Vom Ist-Zustand ausgehend können anschließend gezielte Maßnahmen zur Verbesserung des IT-Sicherheitsniveaus angestrebt werden. An erfolgreiche Umsetzungen sollte dabei angeknüpft und das Angebot flächendeckend zur Verfügung gestellt werden.

5. Schulungsangebote ausbauen

Es bedarf eines kuratierten Angebots von Schulungen, das auf die Bedürfnisse der Kommunalverwaltungen spezialisiert die notwendigen Kompetenzen für die IT-Sicherheitsbeauftragten vermittelt. Flankierend wären digital abrufbare Schulungsangebote sinnvoll, die auf bestehenden Plattformen wie dem KommunalCampus aufbaut, um einen flexiblen Kompetenzerwerb in der Breite zu ermöglichen. Darüber hinaus sollten flächendeckende Awareness-Kampagnen, beispielsweise in Form von Materialien (White-Label) wie Plakaten und Informationsbroschüren, bereitgestellt werden, um das Bewusstsein für Informationssicherheit auf kommunaler Ebene flächendeckend zu stärken und Synergieeffekte zu erzielen. Die Bereitstellung von Awarenessplattformen mit Angriffssimulationen zur Sensibilisierung der Mitarbeiter würden den Handlungsstrang sinnvoll ergänzen.

6. Warn- und Informationsdienste zur Verfügung stellen

Über Warn- und Informationsdienste werden Informationen zu neuen Schwachstellen und Sicherheitslücken sowie aktuellen Bedrohungen für IT-Systeme veröffentlicht. Entsprechende Dienste sind mit einer für die Kommunen relevanten Ersteinschätzung und schnellen Weiterleitung für eine kurze Reaktionsmöglichkeit in den Kommunen einzurichten.

7. Vorfalls- und Notfallmanagement implementieren

Für den Fall eines gravierenden IT-Sicherheitsvorfalls müssen Notfallpläne etabliert werden, die den Alternativbetrieb der wichtigsten kommunalen IT-Infrastrukturen – wie Telefonie und Computer – sichern. Hier sollten die Länder Infrastrukturen zur Verfügung stellen. Über Plattformen wie Open Desk könnte eine schnelle erste Handlungsfähigkeit hergestellt werden.

Zudem müssen konkrete Handlungsempfehlungen zur Einführung eines „Business-Continuity-Managements" entwickelt und Kommunen bei der Durchführung von Cybersicherheitsübungen unterstützt werden.

Die Einrichtung von „MIRT-Strukturen" (Mobile-Incident-Response-Teams) für Kommunen spielt eine weitere wichtige Rolle. Häufig werden Kommunen mit der Bewältigung von Cyberangriffen sich selbst überlassen. Des Weiteren stellen sich Fragen wie mit umfassenden Cyberangriffen auf mehrere Kommunen und die Länder umgegangen werden kann. Hier benötigt es Lösungen wie Rahmenverträge mit auf Cyberangriffe spezialisierte Dienstleister.

8. IT-Infrastruktur und Fachverfahren konsolidieren und befähigen

Eine Vielzahl an kleinteiligen kommunalen IT-Dienstleistern, Eigenbetrieben und Fachverfahren erschwert das Erreichen eines hohen IT-Sicherheitsstandards. Neben der durch die Kommunen selbst anzugehenden Konsolidierung der IT-Infrastruktur kann eine gemeinsame Cloud-Infrastruktur wie bspw. die Deutsche Verwaltungscloud zukünftig eine wichtige Rolle für einen informationssicheren Betrieb von Anwendungen einnehmen. Hierzu ist von den Ländern und dem Bund eine auskömmliche Finanzierung der Deutschen Verwaltungscloud vorzusehen, um eine moderne, sichere und leistungsfähige IT-Infrastruktur für die öffentliche Verwaltung sicherzustellen. Neben der IT-Infrastruktur ist auch die Anwendungsebene in die Betrachtung einzubeziehen. Hier bedarf es der Prinzipien „Security by design" und „Privacy by Design" sowie einer umfassenden Produktstrategie gegenüber den Softwareanbietern als Voraussetzung für zukünftige – vor allem ebenenübergreifende – Softwareentwicklungen der öffentlichen Hand.

9. IT-Planungsrat für die Kooperation in der Informationssicherheit stärken

Die Länder bieten bereits eine Reihe von Unterstützungsmaßnahmen. Diese stehen allerdings nur wenigen Kommunen zur Verfügung. Der IT-Planungsrat sollte hier eine stärkere koordinierende Funktion wahrnehmen und bspw. über zentrale Budgets die Kommunen mit übergreifenden Angeboten unterstützen. Die im Papier dargelegten Vorschläge sind dafür prädestiniert. Das Schwerpunktthema Informationssicherheit des IT-Planungsrates bietet eine gute Möglichkeit, das Thema anzugehen.

10. Fazit

Mit den hier genannten Maßnahmen kann die Informationssicherheit auf kommunaler Ebene nachhaltig gestärkt und die Resilienz der Verwaltung gegenüber den zunehmenden Cyberbedrohungen verbessert werden. Nur durch eine klare politische Zielsetzung und durchdachte Umsetzungsstrategien lassen sich die drängenden Herausforderungen in diesem Bereich bewältigen.

Berlin, den 17.3.2025