kurzum
Nr. 147 / November 2023

KONRAD ADENAUER STIFTUNG

Zwischen den Ländern und Kommunen hakt es noch

Wie die kommunale Informationssicherheit gestärkt werden kann

Ferdinand A. Gehringer

In den vergangenen Jahren kam es zu zahlreichen IT-Sicherheitsvorfällen in kommunalen Verwaltungen und Einrichtungen. Das Onlinezugangsgesetz (OZG) verpflichtet die Kommunalverwaltungen, ihre Prozesse zu digitalisieren. Immer mehr sensible Daten von Bürgerinnen und Bürgern werden digital verarbeitet. In vielen der bundesweit circa 10.900 Kommunen ist die IT-Infrastruktur veraltet, sind die IT-Systeme nicht ausreichend geschützt, die finanziellen Mittel für Informationssicherheit zu gering und der Personalbedarf zu hoch. Das macht Kommunen in Deutschland zu leichten Opfern für Angriffe. In unserer Studie *Kommunale Informationssicherheit und Resilienz – eine Analyse des deutschen Ansatzes zur Förderung* von der Autorin Julia Schuetze werden Handlungsoptionen aufgezeigt, die nachfolgend aufgegriffen oder ergänzt werden.

Das Verhältnis zwischen den Ländern und Kommunen ist noch erheblich ausbaufähig

Sowohl vom Bund als auch von den Ländern werden den Kommunen Leistungsangebote zur Verfügung gestellt, die die kommunale Informationssicherheit und Resilienz erhöhen sollen. **Die Zusammenarbeit zwischen den Ländern und ihren Kommunen ist entscheidend,** da regionale Unterschiede und Besonderheiten im föderalen System besser erfasst werden und vor allem die Kommunen auf die Unterstützung der Länder angewiesen sind. Oftmals fehlt es den Kommunen an der Kenntnis über die zur Verfügung stehenden Leistungen. **Eine bundesweite und fortlaufend aktualisierte Übersicht der Leistungsangebote könnte zunächst Abhilfe schaffen** – beispielsweise ausgehend vom Cybersicherheitskompass. Kooperationen unter den Ländern über bestehende Leistungen gibt es bis dato nur sehr eingeschränkt. Wenn Kooperationen aufgebaut oder verstetigt werden, könnten sich doppelnde oder überschneidende Leistungsangebote (wie Handreichungen, Checklisten oder Übungsformate) vermeiden lassen und länderübergreifend zur Verfügung gestellt werden.

Durch landesgesetzliche Regelungen einen einheitlichen Rahmen und Standards schaffen

Ansprechpartnerinnen oder Ansprechpartner für Informationssicherheit in den Kommunen haben die Länder häufig nicht. Hier könnte eine landesgesetzliche Regelung (wie das SächsISichG) kommunale Einrichtungen und Stellen zur Benennung eines Informationssicherheitsbeauftragten verpflichten. Die im NIS-2-Umsetzungsgesetz festgelegten Mindeststandards für kritische Sektoren finden voraussichtlich keine Anwendung auf Kommunen. **Deshalb sollten im Rahmen einer landesgesetzlichen Regelung Meldepflichten und -wege für Vorfälle, Standards für Sicherheitskonzepte und Austauschplattformen für die kommunale Informationssicherheit eingeführt werden.**

Länder sollten sich auf einheitliche Funktionen verständigen

Die Länder definieren ihre Funktion, die sie bei der Unterstützung der kommunalen Informationssicherheit einnehmen, unterschiedlich. Im Rahmen der Studie unterscheidet die Autorin Julia Schuetze zwischen administrativer (beispielsweise durch Rahmenverträge), bildender (beispielsweise durch Schulungen), finanzierender (beispielsweise durch Mittelvergabe), informierender (beispielsweise durch Orientierungshilfen) und operativer Funktion (beispielsweise durch Tools zur Gefahrendetektion). **Ein einheitlich bundesweites Verständnis über die Funktion(en) der Länder sollte zwingend geschaffen werden, um die Verantwortungsbereiche abzugrenzen, Unterstützungsleistungen gezielt anbieten zu können und um finanzielle und personelle Ressourcen zu sparen.**

Regionale und länderübergreifende Sicherheitsoperationszentren (SOZ) einrichten

Den Kommunen fehlt vorwiegend Unterstützung im administrativen und operativen Bereich. **Demnach sollten Länder mehr administrative und operative Funktionen erfüllen.** So könnten etwa regionale Sicherheitsoperationszentren (SOZ), beispielsweise angelehnt an das Hessen3C CyberCompetenceCenter, die auch länderübergreifend beziehungsweise im Zusammenschluss von mehreren Ländern arbeiten, eingerichtet werden. Diese SOZ werden entweder vom Land beziehungsweise mehreren Ländern selbst oder durch einen externen IT-Dienstleister betrieben. Eine 24/7-Hotline und ein Notfallreaktionsteam (CERT-Team) könnte so bei der Cybervorfallbearbeitung unterstützen. Zugleich könnte dieses SOZ einen Warn- und Informationsdienst betreiben und den Kommunen notwendige Informationen über Vorfälle, Bedrohungen oder neue Schwachstellen über eine Plattform individualisierbar liefern. Weitergehend könnten hierüber auch Tools zur Gefahrendetektion (Softwareprogramme, Webseiten-Checks oder Online-Antiviren-Suche) zur Verfügung gestellt werden.

Das SOZ könnte als rahmengebende Einrichtung für den Austausch der Kommunen untereinander dienen.

Administrative Unterstützung durch Rahmenverträge gewährleisten und finanzielle Ressourcen sparen

Alternativ wäre eine administrative Unterstützung der Kommunen denkbar. Länder greifen teilweise selbst auf externe IT-Dienstleister zurück und binden diese rahmenvertraglich an sich. Externe Dienstleister könnten auf kommunaler Ebene tätig werden, sodass die Leistungen zunächst über das Land durch die Kommunen bezogen werden und die Kommunen gegenüber dem Land für die entstehenden Kosten aufkommen. **Diese rahmenvertragliche Einbindung der Kommunen könnte wiederum vom Land als Anreizsystem genutzt werden:** Je mehr eine Kommune in die Informationssicherheit investiert, desto geringer könnte der Ausgleichsbetrag gegenüber dem Land ausfallen. So wäre eine gezielte und unbürokratische finanzielle Unterstützung der Kommunen gesichert und die Länder hätten einen besseren Überblick über die Investitionen und den Zustand der kommunalen Informationssicherheit.

Konrad-Adenauer-Stiftung e. V.

Ferdinand A. Gehringer
Innere- und Cybersicherheit
Analysen und Beratung

ferdinand.gehringer@kas.de