Stiftung Neue Verantwortung

KONRAD ADENAUER STIFTUNG

Kommunale Informations-sicherheit und Resilienz

Eine Analyse des deutschen Ansatzes zur Förderung

Julia Schuetze

kas.de

Auf einen Blick

In den vergangenen Jahren kam es vermehrt zu IT-Sicherheitsvorfällen bei denen kommunale Verwaltungen in Deutschland betroffen waren. Städte, Landkreise und Gemeinden stellen eine Vielzahl staatlicher Leistungen bereit. Nirgends kommen Bürgerinnen und Bürger so unmittelbar mit der öffentlichen Hand in Berührung wie in den Kommunen. Kommt es hier zu IT-Sicherheitsvorfällen, sind die Schäden für die Einwohnerinnen und Einwohner spürbar. Im schlimmsten Fall funktioniert die kommunale Verwaltung bei solchen Vorfällen nur sehr eingeschränkt. Für die deutsche Cybersicherheitspolitik ist der Schutz kommunaler Einrichtungen deshalb eine wichtige strategische Aufgabe.

Kommunen sind gemäß Subsidiaritätsprinzip zunächst einmal selbst für ihre Informationssicherheit zuständig. Der aktuelle deutsche Ansatz zur Förderung von Informationssicherheit und Resilienz von Kommunen sieht eine Unterstützungsfunktion von Bund und Ländern vor. Bund und Länder wollen Anreize setzen, die Kommunen dazu motivieren, ihre Resilienz zu verbessern.

Die Analyse zeigt, dass Unterstützungsleistungen von Bund und Ländern unterschiedlich verfügbar sind, je nachdem, wo eine Kommune liegt.

Die Weiterentwicklung des Ansatzes sollte vor allem konkrete Bedarfe der Kommunen berücksichtigen. Darüber hinaus sollten bestimmte praxis-geprüfte Leistungen für alle Kommunen bereitgestellt werden. Ein wichtiger Aspekt ist es, die Transparenz des Angebots für die Kommunen zu erhöhen und eine Verlässlichkeit der Leistungen anzubieten. Diese Leistungen müssen systematisch verknüpft werden, um die Effektivität zu steigern.

Die Verbesserung der Resilienz von Kommunen benötigt die Zusammenarbeit von Bundes-, Länder-, und Kommunalebene. Voraussetzung ist ein regelmäßiger Austausch zwischen den unterschiedlichen Akteuren. Dadurch wird Vertrauen zwischen den jeweiligen Entscheidungsträgerinnen und Entscheidungsträgern aufgebaut, um eine verbesserte Zusammenarbeit zu ermöglichen.

Inhalt

Einleitung

In den vergangenen Jahren kam es vermehrt zu Angriffen auf die IT-Systeme kommunaler Verwaltungen in Deutschland. Unter anderem durch Cyberkriminelle[1] ausgelöst, verursachten diese Informationssicherheitsvorfälle. 2021 rief der Landkreis Anhalt-Bitterfeld in Sachsen-Anhalt als Kommune zum ersten Mal den Katastrophenfall aufgrund eines Informationssicherheitsvorfalls aus.[2] Cyberkriminelle hatten die IT-Infrastruktur der Kommune kompromittiert und mittels Schadsoftware die Daten verschlüsselt. Für die Freigabe der Daten forderten die Kriminellen Lösegeld. Als sich herausstellte, dass die Kommune nicht zahlen wollte, drohten die Kriminellen mit der Veröffentlichung von Daten aus dem Netzwerk, die sie vorher kopiert hatten. Die Folgen für die Kommune waren dramatisch: Die Fachbehörden mussten eine Notlösung zur Berechnung der Sozialhilfe finden, Versorgungsleistungen der Bürgerinnen und Bürger gerieten in Gefahr.[3]

Fälle wie Anhalt-Bitterfeld[4] sind bekannt und wurden intensiv diskutiert – auch von den betroffenen Verwaltungsfachkräften. Jede der knapp 11.000[5] Kommunen in Deutschland muss mit einem vergleichbaren Informationssicherheitsvorfall rechnen. Die Digitalisierung von kommunalen Verwaltungsprozessen schreitet voran, nicht zuletzt aufgrund der Umsetzung des Onlinezugangsgesetzes.[6] Eine steigende Digitalisierung bedeutet jedoch auch, dass die Angriffsoberflächen der kommunalen IT-Infrastrukturen größer werden. Zudem streuen kriminelle Akteure ihre Aktivitäten immer breiter. Das Risiko, dass IT-Systeme von Kommunalverwaltungen kompromittiert werden, steigt daher stetig. Wie das konkrete Lagebild zur Cybersicherheit von Kommunen aussieht, ist unklar. Nach wie vor besteht keine allgemeine gesetzliche Meldepflicht für IT-Sicherheitsvorfälle. Auch werden sie bisher nicht systematisch erfasst.[7] Der Lagebericht 2022 des Bundesamtes für Sicherheit in der Informationstechnik (BSI)[8] und eine Übersicht dokumentierter, öffentlicher Vorfälle[9] verdeutlichen allerdings, dass Kommunen in den vergangenen Jahren häufig von Vorfällen betroffen waren.[10]

Wirksame Maßnahmen und Mechanismen zum Schutz von Daten und Systemen gibt es bereits. So werden *technische* Maßnahmen wie Netzwerksegmentierung oder regelmäßiges Patchen von Schwachstellen, *organisatorische* Maßnahmen wie ein Informationssicherheits-Management-System (ISMS) sowie die Analyse der Bedrohungen oder die Bereitstellung eines Warn- und Informationsdienstes implementiert. Kommunale Verwaltungen lernen, ihre Systeme technisch-organisatorisch so aufzustellen, dass zentrale Infrastrukturen und kritische Prozesse sowie Dienstleistungen auch bei einer Kompromittierung der IT-Infrastruktur aufrechterhalten werden können oder zumindest zeitnah wieder betriebsbereit sind. Weiterhin müssen sie aus bestehenden Vorfällen lernen.[11]

Es stellt sich die Frage, wie Deutschland momentan die Förderung von Informationssicherheit und der Resilienz von Kommunen gestaltet und wie wirksam der aktuelle Ansatz ist.

Grundsätzlich ist jede Kommune für die Informationssicherheit der eigenen Systeme und Prozesse selbst zuständig und trägt die Verantwortung für ihre Resilienz selbst (Kommunale Selbstverwaltung[12]).

Diese Analyse erfasst bereitgestellte Leistungen[13] der Bundes- und Landesbehörden zur Erhöhung von Informationssicherheit und Resilienz von Kommunen. Anschließend unterzieht sie einzelne Leistungen einer Wirkungsanalyse und validiert die Wirkung mithilfe von Vertretern und Vertreterinnen einzelner Behörden. Zudem leistet sie einen Beitrag zur aktuellen Diskussion der Zuständigkeiten und Instrumente zur Förderung der Informationssicherheit auf kommunaler Ebene in der Bundesrepublik Deutschland.
Im ersten Teil werden zunächst die Aufgabenverteilungen und Instrumente von Bund und Ländern zur Förderung der Informationssicherheit und Resilienz der Kommunen beschrieben. Im zweiten Teil werden auf Basis dieser Erhebung die eingesetzten Kapazitäten und Rollenverteilungen zur Förderung von Informationssicherheit und Resilienz von Kommunen analysiert. Im dritten Teil werden Vorschläge genannt, mit welchen konkreten Maßnahmen der jetzige Ansatz effektiver die Informationssicherheit und Resilienz von Kommunen fördern könnte. Dabei wird auf die aktuelle Debatte eingegangen, ob eine stärkere Regulierung, etwa durch verbindliche Vorgaben, zielführender sein könnte.

Teil 1: Beschreibung des deutschen Ansatzes – Zuständigkeiten und Instrumente

Wie transparent und nachvollziehbar sind die Leistungen von Bund und Ländern?

Während manche Länder Informationen über Unterstützungsleistungen auf zentralen Webseiten bereitstellen oder sie sogar proaktiv via E-Mail, Brief oder auf Veranstaltungen bewerben, sind Leistungen anderer Länder nicht oder nur schwer auffindbar. Hier liegen lediglich Kenntnisse aus Kleinen Anfragen oder Kontakten in Landes- oder Bundesbehörden vor. Ein Überblick über bestehende Leistungen und deren Ausgestaltung gibt im Folgenden Aufschluss darüber, welche Funktionen Bundes- und Landesbehörden aktuell bei der Cybersicherheit von Kommunen umsetzen. Diese Informationen bilden die Grundlage für eine Analyse der Wirkung dieser Maßnahmen.

Welche Leistung kann eine Kommune nutzen?

Die bestehenden Leistungen der Bundes- und Landesbehörden lassen sich in zwölf Kategorien zur Förderung der Informationssicherheit und Resilienz bündeln (siehe Grafik auf Seite 7).

Nicht alle Leistungskategorien sind für alle Kommunen gleichermaßen verfügbar. Die Verfügbarkeit einer Leistung für die Kommune variiert von Bundesland zu Bundesland, da die Länder bisher ihre Funktion für die kommunale Cybersicherheit unterschiedlich definieren und somit verschiedene Portfolios an Leistungskategorien anbieten.

Leistungen, die *allen* Kommunen zur Verfügung stehen, sind:
1. Vorfallsbearbeitung (nicht in allen Funktionen), (siehe Grafik Seite 10),
2. Bewertung/Evaluation,
3. Warn- und Informationsdienst,
4. Orientierungshilfen,
5. Veranstaltungen,
6. Zertifizierung,
7. regelmäßiger Austausch,
8. Beratung (IT-Sicherheit und Resilienz),
9. und Schulungen (Kompetenzen).

Leistungen, die *wenigen* Kommunen zur Verfügung stehen, sind:
10. Tools zur Gefahrendetektion,
11. finanzielle Förderung,
12. und Übungen/Spiele.

Nur für hessische Kommunen gibt es in jeder Kategorie mindestens eine Leistung, auf die sie zugreifen können.

Kommunale Cybersicherheitspolitik

Leistungen des Bundes und der Länder für Kommunen

Autorin: Julia Schuetze
Design: Ha Thanh Thu Nguyen

Institutionen des Bundes und der Länder stellen verschiedene Leistungen bereit, die Mitarbeiterinnen und Mitarbeiter von Kommunen dabei unterstützen sollen, die Informationssicherheit und Resilienz Ihrer Kommune zu stärken.

Vorfallsbearbeitung

Unter der Kategorie *Vorfallsbearbeitung* finden Kommunen Leistungen, die Ihnen helfen können, wenn Sie mit IT-Sicherheitsvorfällen zu tun haben. Unterstützung gibt es in unterschiedlichen Formen. So bieten der Bund und einige Länder Beratung vor Ort oder per Telefon an. Einige Länder stellen Handreichungen und Checklisten zur Verfügung. Auch gibt es konkrete technische und operative Unterstützung, etwa durch forensische Analysen.

Bewertung/Evaluation

Unter *Bewertung/Evaluation* finden Kommunen Leistungen, die dabei helfen, den Status Quo der Informationssicherheit oder Resilienz Fähigkeiten der Kommune einzuschätzen. Das können Audits sein, auch zur offiziellen Zertifizierung, oder technische Tests, die Netzwerke und Systeme auf Schwachstellen überprüfen. Mit Formaten wie Umfragen oder Checklisten lässt sich die Umsetzung von Maßnahmen zur Cybersicherheit und Resilienz überprüfen. Einige Länder stellen finanzielle Förderungen dafür bereit.

Warn- und Informationsdienst

In der Kategorie *Warn- und Informationsdienst* finden Kommunen Leistungen, die dabei helfen, konkrete Bedrohungen oder Schwachstellen zu erkennen. Mitarbeiterinnen und Mitarbeiter von Kommunen erhalten Warnungen und Informationen, etwa per Online-Tool oder Email. Eine Anmeldung kann hier vonnöten sein, um die Informationen zu bekommen, die auf die Kommune zugeschnitten sind oder zu denen die Mitarbeiterinnen und Mitarbeiter berechtigt sind. Die Informationen dieser Leistungskategorie lassen sich gut in ein Information Security Management System (kurz: ISMS) integrieren.

Beratung (Resilienz/IT-Sicherheit)

Unter *Beratung (Resilienz/IT-Sicherheit)* finden Kommunen Leistungen, die dabei helfen, Maßnahmen zur Informationssicherheit und Resilienz zu identifizieren und umzusetzen. Im Vergleich zu Orientierungshilfen bieten diese Leistungen einen persönlichen Kontakt via Email, Telefon oder in persona. So können Personen mit spezifischem Fachwissen die individuelle Situation einschätzen und mit Mitarbeiterinnen und Mitarbeiter gemeinsam konkrete Lösungen finden.

Orientierungshilfen

In der Kategorie *Orientierungshilfen* finden Kommunen Leistungen, die helfen, Maßnahmen zur Informationssicherheit und Resilienz zu erkennen, zu verstehen und umzusetzen. Diese Hilfen gibt es etwa in Form von Factsheets, Leitfäden oder Excel- und Word-Dateien.

Schulungen (Kompetenzen)

Unter *Schulungen (Kompetenzen)* finden Kommunen Leistungen, die dabei helfen, Kompetenzen auf- und auszubauen. Sie richten sich an verschiedene Zielgruppen und behandeln ein breites Themenspektrum in unterschiedlichen Formaten. Einige Länder stellen Trainings für Führungskräfte bereit oder bieten Awareness-Schulungen, Trainings zur Erkennung von Phishing Mails oder Hilfe bei der Umsetzung von Standards. Je nach Leistung erhalten Mitarbeiterinnen und Mitarbeiter Workshops und Kurse in persona oder virtuell, auch Trainings-Software wird angeboten.

Veranstaltungen

In der Kategorie *Veranstaltungen* sind solche aufgelistet, die Bund und Länder spezifisch für Kommunen zum Thema Informationssicherheit durchführen.

Tools zur Gefahrendetektion

In der Kategorie *Tools zur Gefahrendetektion* finden Kommunen Leistungen, die dabei helfen, mittels Software konkrete technische Gefahren selbst zu erkennen. Es handelt sich um Detection Tools, die bereitgestellt oder finanziert werden, z.B. Honey Pot, oder DDoS Check für Websites.

Zertifizierung

Unter *Zertifizierung* finden Kommunen Leistungen, die dabei helfen, anzuzeigen, welchen Stand der IT-Sicherheit die Kommune umgesetzt hat. Ein Zertifikat ist eine Bestätigung durch Selbstauskunft oder Dritte, dass Anforderungen, zum Beispiel von internationalen Normen, branchenspezifischen Standards oder technischen Regeln erfüllt werden.

Übungen/Spiele

In der Kategorie *Übungen/Spiele* finden Kommunen Leistungen, die dabei helfen, Kompetenzen zu testen und zu evaluieren. Übungen werden in gängigen IT-Sicherheitsstandards empfohlen.

regelmäßiger Austausch

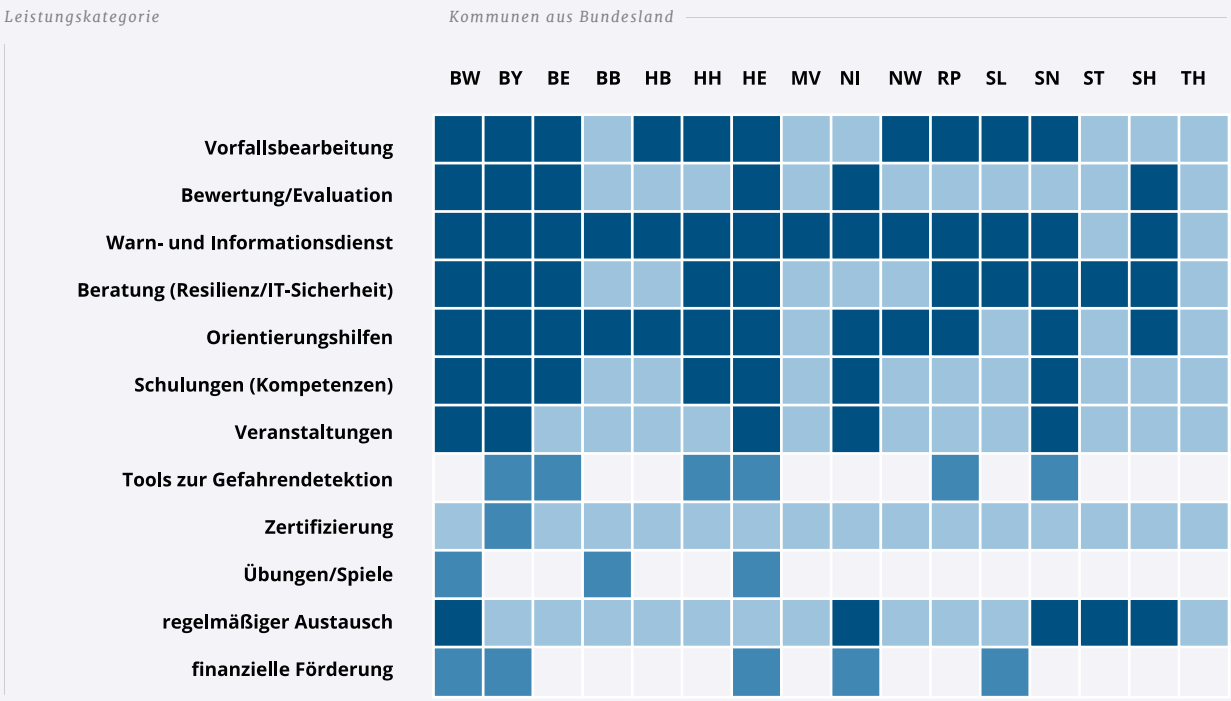
Unter *regelmäßiger Austausch* finden Kommunen Leistungen, die dabei helfen, in Kontakt mit anderen Kommunen zu kommen, die an denselben Aufgaben sitzen wie Sie. In Abgrenzung zu den Veranstaltungen handelt es sich hierbei um vertrauliche Kreise zum kontinuierlichen Austausch. Formate können sein: Stammtische, Sprechstunden, Social-Media-Gruppen, Community-Treffen usw.

finanzielle Förderung

In der Kategorie *finanzielle Förderung* finden Kommunen Budget, das Ihnen dabei hilft, Cybersicherheit und Resilienz umzusetzen. Es handelt sich um Förderungen zur Finanzierung von Software oder Hardware oder zur Finanzierung von Personalkosten und Schulungskosten.

Wann können alle Kommunen die Leistung nutzen?

Einige Leistungen werden bereits nach dem „Einer für Alle“-Prinzip (EfA-Prinzip) bereitgestellt. Das bedeutet, dass einige Länder ihre Leistungen für Kommunen bereitstellen, die in anderen Ländern liegen. Einige Länder tun dies allerdings nur auf Nachfrage und kommunizieren dies nicht proaktiv. Zudem werden ausgewählte Leistungen, die allen Kommunen, manchmal unter bestimmten Umständen, zur Verfügung stehen, auch vom Bund bereitgestellt. Teilweise kann es bei den angebotenen Leistungen innerhalb einer Kategorie zu Dopplungen, Überschneidungen oder Ergänzungen kommen. Kommunen haben beispielsweise Zugang zu verschiedenen Warn- und Informationsdiensten. In der Kategorie Orientierungshilfe ergänzen sich die Leistungen gegenseitig und erhöhen die Diversität der behandelten Aspekte (etwa Informationssicherheit für Schulen, Krisenkommunikationstipps oder Informationssicherheit bei Digitalisierungsprojekten).



Verfügbarkeit der Leistungen zur Förderung der Informationssicherheit von Kommunen

Welche Leistungen können Kommunen nutzen?
Wer stellt die Leistungen bereit?

Leistung:

- *nicht beziehbar*
- *beziehbar von Organisationen anderer Länder oder des Bundes*
- *beziehbar von Organisationen des eigenen Landes*
- *beziehbar von Organisationen des eigenen Landes & von anderen Ländern oder des Bundes*

Kommunen aus:

BW	*Baden-Württemberg*
BY	*Bayern*
BE	*Berlin*
BB	*Brandenburg*
HB	*Bremen*
HH	*Hamburg*
HE	*Hessen*
MV	*Mecklenburg-Vorpommern*
NI	*Niedersachsen*
NW	*Nordrhein-Westfalen*
RP	*Rheinland-Pfalz*
SL	*Saarland*
SN	*Sachsen*
ST	*Sachsen-Anhalt*
SH	*Schleswig-Holstein*
TH	*Thüringen*

Disclaimer: Die Leistungen der Länder für Kommunen entwickeln sich ständig weiter. Die dargestellten Leistungen beziehen sich auf öffentlich verfügbare Informationen. Geplante Leistungen wurden in der Darstellung nicht berücksichtigt. Zur Validierung der Recherche wurden Vertreterinnen und Vertreter der Behörden kontaktiert. (Stand: August 2023)

Welche Unterschiede haben die Leistungen?
Es gibt Unterschiede (etwa in Umfang oder Format), wie die Leistungen innerhalb einer Kategorie bereitgestellt werden. Die Unterschiede werden an folgenden Beispielen deutlich:

Beispiel: Kategorie Vorfallsbearbeitung
- die Abdeckung der Erreichbarkeit *(24/7 versus Bürozeiten)*
- die Funktion, die übernommen wird *(Vermittlung an Expertinnen und Experten versus operative Unterstützung)*
- die Art und Weise der Zusammenarbeit *(Telefonische Unterstützung versus Vorortunterstützung)*
- die Verfügbarkeit der Funktion oder Leistung *(Unterstützung bei herausgehobenen Fällen und nach Verfügbarkeit von Ressourcen versus in jedem Fall)*

Beispiel: Bewertung und Evaluation
- die Methode *(Pentest, Selbstauskunft, Audit, Übung und so weiter)*
- die *Vorortinterviews versus Onlineumfrage*

Welche konkreten Funktionen übernehmen Bund und Länder?
Die Länder nehmen ihre Funktion und Rolle für die Informationssicherheit und die Resilienz von Kommunen uneinheitlich wahr. Aus den bereitgestellten Leistungen lassen sich die unterschiedlichen Funktionen, die Länder bei der Informationssicherheit und Resilienz von Kommunen einnehmen, ableiten. So deutet etwa die Bereitstellung von Orientierungshilfen darauf hin, dass Bund oder Länder eine *informierende* Funktion einnehmen, während die Bereitstellung von Schulungen eine *bildende* Funktion hat. Finanzielle Förderung deutet auf eine *finanzierende* Funktion hin, während die Bereitstellung von Tools zur Gefahrendetektion sowohl eine *operative* als auch *administrative* Funktion hat, da die Bereitstellung von Tools durch Rahmenverträge erfolgt (*administrative* Ressourcen werden bereitgestellt) oder die Tools direkt gemanagt werden (*operative* Funktion). Eine explizit *finanzierende* Funktion nehmen bisher nur Bayern, Hessen und das Saarland ein. Aus den derzeit bereitgestellten Leistungen lässt sich ableiten, dass unterschiedliche Bundesländer unterschiedliche Funktionen einnehmen – es ist kein einheitliches Bild zu erkennen. Neben der Kategorie ist deswegen auch die Leistungsbeschreibung/inhaltliche Ausgestaltung der Leistung ausschlaggebend. Diese Divergenz wurde einmal beispielhaft für die Kategorie *Vorfallsbearbeitung* aufgeschlüsselt (siehe Grafik auf Seite 10): Länder wie Bayern, Baden-Württemberg, Hessen, Saarland und Rheinland-Pfalz schreiben sich mehrere Funktionen zu, während andere ihre Funktion/Aufgabe – öffentlichen Quellen zufolge – noch nicht klar formuliert und kommuniziert haben.

Unterschiedliche Funktionen der Länder aufgezeigt am Beispiel der Kategorie *Vorfallsbearbeitung*

Bund
- Vermittelnd
- Beratend (nur in bestimmten Fällen)
- Operativ und technisch (nur in bestimmten Fällen)

Brandenburg
Öffentliche Quellen weisen auf keine Funktion hin

Mecklenburg-Vorpommern
Öffentliche Quellen weisen auf keine Funktion hin

Saarland
- Beratend
- Operativ und technisch
- Koordinierend

Baden-Württemberg
- Beratend
- Operativ und technisch

Bremen
- Beratend
- Operativ und technisch
- Koordinierend

Niedersachsen
Öffentliche Quellen weisen auf keine Funktion hin

Sachsen
- Beratend

Thüringen
Öffentliche Quellen weisen auf keine Funktion hin

Bayern
- Beratend
- Operativ und technisch

Hamburg
- Beratend
- Operativ und technisch
- Koordinierend

Nordrhein-Westfalen
- Beratend (Funktion wird als "Beihilfen" beschrieben)

Sachsen-Anhalt
Öffentl. Quellen weisen auf keine Funktion hin, allerdings nahm das Land eine finanziell fördernde Funktion im Fall Anhalt-Bitterfeld ein

Berlin
- Operativ und technisch

Hessen
- Vermittelnd
- Beratend
- Operativ und technisch

Rheinland-Pfalz
- Beratend
- Operative und technische
- Koordinierend

Schleswig-Holstein
Öffentliche Quellen weisen auf keine Funktion hin

Disclaimer: Die Leistungen der Länder für Kommunen entwickeln sich ständig weiter. Die dargestellten Leistungen beziehen sich auf öffentlich verfügbare Informationen. Geplante Leistungen wurden in der Darstellung nicht berücksichtigt. Zur Validierung der Recherche wurden Vertreter:innen der Behörden kontaktiert. (Stand: August 2023)

Autorin: Julia Schuetze
Design: Ha Thanh Thu Nguyen

Teil 2: Analyse des deutschen Ansatzes – *Nudging* statt Regulierung

Kommunen sind im Rahmen der kommunalen Selbstverwaltung für die Implementierung von Informationssicherheit und den Aufbau von Resilienzfähigkeiten verantwortlich. Die Unterstützungsleistungen des jeweiligen Bundeslandes oder des Bundes selbst sind hierbei uneinheitlich und zudem abhängig vom jeweiligen Einzelfall. Bund und Länder unterstützen Kommunen bisher nur teilweise bei der Aufgabenwahrnehmung. Bisweilen stellen Bund und Länder Leistungen zur Förderung bereit und nehmen eher eine unterstützende Rolle ein. Zudem existieren nur in einigen Ländern auf Kommunen ausgerichtete Regulierungen, die die Informationssicherheit betreffen.[14] Bund und Länder schaffen grundlegend Anreize und verfolgen einen *Nudging*-Ansatz.[15]

Nudges sind verhaltenspolitische Instrumente, die darauf abzielen, individuelles Verhalten ohne Zwang zu ändern. Die Leistungen, die Bund und Länder den Kommunen anbieten, sollen Anreize schaffen, das Verhalten von kommunalen Akteuren zu verändern. Gesetze bestimmen ebenfalls menschliches Verhalten, jedoch beinhalten Gesetze oftmals eine Pflicht zur Umsetzung. Anders als bei Regulierungen muss beim *Nudging* nichts umgesetzt werden, vielmehr kann die handelnde Person das empfohlene Verhalten umsetzen. Pflicht und Anreize haben unterschiedliche Rechtsfolgen. Anreize sind nur wirksam, wenn sie wirklich das Verhalten verändern.

Teil 3: Weiterentwicklung des deutschen Ansatzes – Vorschläge und Anregungen

Der aktuelle Ansatz – eher (unterschwellig) zu *nudgen* als (klar) zu regulieren – weist eine hohe Komplexität auf und wird sehr uneinheitlich von den Ländern umgesetzt. Es stellt sich also die Frage: Wie kann der *Nudging*-Ansatz weiterentwickelt und wirksam gestaltet werden?

Beispielsweise könnte ein deutschlandweites Programm zur Förderung Anreize setzen, bestimmte Funktionen des Bundes und der Länder für alle Kommunen vergleichbar auszubauen. Da einige Leistungen auf regionale Unterschiede und Bedarfe eingehen müssen, ist eine gewisse Flexibilität in der Umsetzung sehr sinnvoll. So könnten Länder, in denen mehrheitlich IT-Dienstleister die IT der Kommunen betreiben, diese eng in die Leistungserbringung einbinden. Wohingegen in anderen Ländern, in denen Kommunen die IT-Sicherheit eigenständig verwalten, die Kommunen direkt vom Land unterstützt werden könnten. Da die Länder ihre Leistungen und Funktionen unterschiedlich definiert und ausgebaut haben, bedarf es momentan noch eines großen Engagements und Einsatzes der Kommunen selbst, um auszuhandeln, welche Leistungen und Funktionen besonders hilfreich und notwendig sind.

Die folgenden Vorschläge zeigen beispielhaft, wie der Einsatz von Nudges wirksam ausgebaut werden könnte und welche weiteren Maßnahmen diskutiert werden sollten.

Orientierung schaffen

Da es beim jetzigen Ansatz sehr wichtig ist, dass sich die Mitarbeiterinnen und Mitarbeiter in den Kommunen während der Entscheidungsfindung schnell orientieren können, bedarf es einer geordneten Übersicht der verschiedenen Maßnahmen und unterstützenden Leistungen. Das ist vor allem eine kommunikative Herausforderung, da die Mitarbeiterinnen und Mitarbeiter unterschiedliche Ausgangssituationen, Kompetenzen und Fragen haben.

Als ersten Schritt sollten Bund und Länder die verfügbaren Leistungen für die verschiedenen Zielgruppen in den Kommunen ordnen, erklären und niedrigschwellig verfügbar bereitstellen. Der „Cybersicherheits-Kompass“[16] (von der Stiftung Neue Verantwortung und dem Deutschen Städtetag) bietet hier eine Orientierung, bedarf allerdings noch der Weiterentwicklung. Die Leistungskategorien *Beratung (IT-Sicherheit/Resilienz), regelmäßiger Austausch und Veranstaltungen* sollten ebenso proaktiv genutzt werden, um die Zielgruppen persönlich zu erreichen und sie auf verschiedene Unterstützungsmöglichkeiten aufmerksam zu machen. Durch die regionalen Unterschiede bietet es sich zudem an, solche Leistungen auch regional anzubieten – wie es auch schon einige Länder umsetzen.

Nudges und positive Anreize verknüpfen

Nudges in Form von Leistungen werden momentan vor allem dazu genutzt, Personen zu ermutigen, etwas auf eine bestimmte Art zu tun oder zu implementieren. Beispielsweise einen Krisenkommunikationsplan nach dem Vorbild einer Orientierungshilfe zu entwickeln. Solche Nudges sollten auch mit positiven Anreizen verbunden werden. Leistungen wie finanzielle Förderung, Schulungen, Bereitstellung von Tools und so weiter können eingesetzt werden, um die Umsetzung von Zielvorgaben zu fördern. Dies wird auch jetzt schon in Teilen praktiziert, beispielsweise bekommen Kommunen, die einen Vorfall melden, in einigen Ländern passende Unterstützung oder Tools bereitgestellt, die sie nicht bekämen, wenn sie sich nicht meldeten, etwa in Bayern. Dieser Ansatz sollte für jede Zielsetzung durchdacht werden, um die Zielvorgaben, Leistungen und positive Anreize zu verknüpfen. Leistungen aus der Leistungskategorie Bewertung und Evaluation sowie Übungen/Spiele können außerdem gemeinsam mit positiven Anreizen genutzt werden, um das Erreichen der Zielvorgaben zu bestätigen (Zertifizierung oder Auszeichnung). Die positiven Anreize können auf die Kommune als Institution abzielen, beispielsweise eine Zertifizierung für einen erreichten Standard (wie bereits üblich), eine Auszeichnung für ihr Engagement in der Informationssicherheit oder eine Anerkennung für ihre Resilienzfähigkeiten bei einem Vorfall oder für gute gemeinsame Zusammenarbeit. Hierbei sollte allerdings die Sorge vor einem negativen Ergebnis genommen werden. Es sollte sich um eine Art gemeinsame Beobachtung handeln. Der Fokus sollte auf die Förderung von Kapazitäten und Kompetenzen gelegt werden, mit dem Ziel, kontinuierlich Resilienzfähigkeiten[17] zu überprüfen und weiterzuentwickeln. Positive Anreize sollten nicht nur auf die Kommune als Organisation, sondern auch auf Mitarbeiterinnen und Mitarbeiter in den Kommunen abzielen, denn am Ende sind es ihre individuellen Kompetenzen oder Kompetenzen als Team, die für Informationssicherheit und Resilienz sorgen. Bewertungen und Evaluationen sollten demnach nicht auf dem Papier stattfinden, wie es bei Standards oft der Fall ist, sondern auch die Resilienzfähigkeiten praktisch testen, zum Beispiel via Pentests und Übungen.[18] Individuelle und Teamleistungen sollten ausgezeichnet und belohnt werden.

Leistungen nach Bedarf (weiter-)entwickeln

Wenn Leistungen entwickelt werden, ist es besonders wichtig, die Zielgruppe eng einzubinden. Das wird bereits teilweise praktiziert. So werden aktuell Orientierungshilfen entwickelt, die sich besonders auf kleine bis mittlere Kommunen konzentrieren.[19] Andere Zielgruppen, beispielsweise aus Städten, brauchen jedoch gegebenenfalls andere Leistungen, wie die Bedarfsanalyse *Informationssicherheit von deutschen Städten verbessern* zeigt.[20] In jedem Fall liefert die Zusammenarbeit mit den Nutzerinnen und Nutzern der Leistungen und Funktionen konkrete Vorschläge, welche Leistungen das Verhalten fördern würden oder welche Funktionen von Bund oder Ländern übernommen werden könnten. Inwiefern diese bereitgestellt werden, ist wiederum politische Aushandlung. Nicht zielführend wäre der Zustand, wenn eine Leistung aus politischen Gründen bereitgestellt wird, die für die Zielgruppe nicht nützlich ist.

Better Practices identifizieren am Beispiel des Warn- und Informationsdienstes

Durch die aktuellen Unterschiede in den angebotenen Leistungen (siehe Darstellung Seite 8) kann eine Evaluation dazu führen, dass gezielt Leistungen ausgebaut werden, die besser unterstützen als andere. Dabei ist es wichtig, zu untersuchen, welche Better Practices für die Leistung selbst existieren (zum Beispiel das Format, in dem die Leistung angeboten wird) und welche Better Practices auch in der Organisation der Leistung liegen, beispielsweise ob die Leistung bundesweit für alle verfügbar ist.

Es gibt verschiedene Warn- und Informationsdienste[21], die Kommunen nutzen können.

- Der Bedarf in diesem Fall ist nicht die Verfügbarkeit der Informationen, sondern die Menge an Informationen, die kommuniziert wird und wie relevant die Einschätzung der Informationen für die Kommune ist.
- Warn- und Informationsdienste sind somit besonders nützlich, wenn Kommunen Anpassungen und Filterungen vornehmen können, welche Informationen sie erhalten möchten. Die Möglichkeit, die eigene Software- und IT-Landschaft zu erfassen in Form von Profilen, um Meldungen besser filtern und einschätzen zu können, wurde als positiv bewertet.
- Eine Verknüpfung mit IT-Tickets,[22] die bestmöglich auch direkt an IT-Dienstleister weitergeleitet werden können, wurde als positiv bewertet.
- Die Möglichkeit, nicht nur nach Produkten/Komponenten, sondern nach Kritikalität[23] zu filtern, wurde als positiv bewertet.
- Die Möglichkeit, eine Kontaktperson zu benennen und festzulegen, wurde als positives Feature bewertet.
- Eine Bündelung der Informationen in einem Dienst könnte außerdem die Anzahl der Informationskanäle reduzieren, die zumeist Einzelpersonen in Kommunen tracken müssten. Auch sollten sich Ländereinschätzungen nicht mit Bundeseinschätzungen widersprechen oder zumindest beide Perspektiven gebündelt betrachtet werden.
- Vorschläge zu Maßnahmen, die mit den Informationen verbunden werden und Handlungsspielräume aufzeigen, würden Panik und Überforderung vermeiden. Gerade für Personen, die eine andere Person innerhalb der Verwaltung überzeugen müssen, eine Entscheidung zu treffen, sind klare Einschätzungen und Empfehlungen, die von einer höheren und zentralen Stelle kommen, erforderlich.
- Die Kapazitäten zur Informationsanalyse hängen mit den Kompetenzen der eigenen IT zusammen und dies wiederum beeinflusst den Grad der Selbstständigkeit von IT-Dienstleistern. Eine Förderung dieser Kompetenzen würde helfen, dass Informationen besser verarbeitet und rasche Lösungen gefunden werden können.

Unterstützende Funktion bei einem Vorfall festlegen

Es gibt große Unterschiede in den Funktionen, die Länder für die Informationssicherheit und Resilienz von Kommunen übernehmen: von Dopplungen, Überschneidungen bis zu Ergänzungen zwischen den Funktionen des Bundes und der Länder. Bundesweit gibt es keine Einigung darüber, welche Funktionen Bund und Länder übernehmen sollen. Besonders anschaulich wird dies bei der operativen und technischen Funktion der Vorfallsbearbeitung. In einigen Ländern konnte keine Funktion identifiziert werden und der Bund nimmt nur in bestimmten Fällen diese Funktion ein. Insoweit bleibt in einigen Bereichen eine Unterstützung der Kommunen aus.
In Ländern, wo es diese Funktion gibt, sollte der Umfang der Unterstützung (bereits vor einem Vorfall) deutlich kommuniziert werden, sodass es nicht zu einem falschen Erwartungsmanagement kommt. Bund und Länder, die diese Funktion bereitstellen, sollten vorab informieren, in welchem Umfang sie die Funktion übernehmen können – welche Stelle zu welchem Thema angesprochen werden und Hilfe leisten kann.
Die unterschiedlichen Ausprägungen der Aufgaben und Unterstützungsleistungen zwischen den Ländern haben gravierende Auswirkungen auf die Bildungs- und Cybersicherheitspolitik. Welche Aufgaben und Rollen müssen ausgebildet werden? In welchen Fällen sollen andere Akteure der Cybersicherheitsarchitektur bestimmte Funktionen übernehmen, die die Länder nicht einnehmen?
Demnach sollte auch operative und technische Unterstützung bei einem Vorfall für alle Kommunen verfügbar gemacht werden. Dies kann auf unterschiedliche Art und Weise geschehen und ist eine Aufgabe politischer Aushandlung. Eine Festlegung der Zuständigkeit ist allerdings dringend geboten.

Funktionierende Leistungen gemeinsam entwickeln

Konkrete Zielvorgaben, zum Beispiel in Form von kurzen Leitfäden vom Bundesamt für Sicherheit in der Informationstechnik, die zielgruppenspezifisch sind, wurden von Mitarbeiterinnen und Mitarbeitern in Städten als positiv bewertet.[24] Zielvorgaben können also weiterhin in solchen Formaten vermittelt werden. Da Kommunen sehr heterogen aufgestellt sind, sollten Zielvorgaben auch in Zukunft diese Heterogenität und durch die Veränderung der Bedrohungslage auch eine gewisse Flexibilität berücksichtigen. Beispielsweise gibt es noch nicht für jeden Standard Umsetzungspraktiken, die erprobt und empfehlenswert sind. Diese müssen gegebenenfalls zuerst mit Mitarbeiterinnen und Mitarbeitern entwickelt werden. So haben Krisenmanagerinnen und -manager bereits Vorwissen im Business Continuity Management, diesen Standard aber noch nicht für IT-Sicherheitsvorfälle erprobt. Zur Entwicklung dieser Better Practices können Leistungen wie ein *regelmäßiger Austausch* und *Übungen* genutzt werden, bevor sie in Leitfäden oder Schulungen münden.[25] Diese Vorgaben sollten sich nicht nur auf die Informationssicherheitsbeauftragten beziehen, sondern andere wichtige Zielgruppen innerhalb der Verwaltung adressieren, zum Beispiel Krisenmanagerinnen und -manager, Kommunikationsleitung, Fachbereichsleitung und so weiter.

Bestehende Leistungen teilen

Schon jetzt stellen manche Länder Leistungen für Kommunen nach dem „Einer für alle“-Prinzip (EfA-Prinzip) bereit. Dies führt dazu, dass eine Leistung, die beispielsweise in einem Land entwickelt wurde, auch nutzbar für Kommunen ist, die nicht in diesem Land liegen. Bei der Weiterentwicklung könnte dieses Prinzip gezielt angewandt werden, indem sich Akteure, die bestimmte Leistungen entwickeln wollen, gezielt zusammentun und diese dann allen bereitstellen. So können Dopplungen vermieden werden und sich Akteure finden, die sich auf bestimmte Leistungen oder Themen spezialisieren. Dabei sollte das BSI eingebunden werden, um eine Konformität mit BSI-Standards oder die Anpassung nach einem Stufenmodell für verschiedene Zielgruppen sicherzustellen.[26]

Zur Diskussion – Weitere Maßnahmen

Im weiteren politischen Diskurs gibt es außerdem die Möglichkeit, nicht nur die bestehenden Leistungen zu systematisieren und Funktionen zu etablieren, sondern auch zu diskutieren, inwiefern Bund, Länder und Kommunen gemeinsam weitere technische, organisatorische und politische Maßnahmen zur Sicherstellung der Informationssicherheit und Resilienz implementieren. Für die Implementierung solcher Maßnahmen gibt es großen Bedarf.[27]

Hier finden sich Anregungen, welche Maßnahmen implementiert werden könnten:

- Entwicklung der zentralen Zielvorgaben mit Expertinnen und Experten aus allen Ebenen (Bund, Länder, Kommunen) mit interdisziplinärer Begleitung aus den verschiedenen Sektoren von Wissenschaft, Wirtschaft und Zivilgesellschaft. Durch die Heterogenität muss darauf eine regionale Prüfung der Auswirkungen folgen, die Grundlage für den Ausbau von Leistungen und Maßnahmen sein sollte. Diese Prüfung sollte beispielsweise fragen:
  - Was sind die Auswirkungen für verschiedene Kommunen und deren IT-Organisation, etwa Kommunen im Eigenbetrieb, Kommunen mit (mehreren) externen Dienstleistern, Großstädte mit verschiedenen Ämtern, die teilweise eigene IT betreiben und so weiter.
  - Was heißt das für Mitarbeiterinnen und Mitarbeiter und deren Arbeitsgebiet? Welche Kompetenzen sollten sie (weiter) aufbauen und wie?
  - Was bedeutet es für Unternehmen, die mit Kommunen arbeiten? Welche Verantwortung tragen sie?
- Sicherer Austausch von Informationen über Informationssicherheit und Resilienz, der es Kommunen ermöglicht, sich deutschlandweit untereinander schnell auszutauschen. Dies betrifft Informationen über Vorfälle, Angriffswege, aber auch Präventionsmaßnahmen zur Informationssicherheit und Resilienz.
- Zentrale Überprüfung sowohl von Digitalisierungsprojekten als auch von Hard- und Software, die Kommunen nutzen. Gerade bei bundesweit genutzter Soft- und Hardware bietet sich nicht nur eine zentrale Entwicklung an, sondern auch eine zentrale Überprüfung, sodass nicht jede Kommune die IT-Sicherheit immer wieder neu in Ausschreibungen prüfen muss.
- Entwicklung von Lösungen, die den Fachkräftemangel bei Kommunen kurz-, mittel- und langfristig adressiert, in Zusammenarbeit mit Wirtschaft, Zivilgesellschaft und Wissenschaft.
- Testen verschiedener Methoden der Bewertung und Evaluierung von Informationssicherheit und Resilienz: Wie kann die Resilienz von Kommunen effektiv und kontinuierlich überprüft und nachhaltig verbessert werden? Wie kann der Stand der Informationssicherheit erhoben werden?
- Die Bereitstellung von IT-Infrastruktur und/oder von IT-Sicherheitstools als Leistung beispielsweise durch Rahmenverträge.
- Den Aufbau von regionalen Security Operations Centers fördern.

Endnoten

1 BSI (2021), BSI-Lagebericht 2021: Bedrohungslage angespannt bis kritisch. https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2021/211021_Lagebericht.html (zuletzt abgerufen: 18.08.2023).

2 Im Landkreis Anhalt-Bitterfeld war zeitweise die Versorgung der Bürgerinnen und Bürger in Gefahr. Zum Beispiel war es nicht möglich, Sozialhilfe zu berechnen oder Autos zuzulassen. Zudem rief der Landkreis den Katastrophenfall aus, um Leistungen weiterhin garantieren zu können und sich gleichzeitig rechtlich abzusichern. Siehe hierzu Griebsch & Atug (2021), Rebuilding Landkreis Anhalt-Bitterfeld. https://media.ccc.de/v/rc3-2021-chaoszone-295-rebuilding-landkr#t=131 (zuletzt abgerufen: 18.08.2023).

3 MDR Sachsen-Anhalt (2022), Katastrophenfall nach Cyberangriff aufgehoben. https://www.mdr.de/nachrichten/sachsen-anhalt/dessau/bitterfeld/cyberangriff-katastrophenfall-anhalt-bitterfeld-aufgehoben-100.html (zuletzt abgerufen: 18.08.2023).

4 Griebsch & Herpig (2021), Transkript zum Hintergrundgespräch: „Cyberkriminelle erpressen Anhalt-Bitterfeld – Was können wir daraus lernen?“. https://www.stiftung-nv.de/de/publikation/transkript-zum-hintergrundgespraech-cyberkriminelle-erpressen-anhalt-bitterfeld-was (zuletzt abgerufen: 18.08.2023).

5 Schubert (2022), Gemeindeverzeichnis. https://www.gemeindeverzeichnis.de/dtland/dtland.htm (zuletzt abgerufen: 18.08.2023).

6 BSI (2023), IT-Sicherheitsverordnung Portalverbund (ITSiV-PV). https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Moderner-Staat/Online-Zugangsgesetz/IT-Sicherheitsverordnung_PVV/IT-Sicherheitsverordnung_ITSiV-PVV.html (zuletzt abgerufen: 18.08.2023).

7 Schuetze (2023), Stellungnahme von Julia Schuetze für die öffentliche Anhörung des Ausschusses für Digitales zum Thema „Cybersicherheit – Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland“. https://www.bundestag.de/resource/blob/929986/a83f11806d0c6b47cead2437e2b35b4f/Stellungnahme-Schuetze-data.pdf (zuletzt abgerufen: 18.08.2023).

8 „Kommunen sind Kreise, Städte, Gemeinden und Stadtbezirke.“ Bundeszentrale für politische Bildung/bpb (Hrsg.): einfach POLITIK: Lexikon. D. Meyer, T.Schüller-Ruhl, R. Vock u.a./Redaktion (verantw.): Wolfram Hilpert (bpb). Bonn: 2022. Lizenz: CC BY-SA 4.0 //. https://www.bpb.de/kurz-knapp/lexika/lexikon-in-einfacher-sprache/290474/kommunen/ (zuletzt abgerufen: 18.08.2023).

9 Öffentlich dokumentierte Fälle finden sich auf der Webseite Kommunaler Notbetrieb von Jens Lange. Lange (2023), Kommunaler Notbetrieb. https://kommunaler-notbetrieb.de/ (zuletzt abgerufen: 18.08.2023).

10 „Dabei war die Bedrohungslage auch vor dem Kriegsbeginn auf einem unverändert sehr hohen Niveau. Beispielsweise Ransomware-Angriffe bei IT-Dienstleistern, in Landkreisen und Kommunen sowie bei großen Unternehmen, Überlast-Angriffe (DDoS) auf Onlineshops an verkaufsstarken Tagen – all diese IT-Sicherheitsvorfälle machen deutlich, wie wichtig Informationssicherheit für unsere sichere Digitalisierung ist.“ BSI (2022), Die Lage der IT-Sicherheit in Deutschland 2022. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.html?nn=129410 (FG) (zuletzt abgerufen: 18.08.2023).

11 Resilienzfähigkeiten wurden abgeleitet von BSI-Standard 200-4, the BCI, ENISA, NIST-SP 800-172, MITRE Working Group. Vgl. außerdem Herpig (2023), Mehr Resilienz für Deutschlands IT-Systeme. https://background.tagesspiegel.de/cybersecurity/mehr-resilienz-fuer-deutschlands-it-systeme (zuletzt abgerufen: 18.08.2023). Vgl. auch Tiirmaa-Klaar & Skierka (2022), Germany’s National Security Strategy: A Chance to Pivot to Adaptive Cyber Resilience. https://fourninesecurity.de/2023/01/17/germanys-national-security-strategy-a-chance-to-pivot-to-adaptive-cyber-resilience (zuletzt abgerufen: 18.08.2023).

12 Die Selbstverwaltungsgarantie ergibt sich aus Artikel 28 Absatz 2 Satz 1 des Grundgesetzes und beschreibt die Eigenverantwortlichkeit der kommunalen Ebene für ihre Verwaltungsaufgaben.

13 Die Leistungen der Länder für Kommunen entwickeln sich ständig weiter. Geplante Leistungen, die zumeist in Strategiepapieren oder politischen Statements erwähnt werden, wurden in der Analyse nicht berücksichtigt. Die in diesem Papier dargestellten Leistungen beziehen sich auf öffentlich verfügbare Informationen. Eine aktuelle Leistungsübersicht wurde auf Basis dieser Recherche hier veröffentlicht: Stiftung Neue Verantwortung (2023), Cybersicherheits-Kompass für Kommunen. https://cybersicherheitskompass.de (zuletzt abgerufen: 18.08.2023).

14 Keine einheitliche Regelung auf Bundesebene, unterschiedliche, vereinzelte Regulierung auf Landesebene.

15 Zum Beispiel werden *Nudges* als „libertärer Paternalismus“ (Thaler & Sunstein, 2009) bezeichnet und können als Mittelposition zwischen einer Regulierung von oben nach unten betrachtet werden, die die Wahl typischerweise auf eine vorgeschriebene Option beschränkt, und reinem Libertarismus, bei dem alle Auswahl gegeben ist. In einer politischen Umgebung, in der nicht reguliert werden soll oder kann, können Nudges einen Mittelweg bilden. Der traditionelle Nudging-Ansatz bezieht sich auf Individuen. Der Nudging-Ansatz soll ein politisches Instrument sein, der Menschen zu sozial erwünschten Ergebnissen führt und gleichzeitig Zwang vermeiden, wodurch ein Element der freien Wahl erhalten bleibt (Sunstein & Thaler, 2003; Thaler & Sunstein, 2009). Er sollte Regierungen ermöglichen, eine Rolle in Bezug auf gesellschaftlich wünschenswerte Verhaltensweisen zu spielen, die möglicherweise nicht hervorgerufen werden, wenn die Bürgerinnen und Bürger eine vollständige, freie Wahl haben. Thaler, Richard, H., and Cass R. Sunstein. 2003. *Libertarian Paternalism.* American Economic Review, 93 (2): 175–179; und Thaler, R. H., & Sunstein, C. R. (2009). *Nudge:* improving decisions about health, wealth, and happiness. Rev. and expanded ed. New York, Penguin Books.

16 Stiftung Neue Verantwortung (2023), Cybersicherheits-Kompass für Kommunen. https://cybersicherheitskompass.de (zuletzt abgerufen: 18.08.2023).

17 Cyber-Resilienz-Fähigkeiten: Vorfälle antizipieren, Vorfällen zu widerstehen, Zentrale Prozesse und Infrastrukturen (oder Dienstleistungen) aufrechterhalten zu können, Sich von Vorfällen zu erholen, Sich anpassen zu können (Abgeleitet aus BSI-Standard 200-4, the BCI, ENISA, NIST-SP 800-172, MITRE Working Group).

18 Internationales Beispiel: Pohling (2023), Ohio Governor DeWine Announces New Cybersecurity Training for Local Governments. https://tennesseestar.com/the-midwest/ohio-governor-dewine-announces-new-cybersecurity-training-for-local-governments/hpoling/2023/07/18/ (zuletzt abgerufen: 18.08.2023).

19 BSI (2022), IT-Grundschutz-Profil: Basis-Absicherung Kommunalverwaltung. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Basis_Absicherung_Kommunalverwaltung.pdf?__blob=publicationFile&v=9 (zuletzt abgerufen: 18.08.2023).

20 Schuetze (2023), Informationssicherheits von Städten verbessern, Stiftung Neue Verantwortung. https://www.stiftung-nv.de/sites/default/files/informationssicherheit_von_staedten_verbessern.pdf (zuletzt abgerufen: 18.08.2023).

21 Diese Better Practices wurden im Rahmen dieses Projekts in einer Umfrage und in einem Workshop mit Akteuren von Bund, Ländern, Kommunen und Wissenschaft entwickelt.

22 IT-Tickets werden zur internen Verwaltung von Anfragen an den IT-Service oder von Vorgängen erstellt und enthalten eine Problembeschreibung.

23 Die Kritikalität bestimmt die Bedeutung eines Prozesses innerhalb der Verwaltung.

24 Schuetze (2023), Informationssicherheit von Städten verbessern, Stiftung Neue Verantwortung. https://www.stiftung-nv.de/sites/default/files/informationssicherheit_von_staedten_verbessern.pdf (zuletzt abgerufen: 18.08.2023).

25 Schuetze (2023), Informationssicherheit von Städten verbessern, Stiftung Neue Verantwortung. https://www.stiftung-nv.de/sites/default/files/informationssicherheit_von_staedten_verbessern.pdf (zuletzt abgerufen: 18.08.2023).

26 Schuetze (2023), Stellungnahme von Julia Schuetze für die öffentliche Anhörung des Ausschusses für Digitales zum Thema „Cybersicherheit – Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland“. https://www.bundestag.de/resource/blob/929986/a83f11806d0c6b47cead2437e2b35b4f/Stellungnahme-Schuetze-data.pdf (zuletzt abgerufen: 18.08.2023).

27 Schuetze (2023), Informationssicherheits von Städten verbessern, Stiftung Neue Verantwortung. https://www.stiftung-nv.de/sites/default/files/informationssicherheit_von_staedten_verbessern.pdf (zuletzt abgerufen: 18.08.2023).

Danksagungen

Ich bedanke mich herzlich bei den Fachleuten aus Bundes- und Landesbehörden, Kommunen, Wissenschaft, Zivilgesellschaft und Verbänden, die ich in den letzten eineinhalb Jahren zur kommunalen Cybersicherheitspolitik befragt habe oder mit denen ich mich zu dem Thema austauschen konnte.

Insbesondere möchte ich mich für wichtige Impulse bei folgenden Expertinnen und Experten bedanken:

Dr. Götz Fellrath, Professor für Verwaltungsmanagement und E-Government, Hochschule für Polizei und Verwaltung NRW

Sabine Griebsch, Senior Advisor Cyber Resilience, GovThings

Esther Kern, Brandenburg Institut für Gesellschaft und Sicherheit

Marco Lawrenz, scientific consultant politics and public sector, ATHENE – nationales Forschungszentrum für angewandte Cybersicherheit, Berlin

Andreas Lüsebrink, Fachdienstleiter Digitalisierung und IT, Landkreis Märkischer-Kreis, Lüdenscheid

Sabine Meigel, Leitung Abteilung Digitale Agenda, Stadt Ulm

Christian Stuffrein, Referent, Deutscher Landkreistag

Fabienne Tegeler, Fachbereichsleiterin, Fachbereich BL 2 Kundenmanagement und Recht, Bundesamt für Sicherheit in der Informationstechnik

Die Ansichten im Text spiegeln nicht notwendigerweise die der Fachleute, mit denen ich im Austausch stand, oder die ihrer Arbeitgeber wider und alle verbleibenden Fehler sind meine eigenen.

Für die nötige Geduld und Fachexpertise möchte ich vor allem Ferdinand Gehringer danken. Kritik und Kommentare zum Entwurf des Papiers von Ferdinand Gehringer und Dr. Sven Herpig weiß ich sehr zu schätzen.

Besonderer Dank gilt außerdem Ha Thanh Thu Nguyen, die mit ihrer Informations-design-Expertise die Ergebnisse der Studie aufbereitet hat.

Autorin

Julia Schuetze ist Projektleiterin für Cybersicherheitspolitik und -resilienz bei der Stiftung Neue Verantwortung e.V. Seit 2017 leitet sie verschiedene Projekte für die SNV, die sich auf vergleichende Cybersicherheitspolitik, europäische Cybersicherheitspolitik, Cyberoperationen gegen Wahlprozesse und die Cyber-resilienz lokaler Regierungsstellen konzentrieren. Außerdem konzipiert und implementiert sie Übungen zur Cybersicherheitspolitik, an denen mehrere Interessengruppen beteiligt sind.

Impressum

Herausgeberin
Konrad-Adenauer-Stiftung e. V. 2023, Berlin

Kontakt
Ferdinand Alexander Gehringer
Innere- und Cybersicherheit
Analyse und Beratung

ferdinand.gehringer@kas.de

Bildnachweise
Cover mit Material von: rotschwarzdesign – stock.adobe.com

Gestaltung und Satz
KALUZA+SCHMID Studio GmbH, Berlin

Hergestellt mit finanzieller Unterstützung der Bundesrepublik Deutschland.

Konrad-Adenauer-Stiftung e.V.