ITV.SH
Kommunale
Digitalisierung

Jahresbericht 2025

Informationssicherheit

Berichterstattung zur Informationssicherheit
im Geschäftsjahr 2025

Inhalt

Liebe Leser:innen,

Mit dem vorliegenden Bericht zur IT-Sicherheit legen wir erstmals eine systematische Grundlage vor, um Entwicklungen sichtbar zu machen, Herausforderungen einzuordnen und den Handlungsbedarf für die kommunale Ebene in Schleswig-Holstein klar zu benennen. Dass wir diesen Bericht heute vorlegen, ist Ausdruck eines gewachsenen Anspruchs: IT-Sicherheit ist kein Randthema mehr. Sie gehört zum Kern staatlicher Verantwortung und dient somit auch der Verteidigung unseres demokratischen Rechtsstaats.

Die Sicherheit informationstechnischer Systeme ist keine technische Detailfrage. Sie entscheidet darüber, ob staatliches Handeln unter den Bedingungen einer digitalen Gesellschaft überhaupt noch funktioniert. Gerade auf kommunaler Ebene wird das besonders deutlich: Hier treffen steigende Erwartungen an digitale Leistungen unmittelbar auf eine wachsende Bedrohungslage – bei gleichzeitig begrenzten Ressourcen.

Die Angriffe auf öffentliche Einrichtungen nehmen seit Jahren zu: in ihrer Häufigkeit, in ihrer Professionalität und in ihrer Wirkung. Cyberangriffe zielen auf staatliche Strukturen, nutzen systematisch Schwachstellen aus und nehmen bewusst in Kauf, dass Verwaltungen handlungsunfähig werden. Wenn zentrale Systeme ausfallen, steht nicht nur eine IT-Infrastruktur still. In einem solchen Fall steht der Staat an entscheidenden Stellen still.

Für die Kommunen bedeutet das eine grundlegende Verschiebung der Anforderungen. IT-Sicherheit ist Voraussetzung dafür, dass Verwaltung überhaupt noch handlungsfähig bleibt. Gleichzeitig entwickeln Kommunen ihre IT-Landschaft weiter, digitalisieren Verfahren und führen neue Lösungen ein. Sicherheit kann dabei nicht nachgelagert organisiert werden. Sie muss von Anfang an mitgedacht werden. In unserem Bericht zeigen wir auf, was das in der Architektur, in den Prozessen und in der Organisation bedeutet.

Der ITV.SH übernimmt in diesem Kontext Verantwortung als kommunales Kompetenzzentrum. Unsere Aufgabe ist es, Orientierung zu geben, Zusammenarbeit verbindlich zu organisieren und konkrete Unterstützung bereitzustellen. Ziel ist es, IT-Sicherheit in der kommunalen Praxis strukturell und dauerhaft zu verankern. Dazu gehören gemeinsame Standards, abgestimmte Verfahren und ein systematischer Austausch von Wissen und Erfahrungen. Denn eines ist klar: Sicherheit entsteht nicht isoliert, sondern im Verbund.

Die kommenden Jahre werden entscheidend sein. Die Bedrohungslage wird sich weiter verschärfen, während der Druck zur Digitalisierung weiter steigt. Beides lässt sich nicht gegeneinander ausspielen. Im Gegenteil: Ohne ein hohes Niveau an IT-Sicherheit wird Digitalisierung scheitern – nicht nur technisch, sondern auch aufgrund der berechtigten Ansprüche aus der Bevölkerung. Es geht deshalb jetzt darum, IT-Sicherheit konsequent zu priorisieren, strukturell zu stärken und gemeinsam umzusetzen.

Die Sicherung der digitalen Handlungsfähigkeit von Staat und Verwaltung ist keine optionale Aufgabe. Sie ist eine Voraussetzung für das Funktionieren unseres Gemeinwesens. Und sie beginnt in den Kommunen.

Matthi-Bolte Richter

Geschäftsführer des IT-Verbundes Schleswig-Holstein AöR

Der Portalverbund nach § 1 a OZG

Juristische Einordnung, funktionale Bedeutung und Auswirkungen auf die kommunale Informationssicherheit in Schleswig- Holstein

Mit der Einführung des § 1 a OZG hat der Bundesgesetzgeber die zentrale Architekturvorhabe für die föderale Verwaltungsdigitalisierung festgelegt. Der Begriff des Portalverbundes bildet dabei das juristische und technische Leitkonstrukt, das die Verbindung zwischen Bund, Ländern und Kommunen im digitalen Raum normiert. Für die Kommunalverwaltungen in Schleswig-Holstein ist der Portalverbund nicht nur ein technisches Integrationsprojekt, sondern ein rechtlich verbindlicher Rahmen, der die Anforderungen an IT-Sicherheit, Datenschutz, Organisationsstrukturen und technische Standards signifikant erhöht.

§ 1 a OZG ergänzt das OZG um eine föderale Architekturbestimmung, die klarstellt, dass die Verwaltungsportale von Bund und Ländern vernetzt werden müssen. Während das OZG bislang primär auf die Bereitstellung digitaler Verwaltungsleistungen gerichtet war, konkretisiert § 1 a die hierfür notwendige Infrastruktur und die Pflicht zur Interoperabilität der Portale.

Der Portalverbund als architektonisches Fundament

Dieser normierte Portalverbund bildet heute das zentrale architektonische Fundament der föderalen Verwaltungsdigitalisierung. Mit dieser Vorschrift hat der Gesetzgeber nicht lediglich eine technische Vernetzungsoption geschaffen, sondern einen verbindlichen organisatorischen und rechtlichen Rahmen, der die Zusammenarbeit von Bund, Ländern und Kommunen in der digitalen Sphäre maßgeblich strukturiert. Für die Kommunen in Schleswig-Holstein ist der Portalverbund damit weit mehr als ein IT-Konzept: Er verändert die Voraussetzungen für digitale Verwaltungsprozesse grundlegend und hebt die Anforderungen an Informationssicherheit auf ein neues Niveau.

Im Kern verpflichtet § 1 a OZG dazu, die Verwaltungsportale sämtlicher föderalen Ebenen so miteinander zu vernetzen, dass Nutzer:innen digitale Verwaltungsleistungen unabhängig vom gewählten Einstiegsportal auffinden und nutzen können. Damit wird die bisherige Portalvielfalt nicht beseitigt, aber funktional durchlässig gemacht. Dieser Verbund ist kein einzelnes Portal, sondern ein föderales Gesamtsystem aus Landesportalen, dem Bundesportal, kommunalen Zugängen und gemeinsamen Basisdiensten wie Servicekontenlösungen. Die Norm adressiert dabei nicht nur die technologische Verknüpfung, sondern etabliert einen rechtlichen Rahmen für Interoperabilität, Zuverlässigkeit und Sicherheit der Datenverarbeitung innerhalb dieses Netzes.

Governance und föderale Steuerungswirkungen

Der Portalverbund ist damit nicht nur ein technologisches, sondern ein governance-prägendes Instrument. Durch ihn werden Abhängigkeiten geschaffen, die neue Entscheidungs- und Abstimmungsmechanismen notwendig machen. Kommunen müssen künftig deutlich stärker in föderale Steuerungsstrukturen eingebunden werden, etwa durch standardisierte Kommunikationsprozesse, übergreifende Change-Management-Strukturen und verbindliche Verfahren zur Qualitätssicherung. Dies führt zwangsläufig zu einem Professionalisierungsschub innerhalb der Kommunalverwaltungen – sowohl technisch als auch organisatorisch.

Auswirkungen auf die kommunale Ebene

Diese Strukturveränderung hat für die kommunale Ebene erhebliche Konsequenzen. Auch wenn die Kommunen im Wortlaut der Norm nicht ausdrücklich genannt werden, sind die faktisch integraler Bestandteil des Portalverbundes, weil die Länder ihrerseits genannt werden, die kommunalen Verwaltungsleistungen über ihre Landesportale einzubinden. Darauf folgt für die Kommunen eine mittelbare, aber verbindliche Mitwirkungspflicht: Wer digitale Verwaltungsleistungen anbietet, muss diese in einer Weise bereitstellen, die den föderalen Standards genügt. Dies umfasst einheitliche Schnittstellen, sichere Datenübertragungen, die Anbindung

an zentrale Identitätsdienste und die Gewährleistung von Verfügbarkeit und Integrität der eigenen Systeme.

Neue Abhängigkeiten und Risikostrukturen

Besonders bedeutsam ist, dass der Portalverbund eine neue Qualität der gegenseitigen Abhängigkeit erzeugt: Eine Schwachstelle in einem kommunalen System kann potenziell Auswirkungen auf Landes- oder Bundesplattformen haben. Umgekehrt können Störungen auf Bundesebene die kommunale Leistungserbringung beeinträchtigen. Diese Wechselwirkungen verlangen neue Formen des Monitorings, neue Reaktionsketten und ein übergreifendes Risikomanagement, das bislang in vielen Kommunen so noch nicht etabliert ist.

Anforderungen an die Informationssicherheit

Gerade die Anforderungen an die Informationssicherheit sind in der Architektur des Portalverbundes besonders hervorgehoben. Die föderale Verknüpfung führt dazu, dass kommunale Systeme in eine sicherheitskritische Infrastruktur eingebunden werden, in der Schwachstellen einzelner Akteure potenzielle Auswirkungen auf andere Beteiligte haben. Der Portalverbund setzt daher stillschweigend ein vergleichbares Sicherheitsniveau aller angeschlossenen Stellen voraus. Für Kommunen bedeutet dies eine deutlich stärkere Orientierung an den Vorgaben des BSI, eine konsequente Absicherung der Übergabepunkte zu Landesplattformen und eine intensivere Protokollierung sicherheitsrelevanter Ereignisse. Die Nutzung föderierter Authentifizierungsdienste wie der BundID verschärft zudem die Anforderungen an Berechtigungsmanagement, Protokollsicherheit und Manipulationsschutz.

Technischer Reifegrad und Paradigmenwechsel

Hinzu kommt, dass Kommunen zunehmend ein Reifegradniveau erreichen müssen, das mit industriellen Standards vergleichbar ist. Anforderungen wie Zero-Trust-Architekturen, automatisierte Schwachstellenerkennung, Sicherheitsanalytik in Echtzeit oder die Umsetzung von Minimal-Privilege-Privilegien werden künftig nicht mehr optional sein, sondern als Mindeststandard gelten. Diese Entwicklung führt zu einem Paradigmenwechsel: Informationssicherheit wird zu einer Daueraufgaben, die strategisch gesteuert und ressortübergreifend verankert werden muss.

Organisatorische Anforderungen

Doch die Herausforderungen beschränken sich nicht auf technische Aspekte. Auch organisatorisch führt der Portalverbund zu neuen Pflichten. Kommunale Verwaltungen müssen Verfahren implementieren, die den föderalen Melde- und Reaktionsmechanismen bei Sicherheitsvorfällen entsprechen. Verantwortlichkeiten für Datenflüsse und Schnittstellen sind klar zu definieren, und die Dokumentationspflichten steifen, da der Portalverbund die Nachvollziehbarkeit von Transaktionen und Identitätsprüfungen voraussetzt. Gleichzeitig müssen Mitarbeitende für die Arbeit in einer föderierten Plattformstruktur sensibilisiert werden, denn Fehlkonfigurationen oder Unkenntnis über die föderalen Abhängigkeiten können erhebliche Risiken nach sich ziehen.

Governance-Strukturen und Kulturwandel

In diesem Zusammenhang gewinnt die Frage der kommunalen Governance-Strukturen an Relevanz: Die Rolle des Informationssicherheitsbeauftragten, die verlässliche Verankerung des ISMS in der Verwaltungsspitze und die Einführung standardisierter, revisionssicherer Prozesse werden zunehmend Voraussetzung dafür, dass Kommunen den rechtlichen Anforderungen der föderalen Architektur gerecht werden. Viele Kommunen stehen hier vor einem Kulturwandel – weg von einzelnen Verantwortlichen hin zu einem ganzheitlichen Sicherheitsverständnis in der gesamten Organisation.

Chancen und Perspektiven für Schleswig-Holstein

Für Schleswig-Holstein entsteht damit ein ambivalentes, aber zukunftsweisenden Bild. Einerseits verlangt der Portalverbund kontinuierliche Investitionen in Informationssicherheit, Prozessqualität und technische Modernisierung. Andererseits bietet er erstmals eine verbindliche und rechtssichere Grundlage, digitale Verwaltungsleistungen im Verbund bereitzustellen und kom-

munale Angebote in ein föderal orchestriertes digitales Gesamtsystem einzubetten. Der Portalverbund zwingt gewissermaßen zu einem einheitlichen digitalen Verwaltungsstandard – und macht gerade dadurch langfristige Effizienzgewinne möglich.

Strategische Bedeutung der Verwaltungsdigitalisierung

Zugleich eröffnet diese Entwicklung die Chance, Digitalisierung nicht länger als isoliertes IT-Projekt zu betrachten, sondern als strategische Verwaltungsmodernisierung. Die Harmonisierung von Standards, die stärkere Nutzung gemeinsamer Dienste und die Entlastung kleiner Kommunen durch zentrale Lösungen schaffen Gestaltungsspielräume, die in den kommenden Jahren zunehmend wichtig sein werden – insbesondere angesichts des Fachkräftemangels, wachsender Cyberbedrohungen und steigender Erwartungshaltungen der Bürger:innen.

Rolle der Kommunen im Portalverbund

Die kommunale Ebene steht somit an einer wichtigen Schnittstelle. Die Anbindung an den Portalverbund ist kein optionale Zukunftsprojekt, sondern ein rechtlicher Auftrag, eine rechtverbindliche Kommunikationsumgebung und zugleich eine strategische Chance. Wer als Kommune heute die Weichen für ein robustes Informationssicherheits- und Organisationsniveau stellt, wird in der Lage sein, die Potenziale des Portalverbundes auszuschöpfen. Damit wird nicht nur die eigene digitale Leistungsfähigkeit gestärkt; die Kommunen tragen zugleich aktiv zur Stabilität und Funktionsfähigkeit eines föderalen digitalen Gesamtsystems bei, das künftig zu einem zentralen Bestandteil moderner Verwaltungspraxis werden wird.

Unterstützungsrolle des ITV.SH und zentrale Handlungsfelder

Der ITV.SH unterstützt die Kommunen bei diesen Herausforderungen, insbesondere im Hinblick auf die Informationssicherheit. Denn der Portalverbund führt auf kommunaler Ebene zu deutlich erweiterten und konkretisierten Anforderungen an die Informationssicherheit. Besonders relevant sind die folgenden Aspekte:

1. Höhere Schutzbedarfe durch föderierten Datenaustausch

Kommunale Systeme müssen Daten sicher mit Landes- und Bundesportalen austauschen. Dies erhöht den Schutzbedarf insbesondere in den Bereichen:

- Vertraulichkeit,
- Integrität,
- Nachvollziehbarkeit,
- Verfügbarkeit.

Der Portalverbund arbeitet mit personenbezogenen und teilweise besonders schutzwürdigen Daten (Identitätsdaten, Antragsunterlagen, Verfahrensdokumente). Dadurch steigen die Anforderungen an:

- Transportverschlüsselung,
- API-Absicherung,
- Sichere Session-Verwaltung,
- Logging und Protokollierung.

2. Pflicht zur Umsetzung föderierter Authentifizierungs- und Berechtigungskonzepte

Die Nutzung bundes- oder landesweit bereitgestellter Identitätsdienste (z.B. BundID, Servicekonto) verlangt eine robuste kommunale Einbindung. Fehlkonfigurationen können systemübergreifende Sicherheitslücken erzeugen, da Identitätsdaten über mehrere Verwaltungsebenen hinweg verwendet werden.

Kommunen müssen daher:

- Manipulationssicherheit gewährleisten,
- Protokolle korrekt verarbeiten,
- Rollen- und Berechtigungsmodelle harmonisieren,
- Integrität von Antrags- und Identitätsdaten sicherstellen.

3. Notwendigkeit eines durchgängig harmonisierten IT- Sicherheitsniveaus

Der Portalverbund basiert auf dem Prinzip, dass Schwachstellen in einer angeschlossenen Stelle das Gesamtsystem beeinträchtigen können. Deshalb ist ein einheitliches Sicherheitsniveau unverzichtbar.

Für Kommunen bedeutet dies:

- Orientierung an BSI- Grundschutz,
- Einhaltung föderal verbindlicher Mindeststandards,
- Umsetzung von Netzsegmentierung,
- Einsatz gesicherter Übergabepunkte (Gateway-Absicherung),
- Kontrolle und Überwachung sicherheitsrelevanter Ereignisse.

4. Erweiterte organisatorische Sicherungsmaßnahmen

Neben der Technik gewinnt die Organisation an Bedeutung:

- Incident-Response-Prozesse
- Meldepflichten innerhalb des föderalen Verbundes
- Notfallkonzepte und Wiederanlaufstrategien
- Berechtigungsmanagement über mehrere Systeme hinweg
- Schulungen für Mitarbeitende, die mit föderalen Diensten arbeiten.

5. Verantwortlichkeitszuordnung im föderalen Sicherheitsverbund

Bei Sicherheitsvorfällen müssen Kommunen und in persona die jeweiligen Verwaltungsleitungen klar nachweisen können:

- Welche Daten übertragen wurden,
- Welcher technische Endpunkt beteiligt war,
- Wer für welche Systemkomponenten verantwortlich ist.

Die Dokumentations- und Rechenschaftspflichten steigen damit erheblich.

Fazit

Der Portalverbund nach § 1a OZG stellt die kommunale Ebene damit vor tiefgreifende strukturelle und sicherheitsrelevante Veränderung, eröffnet ihr jedoch zugleich neue strategische Handlungsspielräume. Kommunen sind nicht mehr lediglich technische Anschlussnehmer föderaler Systeme, sondern aktive Akteurinnen in einem vernetzten digitalen Gesamtraum, dessen Stabilität und Leistungsfähigkeit maßgeblich von ihrem Beitrag abhängt. Die Anforderungen an Interoperabilität, Sicherheit, Governance und Nachvollziehbarkeit werden in den kommenden Jahren weiter steigen. Wer diese Entwicklungen frühzeitig aufgreift, interne Strukturen professionalisiert und Informationssicherheit als dauerhaften Führungsauftrag versteht, positioniert sich nicht nur rechtssicher, sondern schafft die Voraussetzung für eine moderne, resiliente und bürgerorientierte Verwaltung. Der Portalverbund ist damit nicht allein eine gesetzliche Vorgabe – er ist ein zentraler Baustein der öffentlichen Daseinsvorsorge der Zukunft.

Kontakt

Heike Ghiladi
ITV.SH | Justiziarin & Informationssicherheitsbeauftragte

heike.ghiladi@itvsh.de
+49 431 530550-12

Die Betrachtung des Portalverbundes im vorherigen Artikel macht eindrücklich deutlich, wie stark sich die Rahmenbedingungen kommunaler Digitalisierung in den vergangenen Jahren gewandelt haben. Mit der Einführung des § 1 a OZG ist ein verbindliches architektonisches Grundgerüst entstanden, das nicht nur die technische Interoperabilität zwischen Bund, Ländern und Kommunen regelt, sondern gleichzeitig hohe Anforderungen an Informationssicherheit, Datenschutz, Dokumentation und organisatorische Verlässlichkeit stellt. Die kommunale Ebene ist damit längst nicht mehr nur „Anwenderin" föderaler Basisdienste, sondern integraler Bestandteil eines vernetzten digitalen Gesamtsystems, dessen Stabilität entscheidend davon abhängt, dass jede angeschlossene Stelle ein vergleichbar hohes Sicherheitsniveau gewährleistet.

Diese strukturelle und normative Verdichtung führt allerdings zu einer wachsenden Komplexität in den kommunalen IT-Landschaften. Die Notwendigkeit, föderierte Identitätsdienste einzubinden, sensible Daten über gesicherte Schnittstellen mit Landesportalen auszutauschen, Protokollierungs- und Meldeprozesse einzuhalten oder ein konsistentes Berechtigungsmanagement über mehrere Ebenen hinweg zu implementieren, bedeutet für die Kommunen steigende technische und organisatorische Anforderungen – bei gleichzeitig begrenzten Ressourcen und steigenden Erwartungen der Öffentlichkeit.

Genau an dieser Stelle setzt der folgende Beitrag „Onlinedienste aber sicher" an. Er führt die im vorangegangenen Leittext beschriebenen strategischen und rechtlichen Anforderungen in den operativen Alltag der kommunalen Verwaltung über und zeigt detailliert auf, welche Risiken sich aus der zunehmenden Digitalisierung von Verwaltungsverfahren tatsächlich ergeben. Durch die Vielzahl beteiligter Systeme – von Formularservern über Authentifizierungs- und Bezahlsysteme bis hin zu Bundes- und Landesportalen – entsteht eine komplexe föderale Servicearchitektur, bei der jedes zusätzliche technische Bindeglied potenziell eine neue Angriffsfläche darstellen kann.

Der Beitrag macht deutlich, dass Informationssicherheit kein abstraktes Fachthema ist, sondern eine betriebswirtschaftliche und verwaltungsorganisatorische Notwendigkeit. Er zeigt zugleich, wie Verwaltungen diese Herausforderungen praktisch bewältigen können: mithilfe eines methodischen Informationssicherheitsmanagements (ISMS) nach SiKoSH, regelmäßigen Sicherheitsprüfungen, der Nutzung zentraler Warn- und Unterstützungsstrukturen wie CERT-Nord oder durch gezielte Sensibilisierung der Mitarbeitenden. Damit schließt er nahtlos an die vorgelagerten strategischen Überlegungen an und übersetzt sie in konkrete Handlungsempfehlungen für die kommunale Praxis.

Onlinedienste aber sicher!

Management Summary

Durch die digitale Transformation der Verwaltung werden auf der einen Seite immer mehr Verwaltungsverfahren digitalisiert. Auf der anderen Seite verstärkt diese kriminellen Aktivitäten mittels Cyberattacken verbunden mit hohen Risiken hinsichtlich eines Stillstands der kommunalen IT, des Verlusts wertvoller Daten und ggf. auch hoher finanzieller Schäden zur Systemwiederherstellung oder auch immaterieller Schäden wie Rufschäden. Der ITV.SH bietet in Zusammenarbeit mit dem Zentralen IT-Management des Landes (ZIT-SH), Dataport und dem CERT-Nord seinen Trägern verschiedene Unterstützungsangebote im Bereich Informationssicherheit, Datenschutz und Notfallmanagement an:

- Hilfsmittel zum Aufbau eines Informationssicherheitsmanagementsystems (ISMS) mittels SiKoSH
- Consultingleistungen zum Aufbau eines ISMS nach SiKoSH durch Dataport
- Informationen zur Sicherheitslage durch das Portal des CERT-Nord
- Sicherheitsprüfung der kommunalen IT durch Schwachstellenscans
- Unterstützungsleistungen im Notfall durch Notfallhotline des CERT-Nord
- ITV.SH-Netzwerktreffen im Kontext Informationssicherheit
- ITV.SH-Netzwerktreffen im Kontext Datenschutz
- ITV.SH-Forum
- SiKoSH-Workshops
- Sensibilisierungen und Schulungen

Diese Angebote sollen dabei helfen, das Betriebsrisiko der Verwaltungen zu senken und damit auch eine mögliche persönliche Haftung für Schäden durch die Behördenleitungen im Rahmen ihrer Gesamtverantwortung für die innerbehördliche Organisation zu reduzieren. Diese sollen nachfolgend zusammen mit den Regelungen zur jeweiligen Beantragung kurz skizziert werden. Besonders bemerkenswert ist, dass alle Angebote nicht nur kommunal maßgeschneidert, sondern auch völlig kostenfrei sind.

Ausgangslage

Alle Verwaltungsleistungen auch online? Von dieser Praxis sind wir nicht mehr weit entfernt. Neue digitale Angebote bergen aber auch neue Risiken in sich und insofern sind die Erwartungen in Sachen Schutz der zu verarbeitenden Informationen nicht nur seitens des Gesetzgebers, sondern auch seitens der Bürgerinnen und Bürger als Kundinnen und Kunden der Verwaltungsleistungen hoch.

Neben einem benutzerfreundlichen niederschwelligen Zugang zu den neuen Diensten ist insbesondere auch das Vertrauen in eine ordnungsgemäße und sichere Datenverarbeitung auf Kundenseite entscheidend für den Erfolg digitaler Angebote.

Soweit die Theorie. Was zeigt uns die Praxis?

Onlinedienste sind sehr komplex. Es erfordert eine aufwendige Infrastruktur zur medienbruchfreien digitalen Bereitstellung der Onlinedienste (beginnend mit der Suche eines passenden Dienstes bis hin zur Bescheidung). Da bedarf es Webserver, Formularserver, Authentifizierungsserver, Bezahlsysteme, etc. um nur einige Systeme zu nennen. Keine Kommune kann das alleinstehend stemmen und so gibt es folgerichtig der föderalen Infrastruktur entsprechend Bundes-, Landes- und kommunale Systeme, die miteinander zahlreiche Schnittstellen zur gegenseitigen Kommunikation vorhalten.

Fest steht: jede Schnittstelle birgt ein Risiko hinsichtlich eines unberechtigten Missbrauchs in sich. Je mehr Schnittstellen untereinander, umso höher das Risiko, wobei mit Risiko ganz klassisch der Multiplikator zwischen Eintrittswahrscheinlichkeit und erwarteter Schadenshöhe gemeint ist.

Diese Risiken sind nicht nur theoretisch, sondern treten auch ein, wie fast täglich der Presse oder auch bewährten Informationsquellen wie beispielsweise der Übersicht https://kommunaler-notbetrieb.de/ des Informationssicherheitsbeauftragten (ISB) der Stadt Kassel Jens Lange entnommen werden kann. Die Risikobehand-

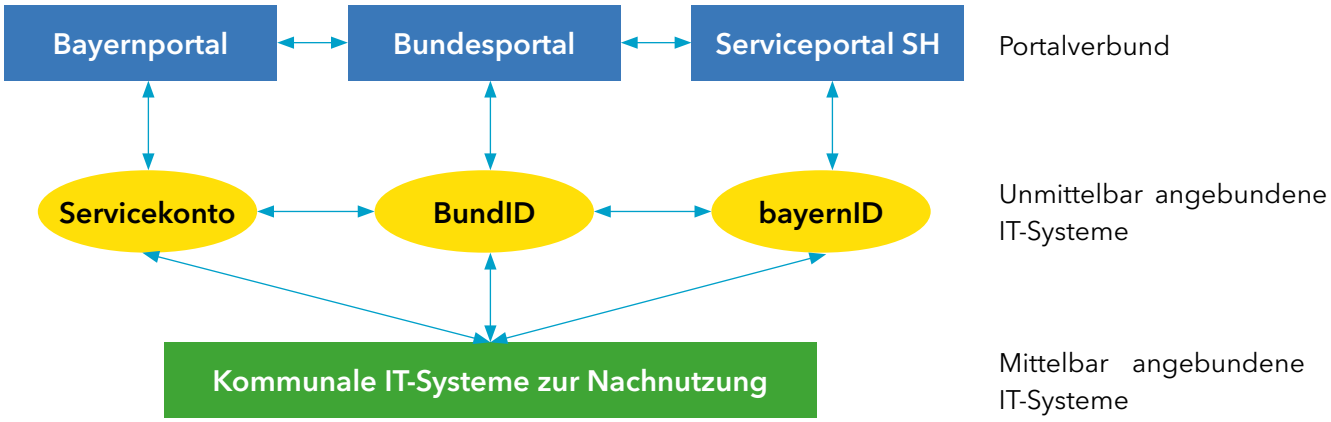
lung ist indes komplex; es stehen vier Methoden zur Verfügung in Form der Vermeidung, der Reduzierung, der Verlagerung und der Akzeptanz.

Die Vermeidung, also der Verzicht auf den Betrieb einer IT-Infrastruktur oder eines IT-Verfahrens aufgrund zu hoher Risiken kommt im Behördenbereich in der Regel nicht in Frage, da die umzusetzenden IT-basierten Behördenprozesse üblicherweise gesetzlich vorgegeben sind. Ein Risikotransfer, also die Verlagerung des Risikos auf einen Dritten z. B. in Form einer Cyberversicherung bedarf zahlreicher Vorbereitungen in mehr vorgehaltener IT-Sicherheit, da kein Versicherer ein unkalkulierbares Risiko absichern würde; zu bedenken ist dabei auch, dass nur materielle Schäden, aber z. B. keine Rufschäden abgesichert werden können. Die Risikoakzeptanz, also das Hinnehmen, dass gewisse Risiken nicht oder nur unter sehr erhöhten Bedingungen (wie z. B. Kosten) weiter reduziert werden können, hängt immer vom Risikoappetit der risikotragenden Person, also der Behördenleitung, ab.

Dieses gilt umso mehr im Kontext der sich immer mehr verstärkenden Zusammenarbeit im Rahmen der digitalen Bereitstellung von Verwaltungsleistungen.

Zusammenarbeit

Hier bedarf es klarer Spielregeln für die behördliche Zusammenarbeit untereinander innerhalb unseres föderativen Aufbaus. Die Spielregeln liegen auch vor und zwar in Form der Verordnung zur Gewährleistung der IT-Sicherheit der im Portalverbund und zur Anbindung an den Portalverbund genutzten IT-Komponenten (IT-Sicherheitsverordnung Portalverbund - ITSiV-PV). Diese Rechtsverordnung gestaltet die Anforderungen des § 5 OZG für die Informationssicherheit aus.



Die Rechtsverordnung unterscheidet zwischen dem Portalverbund, der sich aus den Serviceportalen des Bundes (https://verwaltung.bund.de/portal/) und den einzelnen Landesportalen, wie z. B. das Serviceportal SH (https://serviceportal.schleswig-holstein.de/Verwaltungsportal/) zusammensetzt und den zentralen Einstiegspunkt für die Dienste der angebundenen IT-Systeme darstellen.

Hinsichtlich der angebundenen IT-Systeme wird noch zwischen unmittelbar und mittelbar angebundenen IT-Systemen unterschieden.

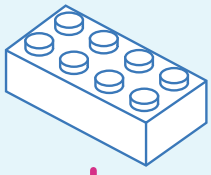
Unmittelbar angebunden bedeutet in diesem Fall, dass die angebundenen IT-Systeme unmittelbar Daten mit dem Portalverbund austauschen. Das betrifft dann nicht nur IT-Systeme des Bundes und der Länder wie z. B. die OSI-Infrastruktur bei Dataport, die beispielsweise zentrale Online-, Authentifizierungs- (Servicekonto SH) und Bezahldienste (ePayBL) beinhaltet, sondern durchaus auch kommunale IT-Systeme wie Formularserver, die mit den IT-Systemen des Bundes und der Länder kommunizieren, um z. B. den Bezahldienst ePayBL zu nutzen. Das gilt dann im Übrigen auch für in Auftragsverarbeitung betriebene Formulardienste, wo nach der DSGVO der Auftraggeber gegenüber dem Auftragsverarbeiter verantwortlich ist für die Einhaltung der datenschutzrechtlichen Grundsätze inklusive Vertraulichkeit, Integrität und Verfüg-

barkeit. Wer unmittelbar angebundene IT-Systeme betreibt, hat ein sich auf dem Stand der Technik befindliches Informationssicherheitsmanagementsystem (ISMS) aufzubauen und in diesem alle sicherheitsrelevanten Rollen (Aufbauorganisation) und Prozesse (Ablauforganisation) und alle ergriffenen Maßnahmen zur Risikominimierung zu dokumentieren und in einem kontinuierlichen PDCA-Zyklus fortzuschreiben. Dabei geht es darum, die identifizierten behördeninternen Prozesse einer Risikobewertung zu unterziehen und technische und organisatorische Maßnahmen umzusetzen, die das Betriebsrisiko auf ein für den Betreiber vertretbares Risiko zu senken. Ca. 8.000 zu betrachtende Anforderungen hält das BSI in 111 verschiedenen Bausteinen bereit, wobei zur vollständigen Absicherung dann grundsätzlich je nach Risikobewertung noch selber definierte Maßnahmen hinzukommen müssen. Zudem sind diverse Technische Richtlinien des BS zu berücksichtigen, ein Notfallmanagement aufzubauen und Pentests und Webchecks durchzuführen.

Wer die zentralen Dienste lediglich nachnutzt, ist entsprechend des Wortlauts der ITSiV-PV mittelbar angebunden, hier gelten deutlich weniger Spielregeln. Allerdings ist auch hier ein ISMS aufzubauen, als Mindestsicherheitsniveau wird hier aber die Umsetzung der Basis-Absicherung genannt. Das heißt, dass sich die potentiell umzusetzenden Maßnahmen auf ca. 2.000 reduzieren und die Verpflichtung durch weitere Auflagen entfällt. Potentiell umzusetzende Maßnahmen heißt in diesem Kontext, dass man für nicht vorhandene Komponenten keine Maßnahmen umzusetzen braucht; wer also zum Beispiel keinen Webserver betreibt, kann die korrespondierenden Maßnahmen hierfür von vornherein weglassen. Unter der Berücksichtigung, dass der Aufbau eines ISMS mit dem Niveau Basisabsicherung genau das SiKoSH-Ziel ist, dann reduziert sich der Umsetzungsaufwand nochmals erheblich.

Aufbau eines ISMS mit SiKoSH

SiKoSH (Sicherheit für Kommunen in Schleswig-Holstein) ist ein Informationssicherheitsframework, das durch den IT-Verbund Schleswig-Holstein, der Staatskanzlei Schleswig-Holstein, dem Unabhängigen Landeszentrum für Datenschutz, dem Landesrechnungshof Schleswig-Holstein und zahlreichen Praktikern aus Schleswig-Holsteins Kommunalverwaltungen sowie Dataport AöR in partnerschaftlicher Zusammenarbeit entwickelt und gepflegt wird.



Die BSI-IT-Grundschutzbausteine definieren Anforderungen an Informationssicherheit.

Das IT-Grundschutzprofil „Basis-Absicherung Kommunalverwaltung“ wählt die für kommunale Einrichtungen nötigen Bausteine und kommunalen Basisanforderungen aus.

SIKO.SH
Sicherheit für Kommunen

Die SiKoSH-Methodik setzt die Anforderungen der Bausteine effizient, praxisorientiert und wirksam um.

Ziel ist der Aufbau eines geregelten Informationssicherheitsmanagementsystems (ISMS) auf Basis des BSI-Grundschutzstandards 200-2. Die 111 BSI-IT-Grundschutzbausteine liefern dabei die umzusetzenden Anforderungen auf Grundlage des Stands der Technik und das IT-Grundschutzprofil „Basis-Absicherung Kommunalverwaltung" fungiert als kommunaler Filter. Hier wird eine typische Modellkommune mit all Ihren sicherheitsrelevanten Assets wie z. B. Server, Clients und Gebäude betrachtet. Das reduziert die umzusetzenden Anforderungen nochmals um die Hälfte auf ca. 1.000.

SiKoSH baut auf dem BSI IT-Grundschutzprofil Basis-Absicherung Kommunalverwaltung auf und liefert kochbuchartig Rezepte für eine effektive Umsetzung der Anforderungen. Der Standard kann kostenlos unter www.sikosh.de heruntergeladen werden.

Er gliedert den komplexen Prozess zur Umsetzung des BSI-Grundschutzes in sieben Phasen:

1. Organisatorische Grundlagen (Aufbau- und Ablauforganisation ISMS)
2. Sensibilisierung und Schulung (Technik kann unmöglich alle Risiken abfedern, der Mensch ist ein sehr wesentlicher Faktor der Mensch in der Kette Informationssicherheit)
3. Standard-Regelungen (wie z. B. Datenschutz, Virenschutz)
4. Allgemeine Musterregelungen (wie z. B. Gebäudemanagement)
5. Technische Musterregelungen (wie z. B. Server, Vernetzung)
6. Regelungen für Verfahren (wie z. B. Verzeichnisdienste)
7. Notfallmanagement (wie z. B. Behandlung von Sicherheitsvorfällen)

Die Umsetzungsreihenfolge der einzelnen Kapitel sollte sich dabei nach den Ergebnissen eines vorab durchgeführten Selbstaudits in Form eines SiKoSH-Querschnittsquickchecks im Excel-Format richten. Anhand der Ergebnisse sieht man sehr schnell, wo ein akuter Nachholbedarf vorliegt und wo man bereits gut aufgestellt ist. Wenn beispielsweise das Netzwerk Lücken aufweist, empfiehlt sich eine Priorisierung der Phase 5.

Der SiKoSH-Standard zeigt dann innerhalb der Phasen auf, was wann gemacht werden sollte und welche Anforderungen dabei umgesetzt werden sollten, zahlreiche Hilfsmittel wie Richtlinien, Beispiele und eine Musterleitlinie runden das Angebot ab.

Der Einstieg ist nachweislich einfach und schnell und besteht aus einer Bestandsaufnahme der Phase 1, der Erstellung einer Informationssicherheitsleitlinie anhand des SiKoSH-Musters, der Benennung eines Informationssicherheitsbeauftragten (ISB) mittels vorgefertigter Bestellurkunde und der Beschreibung der behördeninternen Aufbau- und Ablauforganisation im Informationssicherheitsmanagement anhand der mitgelieferten Richtlinie ISMS, die nach entsprechenden individuellen Anpassungen in eine Dienstanweisung oder Dienstvereinbarung umgewandelt werden kann.

Dokumentiert wird das ganze dann in der neuen ISMS-Übersicht, die die Umsetzungserfolge grafisch für das Managementberichtswesen aufbereitet.

SiKoSH-Beratung

Informationssicherheit ist das Fundament einer modernen Verwaltung. Doch wie gelingt der Aufbau eines geregelten Informationssicherheitsmanagements, ohne den täglichen Dienstbetrieb zu blockieren? Die Lösung liegt in einem methodischen Vorgehen, das Sicherheit und Verwaltungspraxis in Einklang bringt. Das Zentrale IT-Management Schleswig-Holstein fördert die Einführung der SiKoSH-Methodik in den Kommunen und bietet hierzu voraussichtlich ab Q2/2026 entsprechende Unterstützungsleistungen an. Hierzu führen Sicherheitsexperten von Dataport einen Aufklärungsworkshop mit interessierten Kommunen durch, um dann anhand des festgestellten Bedarfs eine zielgerichtete Beratung durchzuführen hin zu einer erhöhten Resilienz der Behörde gegenüber Bedrohungen. Interessenten wenden sich hierzu formlos per E-Mail an sikosh@itvsh.de.

Informationen zur Sicherheitslage

Schützen kann sich nur, wer vorbereitet ist. Und dazu sollte man gut hinsichtlich der aktuellen Sicherheitslage und potentieller Bedrohungen

informiert sein. Das bei Dataport aufgehängte Computer Emergency Response Team (CERT Nord, https://www.certnord.de/) beobachtet weltweit die Informationssicherheitslage, warnt vor IT-Sicherheitsbedrohungen (offengelegte Schwachstellen), erstellt Lagebilder und begleitet unterstützend bei Vorfällen.

Die Warnung vor den IT-Sicherheitsbedrohungen erfolgt im Auftrag der Dataport-Trägerländer für die beteiligten Landesressorts. Diese Informationen stehen grundsätzlich auch Kommunen zur Verfügung. Hier ist allerdings zu beachten, dass diese Informationen teilweise sicherheitssensitiv sind und daher entsprechend des Traffic-Light-Protokolls (TLP-Protokoll) eingestuft werden. Der Zugriff auf vertrauliche Informationen darf nur gewährt werden, wenn eine entsprechende persönlich unterzeichnete Vertraulichkeitserklärung vorliegt. Teilnahmeberechtigt sind bestellte ISB, DSB und IT-Verantwortliche unserer Träger. Der Antrag erfolgt über den OZG-Shop des ITV.SH: https://shop-digitales.schleswig-holstein.de/CERT-Nord/SW10134.

Frei verteilbare Sicherheitsinformationen (tlp clear) des CERT-Nord stellt der ITV.SH seinen Trägern in seiner Kollaborationsplattform unter https://netzwerk.itvsh.de/project/aktuelle-cert-warnungen/ zur Verfügung. Zum Zugriff ist – sofern noch nicht geschehen – eine einmalige Registrierung erforderlich.

Sicherheitsprüfung der kommunalen IT durch Schwachstellenscans

Das Zentrale IT-Management des Landes Schleswig-Holstein bietet den Trägern des ITV.SH einen professionellen Schwachstellenscan zur Aufdeckung möglicher Sicherheitsbedrohungen (Schwachstellen in der IT-Infrastruktur) an. Interessenten wenden sich bitte formlos per E-Mail an info@itvsh.de. Nach Unterzeichnung eines LOI erhalten die Träger des ITV.SH im Rahmen eines Proof of Concept folgende Leistungen durch die beauftragte Firma Greenbone:

- Abstimmungsgespräch zur Aufnahme der Rahmenbedingungen
- Zeitlich begrenzte Bereitstellung einer Appliance (vorzugsweise eine virtuelle Appliance)
- Kick-Off-Gespräch zum Start
- Zwischenbesprechung nach 1 – 2 Wochen
- Abschlussgespräch mit Festlegung weiterer Schritte

Unterstützungsleistungen im Notfall durch Notfallhotline des CERT-Nord

Das CERT-Nord stellt 24/7 eine Hotline zur Meldung von Sicherheits- und Notfällen bereit und zwar zu den Servicezeiten über die Hotline (0431 3295-1984), außerhalb der Servicezeit über die Rufbereitschaft 040 428 99-6710).

Das CERT Nord klärt mit dem Melder (ISB oder fachkundige IT-Kraft) wichtige Details (Name, Telefonnummer, Dienststelle) und führt mit dem Melder eine erste Analyse des möglichen Vorfalls durch. Auf Grundlage dieser Ergebnisse werden dann weitere Unterstützungsmaßnahmen, wie z. B. tiefergreifende forensische Untersuchungen angestoßen.

ITV.SH-Netzwerktreffen im Kontext Informationssicherheit

Der ITV.SH lädt regelmäßig zu einem Netzwerktreffen im Kontext Informationssicherheit ein. Angesprochen sollten sich hier insbesondere bestellte interne und externe Informationssicherheitsbeauftragte fühlen. Nach dem Auftakt 2025 mit einer Veranstaltung zum Thema Hacking und eine über die seinerzeit existierenden Angebote zur Beratung und Unterstützung im Kontext Informationssicherheit und Datenschutz sind für 2026 drei Treffen geplant, mögliche Themen sind „kommunales Sensibilisierungs- und Schulungskonzept“ sowie „Cyberversicherungen“.

Die Einladung erfolgt über die ITV.SH-Kollaborationsplattform unter https://netzwerk.itvsh.de/project/netzwerktreffen-informationssicherheit/, auch hier ist eine einmalige Registrierung erforderlich. Anregungen für weitere interessante Themen werden sehr gerne berücksichtigt.

ITV.SH-Netzwerktreffen im Kontext Datenschutz

Der ITV.SH lädt regelmäßig zu einem Netzwerktreffen im Kontext Datenschutz ein. Angesprochen sollten sich hier insbesondere bestellte interne und externe Datenschutzbeauftragte

fühlen. Nach dem Auftakt 2025 mit einer Veranstaltung zum Thema OZG und Datenschutz sind für 2026 zwei Treffen geplant, ein mögliches Thema ist dabei das „Verhältnis Informationsfreiheit gegenüber dem Datenschutz".

Die Einladung erfolgt über die ITV.SH-Kollaborationsplattform unter https://netzwerk.itvsh.de/project/netzwerktreffen-datenschutz/, auch hier ist eine einmalige Registrierung erforderlich. Anregungen für weitere interessante Themen werden sehr gerne berücksichtigt.

ITV.SH-Forum

Das nächste ITV.SH-Forum findet Anfang Juni statt; weitere Infos hierzu folgen zeitnah. Geplant im Kontext Informationssicherheit ist ein Vortrag über einen prominenten Sicherheitsvorfall aus der Sicht eines betroffenen IT-Verantwortlichen sowie ein Einführungsworkshop in die SiKoSH-Vorgehensweise.

SiKoSH-Workshops

Auch unabhängig vom ITV.SH-Forum werden bei Bedarf noch weitere SiKoSH-Workshops im Jahr 2026 durchgeführt, so auch am 11.02.2026. Damit werden drei Ziele verfolgt, Neulinge werden in die SiKoSH-Vorgehensweise eingeführt, Fortgeschrittene werden mit Updates versorgt und die Gemeinschaft profitiert direkt von Anregungen zur Überarbeitung und Fortschreibung von SiKoSH. Anmeldungen werden per E-Mail erbeten unter info@sikosh.de.

Sensibilisierungen und Schulungen

Das Land Schleswig-Holstein entwickelt derzeit für die eigenen Ressorts Schulungs- und Sensibilisierungsprogramme, die sowohl toolgestützt als auch in Präsenzformaten angeboten werden sollen. Eine kommunale Mitnutzungsmöglichkeit ist vorgesehen.

Fazit

100%-ige Sicherheit gibt es nicht und insofern müssen sich die Bestrebungen darauf ausrichten, mögliche Risiken auf ein akzeptables Restrisiko zu reduzieren. Zur Zielerreichung werden zahlreiche unterschiedliche Methodiken seitens ITV.SH, ZIT-SH, Dataport und CERT-Nord angeboten, die zwingenderweise auch im Gesamtzusammenhang betrachtet und genutzt werden müssen. Dabei ist noch einmal zu betonen: alle Angebote sind für die Träger des ITV.SH kostenfrei.

Kontakt

Frank Weidemann
ITV.SH | Behördlicher Datenschutzbeauftragter

frank.weidemann@itvsh.de

+49 431 530550-13

Während der Beitrag „Onlinedienste aber sicher“ die operative Ebene kommunaler IT-Sicherheit beleuchtet und die praxisnahe Unterstützungsangebote aufzeigt, wird im folgenden Artikel deutlich, wie entscheidend die Frage nach der Resilienz der kommunalen IT-Infrastrukturen mittlerweile geworden ist. Die dort beschriebenen Entwicklungen – von der Professionalisierung krimineller Akteure über die zunehmende Organisiertheit internationaler Angriffe bis hin zu staatlich gesteuerten Cyberoperationen – zeigen, dass Kommunen sich heute nicht mehr nur gegen sporadische Vorfälle schützen müssen, sondern gegen eine globalisierte, permanente und zunehmend automatisierte Bedrohungslage.

Besonders eindrücklich ist die Darstellung der potenziellen Folgen erfolgreicher Cyberangriffe: Der Ausfall kritischer Verwaltungsdienste, Verzögerungen bei existenziell bedeutsamen Leistungen wie Sozialzahlungen oder Kfz-Zulassungen, immense wirtschaftliche Schäden durch Wiederanlaufmaßnahmen sowie ein möglicher Vertrauensverlust in die Leistungsfähigkeit staatlicher Institutionen. Kommunale Verwaltungen stehen damit an einem Punkt, an dem die Sicherstellung digitaler Handlungsfähigkeit nicht nur eine technische Aufgabe, sondern eine zentrale Voraussetzung für Demokratie, Daseinsvorsorge und gesellschaftliche Stabilität geworden ist.

Der Artikel von Dataport Kommunal knüpft daher folgerichtig an die zuvor vorgestellten Maßnahmen und Standards an, geht jedoch einen entscheidenden Schritt weiter: Er zeigt, welche infrastrukturellen, organisatorischen und operativen Voraussetzungen tatsächlich notwendig sind, um die Resilienz der kommunalen IT effektiv zu stärken. Besondere Aufmerksamkeit erhält dabei die Rolle von Dataport als zentralem IT-Dienstleister, der mit einem hochsicheren, redundant aufgebauten Rechenzentrum, einem mehrschichtigen Sicherheitsmodell, einem permanent überwachenden Security Operations Center (SOC) und einem umfangreichen Notfallmanagement echte Schutzarchitektur bereitstellt.

Diese Darstellung ergänzt die zuvor beschriebenen Grundlagen von SiKoSH, CERT-Nord und Schwachstellenscans um eine Perspektive, die zeigt, wie Kommunen professionelle IT-Sicherheits- und Resilienzstrukturen nutzen können, um die eigene Leistungsfähigkeit dauerhaft zu sichern. Sie macht zudem deutlich, dass IT-Sicherheit längst nicht mehr nur aus technischen Maßnahmen besteht, sondern aus einem Zusammenspiel von Governance, Prozessen, Schulungen, Infrastruktur und permanenter Weiterentwicklung. Damit vertieft der folgende Beitrag den Fachdiskurs und zeigt auf, wie eine moderne, stabile und sichere digitale kommunale Verwaltung konkret aufgebaut sein muss.

Sichere Kommunen in digitalen Zeiten: Dataport stärkt IT-Sicherheit und Resilienz

Die Digitalisierung in Kommunen schreitet mit großen Schritten voran. Digitale Verwaltungsdienste, Online-Bürgerportale und vernetzte Infrastrukturen eröffnen viele neue Möglichkeiten. Sie bieten ein großes Potenzial für die Bewältigung der aktuellen und zukünftigen Herausforderungen und übernehmen eine Schlüsselrolle bei der Gestaltung zukunftsfähiger Kommunen.

Gleichzeitig entstehen durch die Digitalisierung aber auch herausfordernde Risiken, die die kommunale IT und damit Arbeits- und Funktionsfähigkeit der Kommunen insgesamt bedrohen. Die Themen IT-Sicherheit und Resilienz gewinnen angesichts wachsender Cyber-Bedrohungen und steigender Anforderungen an die Verfügbarkeit kommunaler IT-Systeme immer mehr an Bedeutung. Anfänglich waren es noch einzelne Hacker, die versucht haben, IT-Systeme zu kompromittieren. Später war eine Professionalisierung der Kriminalität bis hin zu organisierten Banden zu beobachten. Mit der Zunahme der globalen politischen Spannungen und spätestens seit dem Angriff Russlands auf die Ukraine kommen vermehrt staatlich gelenkte Angriffe auf IT und IT-Infrastrukturen hinzu. Das Risiko und die potenziellen Schäden nehmen also zu. Alle Statistiken und Zahlen zeigen eine rasante Entwicklung nach oben. Die Bedrohungen nehmen weiterhin dramatisch zu. Zu hoffen, sie wären eine temporäre Erscheinung, ist illusorisch.

Niemand ist vor Bedrohungen sicher,

- sie finden rund um die Uhr statt,
- sie halten sich nicht an Öffnungszeiten der Verwaltung,
- sie nehmen keine Rücksicht auf Unterbesetzungen durch Krankheiten,
- Sonn- und Feiertage sind ihnen nicht heilig.

Die Folgen von geglückten Cyberangriffen sind für die kommunale Daseinsvorsorge gravierend. Wenn die IT ausfällt, können wichtige Verwaltungsleistungen nicht mehr erbracht werden. Das betrifft zum Beispiel die Auszahlung von Sozialleistungen, die Verlängerung von Ausweisen oder die Zulassung von Fahrzeugen. Für viele Menschen sind diese Dienste lebenswichtig, und Verzögerungen können gravierende Probleme verursachen.

Darüber hinaus entstehen durch erfolgreiche Zwischenfälle hohe Kosten für die Wiederherstellung der Systeme und den Arbeitsausfall. In manchen Fällen kann es sogar notwendig sein, den Katastrophenfall auszurufen, um die Lage zu bewältigen. Cyberattacken sind also in hohem Maße geeignet, Kommunen für einen längeren Zeitraum zu beeinträchtigen oder vollständig funktionsunfähig zu machen. Darüber hinaus können hohe Vertrauensverluste für das Funktionieren des Gemeinwesens und das Funktionieren unserer Demokratie entstehen – sind Kommunen doch für viele Menschen der Kristallisationspunkt für die örtliche Gemeinschaft und das Leben in unserem Staat – ein fatales Signal.

Ein Gedanke könnte natürlich in diesem Zusammenhang auch sein:

- Verzicht auf Digitalisierung,
- IT nur noch innerhalb der Verwaltung,
- keine oder nur gering vernetzten Infrastrukturen.

Die Idee „möglichst wenig Angriffsfläche zu bieten“ erscheint auf den ersten Blick bestechend und einfach.

Die großen strukturellen Probleme für die Zukunftsfähigkeit der Kommunen werden sich auf diesem Weg jedoch nicht lösen lassen.

- Es würde zwangsläufig noch mehr Personal benötigt.
- Verwaltungsvorgänge würden nur in geringem Umfang verkürzt und vereinfacht werden.
- Prozesse und Verwaltungen würden sich noch weiter von den dynamischen Entwicklungen in der privaten Wirtschaft abkoppeln.

Die Herausforderungen, denen sich Kommunen durch den demografischen Wandel und die Finanzknappheit stellen müssen, verschärfen sich, anstatt sie zu verringern.

Die Kommunen müssen sich also

- intern weiter digitalisieren,
- Verwaltungsleistungen automatisieren,
- Verwaltungsleistungen online verfügbar machen,
- Prozesse vereinfachen und Ende-zu-Ende digital anbieten
- übergreifend zusammenarbeiten.

Moderne, vernetzte und verbundene IT und IT-Infrastrukturen werden verstärkt Einzug in Verwaltungen halten (müssen).

Wie kann man diesen scheinbaren Widerspruch auflösen?

Die Lösung ist eine Stärkung von Sicherheit und Resilienz aller Informationssicherheitsbereiche.

Als IT-Dienstleister der öffentlichen Verwaltung unterstützt Dataport Kommunen dabei, ihre digitale Infrastruktur sicher, zukunftsfähig und digital souverän zu gestalten. Das Angebot reicht von modernen Sicherheitslösungen über Notfallvorsorge bis hin zu umfassenden Beratungsleistungen.

Dataport bietet sicheren IT-Betrieb

Dataport betreibt ein hochsicheres, redundantes und energieeffizientes Rechenzentrum - eines der sichersten in ganz Europa. Durch regelmäßige Zertifizierungen, unter anderem durch das BSI und durch TÜViT, belegt Dataport den jeweils aktuellen Sicherheitsstand.

Moderne Firewalls, Virenschutz und E-Mail-Security-Lösungen sorgen dafür, dass (potenzielle) Schadensfälle frühzeitig erkannt und abgewehrt werden. Dataport hat ein 10-Schichten Sicherheitsmodell im Rechenzentrum implementiert. Es ist mandantenfähig aufgebaut und eine eigens entwickelte Admin-Plattform sorgt dafür, dass administrative Zugriffe nur im erforderlichen Umfang genutzt werden können und nur auf die betroffenen Kunden begrenzt werden.

Ein so genanntes Security Operations Center (SOC) überwacht technikunterstützt die Systeme permanent und leitet im Ernstfall sofort die notwendigen Gegenmaßnahmen ein. Weitere Aufgabe ist die permanente Suche und Behebung von Schwachstellen und neuen Bedrohungen.

Regelmäßige Datensicherungen und schnelle Wiederherstellungsdienste sorgen dafür, dass wichtige Informationen auch nach einem Ausfall schnell wieder verfügbar sind. Interne Notfall- und Wiederanlaufpläne für den Fall der Fälle unterstützen für ein geordnetes und gezieltes Krisenmanagement.

IT-Sicherheit besteht nicht nur aus technischen Maßnahmen. Dataport verfügt daher über ein ganzheitliches IT-Sicherheitsmanagement gemäß den Vorgaben nach BSI-Grundschutz

Cloud Computing ist ein zentraler Baustein der Digitalisierung von Verwaltungen. Schon heute stehen zahlreiche Anwendungen und Dienste in der Cloud im Dataport-Rechenzentrum bereit – in den Standards und den geltenden und zertifizierten Regeln des Dataport-Rechenzentrums.

Stillstand ist Rückschritt in der IT – das gilt ganz besonders auch für alles rund um das Thema Informationssicherheit. Im Wettlauf mit neuen Sicherheitslücken und Bedrohungen entwickelt Dataport das Rechenzentrum und die Sicherheitsmaßnahmen permanent weiter um sie mindestens auf dem aktuellen Stand der Technik zu halten.

Dataport bietet Beratung, Schulung und Sensibilisierung

Dataport unterstützt Kommunen bei Bedarf auch mit Beratung, insbesondere in den Schwerpunkten:

- Unterstützung bei der Einführung der SiKoSH-Methodik (Sicherheit für Kommunen in Schleswig-Holstein).
- Beratung und Unterstützung bei der Einhaltung gesetzlicher Vorgaben (DSGVO, IT-Grundschutz)
- Unterstützung beim Aufbau eines Information Security Management System (ISMS). Ein ISMS ist ein systematischer, risikobasierter Ansatz zum Schutz sensibler Daten, der Regeln, Pro-

zesse und Verfahren festlegt. Es gewährleistet Vertraulichkeit, Integrität und Verfügbarkeit von Informationen,

- Bedrohungs- und Risikoanalyse: Die Identifizierung potenzieller Bedrohungen und Risiken für die IT-Infrastruktur und die Daten in Kommunen. Durchführung von so genannten Grundschutz-Checks sowie Erstellung von Sicherheitskonzepten zur Ergänzung des bestehenden ISMS.
- Technische Sicherheitsbewertungen: Überprüfung der aktuellen IT-Infrastruktur oder -Komponenten, inklusive der Sicherheitsrichtlinien und -verfahren sowie deren Regelkonformität (Compliance).
- Ergänzend: Durchführung von Sicherheitschecks, Penetrationstest und einschlägiger Audits.
- Unterstützung bei akuten Sicherheitsvorfällen: Notfallleistungen von der Analyse, über Schadensbegrenzung bis hin zur Wiederherstellung des Regelbetriebs.
- Mitarbeiterschulungen: Durchführung von Schulungen und Workshops rund um das Thema Sicherheit und Datenschutz.

Kontakt

Uwe Störmer
Dataport | Abteilungsleitung Kommunale Infrastruktur

uwe.stoermer@dataport-kommunal.de

Altenholzer Straße 10-14, 24161 Altenholz

Mit den drei vorliegenden Beiträgen entsteht ein umfassendes Gesamtbild kommunaler Digitalisierung im Jahr 2026. Der erste Beitrag beschreibt die rechtlichen, organisatorischen und strategischen Rahmenbedingungen, die mit dem Portalverbund und den föderalen Architekturvorgaben gesetzt sind. Darauf aufbauend analysiert der Artikel „Onlinedienst aber sicher", welche praktischen Risiken und Herausforderungen sich aus der zunehmenden Vernetzung der IT-Systeme ergeben und welche Unterstützungsangebote den Kommunen bei ihrer Bewältigung zur Verfügung stehen. Der abschließende Beitrag erweitert diese Perspektive durch eine tiefgehende Betrachtung der technischen und sicherheitsrelevanten Infrastrukturen, die notwendig sind, um die kommunale Handlungsfähigkeit auch bei ernsthaften Cybervorfällen aufrechtzuerhalten.

Zusammengenommen zeigen die drei Artikel, dass Digitalisierung, Informationssicherheit und Resilienz in der kommunalen Verwaltung keine getrennten Themenbereiche mehr sind. Sie bilden ein integriertes Aufgabenfeld, in dem rechtliche Vorgaben, technische Standards, organisatorische Maßnahmen und professionelle IT-Dienstleistungen eng ineinandergreifen müssen. Für Kommunen bedeutet dies einen klaren Auftrag: die digitale Transformation aktiv zu gestalten, Risiken methodisch zu beherrschen und Sicherheit als dauerhaften Prozess zu verstehen. Gleichzeitig wird sichtbar, wie vielfältig die Unterstützungsmöglichkeiten durch Land, ITV.SH, Dataport und CERT-Nord mittlerweile sind – und dass diese Infrastruktur den Kommunen ermöglicht, die Herausforderungen der digitalen Zukunft kompetent und verantwortungsbewusst zu bewältigen.

Impressum

Herausgeber

IT-Verbund Schleswig-Holstein AöR (ITV.SH)

Deliusstraße 10

24114 Kiel

Stand

März 2026