

2/2025



**Liebe Leserinnen und Leser,
liebe Kreistagsabgeordnete,**

Auf Bundesebene wurde nicht nur über eine Grundgesetzänderung der Weg frei gemacht für ein Sondervermögen für Investitionen in die Infrastruktur, sondern mittlerweile liegt auch ein Koalitionsvertrag vor. An den auf Schleswig-Holstein entfallenden Mitteln aus dem Sondervermögen des Bundes müssen die schleswig-holsteinischen Kommunen entsprechend ihres Anteils an der Infrastruktur beteiligt werden. Dies hat die Mitgliederversammlung am 28. März bekräftigt (siehe dazu nachfolgenden Beitrag).

Neben dem Sondervermögen besteht eine Möglichkeit der Länder zu weiterer Verschuldung. Wie auch auf Bundesebene darf die erleichterte Aufnahme von Krediten aber nicht dazu führen, dass strukturelle Maßnahmen zur Haushaltkskonsolidierung nicht weiterverfolgt werden: Aufgabekritik, Aufgabenreduktion, Verschlankung von Prozessen, Abbau von Doppelzuständigkeiten sowie die Entbürokratisierung, z. B. von Förderverfahren, müssen konsequent in den Blick genommen werden. Soweit zusätzlicher Spielraum entsteht, müssen die Kommunen im Land hinreichend daran partizipieren. Entbürokratisierung und die Beschleunigung von Planungsprozessen sind zudem erforderlich, um die zusätzlichen finanziellen Mittel auch schnell und nachhaltig im wahrsten Sinne des Wortes „auf die Straße zu bekommen.“

Der Koalitionsvertrag auf Bundesebene enthält aus Sicht der Kreise in Schleswig-Holstein einiges Positives (so im Bereich der Migration, im Sozial- und Gesundheitsbereich), ansonsten aber wenig Belastbares aus kommunaler Perspektive: Das zentrale Problem der offenkundig dramatischen Unterfinanzierung der Kreise, Städte und Gemeinden wird nicht gelöst. Auf die zentralen kommunalen Anliegen einer signifikanten Verbesserung der kommunalen Steuerbeteiligung und der Fokussierung steuerfinanzierter Sozialleistungen wird kaum eingegangen.

An einem Punkt können die Pläne der neuen Bundesregierung aber auch Impuls für Schleswig-Holstein sein: So haben die Kommunalen Landesverbände schon zum Landeshaushalt 2025 eigene Einsparvorschläge formuliert und das Land u. a. aufgefordert, bei eigenen Aufgaben zu sparen. Der Vorschlag, den Personalbestand des Landes um 1,5 Prozent zu reduzieren, liegt noch deutlich unter dem, was sich der Bund mit einer Reduktion um jährlich 2 Prozent vorgenommen hat. Übertragen auf Schleswig-Holstein würde dies, lässt man die Bereiche Bildung, Justiz und Polizei außen vor, eine Reduktion um ca. 250 Stellen pro Jahr (in Summe 1.000 Beschäftigte) und damit eine Ersparnis von 25 Mio. Euro p. a. (bzw. nach vier Jahren von 100 Mio. Euro p. a.) bedeuten. Wir erwarten von der Landesregierung, dass sie ebenfalls mindestens einen so ambitionierten Kurs verfolgt. Anders als auf Bundesebene, wo ein weiteres Ministerium geschaffen wurde, wäre auch die Reduktion von Ministerien und Landesbehörden ein richtiges Signal. Auch der Abbau von Beauftragten, die Reduktion der personellen und sachlichen Ausstattung der Beauftragten bzw. die Rückführung auf deren Kernaufgaben (Beispiel: Datenschutzaufsicht) kann beispielgebend sein. Nicht nur Anzahl und Ausstattung der Landesbeauftragten, sondern auch die kommunalen Verpflichtungen zur Bestellung von Beauftragten für eine Vielzahl von Themen müssen auf den Prüfstand.

Die Kommunalen Landesverbände werden die Landesregierung trotz neuer finanzieller Spielräume nicht aus der Pflicht entlassen, Einsparungen vorzunehmen und so eine auskömmliche Finanzierung der Kommunen sichern zu können. Für die Bundesebene gilt zu Recht, wie zutreffend von einem Kommentar in der Bild-Zeitung beschrieben: „Die Wahrheit ist auf dem Platz.“ Es bleibt also abzuwarten, welche Vorschläge wann und wie umgesetzt werden.

Herzlichst Ihr

Dr. Sönke E. Schulz

Inhalt

Editorial	1
Sondervermögen trifft auf IT-Sicherheit	2
Die Einfallstore sind weit offen . .	3
Taskforce Zivile Verteidigung . .	4
Termine	5

SONDERVERMÖGEN TRIFFT AUF IT-SICHERHEIT

Zwei auf den ersten Blick sehr unterschiedliche Themen - und doch beschäftigten sie die Delegierten der Mitgliederversammlung des Landkreistages bei ihrer ersten Sitzung des Jahres im Kreishaus in Bad Oldesloe intensiv.

KOMMUNEN FORDERN FAIREN ANTEIL AM SONDERVERMÖGEN

Mit Blick auf das Sondervermögen des Bundes fordern die Kommunen, dass 75 Prozent der Infrastrukturmittel an sie fließen. Begründet wird dies mit ihrer zentralen Rolle für die Daseinsvorsorge - insbesondere in den Bereichen Straßen, Schulen, frühkindliche Bildung, Verwaltungsgebäude, Digitalisierung, Energienetze und öffentlicher Nahverkehr.

Die Kernforderungen der Kommunen lauten:

- eine faire Verteilung der Mittel, basierend auf dem tatsächlichen Investitionsbedarf,
- pauschale Zuweisungen statt bürokratischer Förderprogramme, da die Kommunen ihre Bedarfe selbst am besten kennen,
- keine zusätzlichen Zweckbindungen oder gesetzliche Kofinanzierungspflichten,
- sowie eine Beteiligung an weiteren finanziellen Spielräumen des Landes - über das Sondervermögen hinaus.

Gleichzeitig fordern die Delegierten, dass das Land strukturelle Haushaltsreformen konsequent fortsetzt, insbesondere durch Entbürokratisierung, Aufgabenreduktion und den Abbau von Doppelstrukturen. Kritik gab es an einseitigen Einsparungen zugunsten der Kommunen - etwa durch Kürzungen beim ÖPNV oder Eingriffe in den kommunalen Finanzausgleich. (Die ausführliche Pressemitteilung finden Sie [hier](#).)

IT-SICHERHEIT: WENN PLÖTZLICH NICHTS MEHR GEHT

Das eigentliche Schwerpunktthema der Sitzung war jedoch ein anderes - die IT-Sicherheit in der öffentlichen Verwaltung. Was passiert, wenn plötzlich gar nichts mehr funktioniert? Ein Cyberangriff kann die gesamte digitale Infrastruktur lahmlegen - mit schwerwiegenden Folgen: Leistungen können nicht mehr ausgezahlt werden, Verwaltungsvorgänge wie Fahrzeugzulassungen oder Passanträge kommen zum Erliegen. Was zunächst "nur" ärgerlich erscheint, kann schnell existenziell werden - insbesondere, wenn auch sensible Daten gestohlen werden.

Wie gut sind unsere Verwaltungen auf ein solches Szenario vorbereitet?

Die Delegierten widmeten sich dieser Frage intensiv. Ziel war es, Sensibilität und Wissen zum Thema zu stärken - unterstützt durch drei Gastbeiträge.

Dr. Astrid Schumacher, Leiterin des Fachbereichs Umsetzungsberatung - Länder und Kommunen beim Bundesamt für Sicherheit in der Informationstechnik (BSI), führte in das Thema ein. Sie machte die akute Bedrohungslage deutlich, wies auf niedrigschwellige Unterstützungsangebote des BSI hin und warb eindringlich für die Einführung der sogenannten Basis-Absicherung in den Verwaltungen.

Im Anschluss berichtete Melitta Kühnlein aus erster Hand über den Cyberangriff auf die Stadt Potsdam im Jahr 2022. Sie zeigte eindrucksvoll, welche Herausforderungen mit einem solchen Vorfall verbunden sind - und welche Faktoren ein erfolgreiches Krisenmanagement ausmachen: Kommunikation, klare Strukturen, Transparenz, sorgfältige Dokumentation und ein kompetentes IT-Team. Die Stadt Potsdam war fast drei Monate "vom Netz" und die Kosten des Vorfalls beliefen sich auf rund zwei Millionen Euro.

Um den Kommunen in Schleswig-Holstein solche Erfahrungen zu ersparen, stellte der Geschäftsführer des ITV.SH (IT-Verbund Schleswig-Holstein) Matthi Bolte-Richter, die Angebote des Verbundes vor, die präventiv - etwa durch Trainings, Netzwerke und die Bereitstellung von Dienstleistungen, zum Beispiel über Rahmenverträge für Sicherheitshardware Kommunen bei der Entwicklung und Optimierung ihrer IT-Sicherheit unterstützen.

Zum Abschluss wurde sehr eindrucksvoll vor Augen geführt, wie leicht man selbst Opfer eines Cyberangriffs werden kann: In Kooperation mit einer darauf spezialisierten Firma (mehr Infos dazu im folgenden Beitrag) wurde ein Phishing-Angriff simuliert. Alle Delegierten erhielten eine täuschend echt aussehende, gefälschte E-Mail. Das Ergebnis: 33 Prozent klickten auf den Link - ein alarmierendes Zeichen dafür, wie angreifbar wir alle im digitalen Alltag sind.



DIE EINFALLSTORE SIND WEIT OFFEN

DR. WERNER DEGENHARDT, HUMAN FACTORS SPEZIALIST BEI CODE AND CONCEPT

„Ein IT-System ohne Nutzer ist sinnlos, ein IT-System mit Nutzern ist gefährlich“, sagt man. Und es stimmt, wie man täglich den Medien entnehmen kann. Das „**Signal-Gate**“ der Trump-Administration, der Versuch bei der **Agentur für Arbeit Arbeitslosengelder** abzufischen, jeden Tag gibt es neue Nachrichten zu Sicherheitslücken, die man sich vorher so nicht vorstellen konnte. Man kann dabei zusehen, wie sich die Angriffsfläche von Unternehmen und Personen vergrößert.

Das Angriffsflächenmanagement (ASM - Attack Surface Management) unterscheidet:

1. die **Physische Angriffsfläche** (das sind Angriffe auf die Hardware und die Datenübertragung),
2. die **Digitale Angriffsfläche** (das sind Angriffe auf Schwachstellen in Software und Protokollen, in Konfigurationen und vieles mehr)
3. und die **Angriffsfläche für Social Engineering**, die Bediener dazu bringt Dinge zu tun, die nicht in ihrem Interesse und dem Interesse ihres Arbeitgebers sind.

Die Angriffsfläche für Social Engineering ist - aus Sicht der Angreifer - das erfolgversprechendste Ziel. Denn Fakt ist: 95 Prozent aller Cyberangriffe verdanken ihren Erfolg der Mithilfe von Bedienern. Das sind

- Entwickler, die Funktionalität und Benutzerfreundlichkeit priorisieren, aber nicht die Sicherheit.
- Systemadministratoren, die Software und Geräte nicht ausreichend sicher konfigurieren.
- Sachbearbeiter, die bei ihrer Arbeit Anforderungen von Informationssicherheit und Datenschutz nicht angemessen berücksichtigen
- Bürger, die sich wie im Bürgerbüro in Sicherheit wähnen und mit der Benutzerschnittstelle ohne die gebotene Umsicht und Vorsicht arbeiten und dadurch zum Einfallstor für den nächsten Rathaus-Hack werden.

Vor allem Sachbearbeiter und Bürger geraten mit dem Fortschreiten der Digitalisierung in ungewohnte und gefahrgeneigte Situationen.



Im Bürgerbüro kommunizieren geschulte Sachbearbeiterinnen und Sachbearbeiter in einer geschützten Umgebung mit durch den direkten und persönlichen Kontakt sicher authentisierten und autorisierten Bürgerinnen und Bürgern. Das ist etwas vollkommen anderes als die Nutzung derselben Daten über eine Online-Schnittstelle durch einen entfernten Benutzer, der keine Ahnung hat, was sich hinter der Benutzerschnittstelle an technischen Vorgängen verbirgt oder auch ein Hacker sein kann, der die Sachbearbeitung hinter Licht führt.

Die Angriffsfläche für Social Engineering - die Human Firewall - muss proaktiv verkleinert werden, Informationssicheres Verhalten muss geschult werden. Das SOC (security operations center) muss um ein SLC (security learning center) ergänzt werden. Zur Grundausrüstung eines SLC gehören Mitarbeiterinnen und Mitarbeiter oder Dienstleister, die sich mit dem menschlichen Faktor in der Informationssicherheit auskennen und eine Schulungsplattform, die Daten über den Sicherheitsstand der Bediener nicht in der Cloud speichert.

Es tritt sonst genau das ein, was **Kevin Mitnick**, der berüchtigte und berühmte Sozialingenieur nach seiner Entlassung aus dem Gefängnis 2005 in einer Senatsanhörung sagte: "Ein Unternehmen kann hunderttausende Dollar für Firewalls, Intrusion-Detection Systeme, Verschlüsselung und andere Sicherheitstechnologien ausgeben, aber wenn der Hacker einen Bediener findet, der ihm wissentlich oder unwissentlich Zugang verschafft, dann ist der Aufwand vergebens gewesen und das Geld verschwendet."

Das zeigt, dass zusätzlich zum technischen Angriffsflächenmanagement durch CERT und SOC ein Security Learning Center (SLC) zum Management der Angriffssoberfläche für Social Engineering aufgebaut werden muss. Sensibilisierung, Training und Schulung sind effizient und nachhaltig, wenn einige grundlegende Hinweise beachtet werden:

1. Lerninhalte und Training müssen für die Bediener relevant sein. Unterschiedliche Rollen haben unterschiedlichen Bedarf
2. Das Training muss Spaß machen. "Gamification" als Teil des "active learning" ist nicht von ungefähr ein Schlagwort das viele Schulungsangebote begleitet.
3. Das Training muss häufig wiederholt und variiert werden, um sichere Reflexe auszubilden.
4. Das Schulungskonzept und die didaktische Aufbereitung der Inhalte müssen zur speziellen Organisationskultur der Einrichtung passen.
5. Denken Sie wie ein Human Factors Spezialist und lassen sie sich von Experten auf dem Gebiet der Erwachsenenbildung und Verhaltensänderung beraten. Es gibt Psychologen und Pädagogen, die sich auskennen.
6. Pflegen Sie den "security mindset". Was immer Sie tun, denken sie darüber nach, wie man Ihre Prozesse aushebeln und Schnittstellen missbrauchen könnte.
7. Machen Sie das SLC zur Informationsdrehscheibe für Sicherheit. Sensibilisierung, Training und Schulung sind eine Daueraufgabe.



Quelle: Tim Radtke, Innenministerium

ZUSAMMENFASSUNG DER PRESSEMITTEILUNG:

LANDESREGIERUNG BESCHLIESST EINSETZUNG DER TASKFORCE ZIVILE VERTEIDIGUNG - MINISTERPRÄSIDENT DANIEL GÜNTHER: „MIT DIESEM BREITEN BÜNDNIS STÄRKEN WIR UNSERE VERTEIDIGUNGSFÄHIGKEIT UND DEN SCHUTZ DER BÜRGERINNEN UND BÜRGER“

Am 1. April hat die Landesregierung Schleswig-Holsteins die **Taskforce Zivile Verteidigung** beschlossen - im Beisein von Vertretern der Bundeswehr. Ziel ist es, die zivile Verteidigungsfähigkeit im Land zu stärken. Die Taskforce setzt sich aus der Landesregierung, der Bundeswehr, der Polizei, dem Technischen Hilfswerk, den Kommunalen Landesverbänden, dem Feuerwehrverband, Hilfsorganisationen sowie der Industrie- und Handelskammer zusammen.

Ministerpräsident Daniel Günther betonte, dass der russische Angriffskrieg gegen die Ukraine und der unberechenbare Kurs der US-Regierung eine neue sicherheitspolitische Lage geschaffen hätten. Deutschland und Europa müssten mehr Verantwortung für ihre eigene Sicherheit übernehmen - auch im zivilen Bereich. Dazu gehöre die Vorbereitung auf hybride Bedrohungen wie Cyberangriffe und Sabotage.

Die Bundeswehr wird in Schleswig-Holstein beim sogenannten **Operationsplan Deutschland** unterstützt. Zivile Kräfte spielen dabei eine zentrale Rolle. Die vier Kernaufgaben der zivilen Verteidigung sind:

1. Die Aufrechterhaltung staatlicher und öffentlicher Strukturen (z. B. Polizei, Medien, Gesundheitswesen),
2. der Schutz der Bevölkerung,
3. die Versorgung mit Lebensmitteln, Wasser, Medizin und Verkehrsinfrastruktur,
4. sowie die Unterstützung der Streitkräfte.

Diese vier Hauptaufgaben werden eng abgestimmt mit dem Bund umgesetzt werden. Wichtig ist, dass nach den jüngsten Entscheidungen auf Bundesebene die künftig zur Verfügung stehenden finanziellen Mittel auch zügig in den Aufbau der Verteidigungsfähigkeit Deutschlands fließen. Die Umsetzung in Schleswig-Holstein wird die Taskforce vorbereiten.

Ein weiterer Beschluss betrifft die **Reservistinnen und Reservisten**: Künftig können sie bis zu fünf Arbeitstage pro Jahr für Bundeswehrübungen freigestellt werden – auch ohne Zustimmung der Arbeitgeber, analog zum Bildungsurlaub.

Für die Arbeitsgemeinschaft der kommunalen Landesverbände äußerte Dr. Sönke E. Schulz, Geschäftsführer des Schleswig-Holsteinischen Landkreistages: „Es ist nicht nur richtig, dass sich die Landesregierung für die Zivile Verteidigung neu aufstellt, sondern vor allem, dass dies unter Einbindung aller maßgeblichen Akteure im Land erfolgt. Die schleswig-holsteinischen Kommunen benötigen Planungssicherheit, die Bereitstellung von Informationen und werden sich gern aktiv einbringen sowie ihren Beitrag leisten, Schleswig-Holstein für kommende Herausforderungen krisensicher aufzustellen. Dabei kann auf viel Vorarbeit und Erfahrungen, zum Beispiel aus der Corona-Zeit und in der Rolle als Katastrophenbehörden, zurückgegriffen werden. Wichtig sind die richtigen Rahmenbedingungen, nicht nur, was die erforderlichen Ressourcen angeht. Auch hier bin ich zuversichtlich, dass wir schnell zu guten Lösungen kommen.“

Die ausführliche Pressemitteilung erhalten Sie [hier](#).

TERMINE

→ MAI

Di. 06.05. - 15.00

Bau- und Umweltausschuss 1/2025, Kiel

Di. 27.05. - 15.00

Finanzausschuss 1/2025, Kiel

Mi. 04.06. - 14.00

Landräterunde 3/2025, Ratzeburg

Mi./Do. 04./05.06.

Vorstand Klausurtagung Vorstand 3/2025, Ratzeburg

Alle Termine für 2025 finden Sie unter:

www.sh-landkreistag.de/aktuelles/termine/

Volle Power

für den Norden

Großer
Arbeitgeber



Attraktives
Gehalt



Starkes
Team



Komm ins
Team!

hansewerk.com/karriere



teil der
HanseWerk-
Gruppe

 Schleswig-Holstein
Netz