Landkreistag
BADEN-WÜRTTEMBERG

„Cybersicher zusammen – zusammen cybersicher?“

von Prof. Dr. Alexis von Komorowski
Hauptgeschäftsführer des Landkreistags Baden-Württemberg
aus Anlass des 2. Cybersicherheitstags

Sehr geehrte Damen und Herren,

sie hat es in sich gehabt, die Tour d’horizon, auf die uns der Vorstandsvorsitzende von Komm.ONE gerade mitgenom-men hat. Es ist nochmals sehr deutlich geworden, weshalb Cybersicherheit zu einem der ganz wichtigen Megatrends geworden ist. Megatrend verstanden als langanhaltende und systemverändernde Entwicklung mit globaler Ausprä-gung und einer Dauer von mehreren Jahrzehnten.

Auf diesen Megatrend will ich gerne zu Anfang noch einmal drei Schlaglichter werfen.

1. Schlaglicht: Die Cyberangriffe nehmen nicht nur zu, sie wachsen exponentiell an. Dies kommt nicht von ungefähr. Der wachsende Einfluss von künstlicher Intelligenz auf Cy-berangriffe ist bereits erwähnt worden. Zugleich machen die sich immer weiter ausdehnende Welt der IT, das Internet der Dinge sowie operative Technologien uns immer vul-nerabler. Man muss daher kein Prophet sein, um zu konsta-tieren, dass sich der Megatrend Cybersicherheit in Zukunft nur noch weiter verstärken wird. Oder um es etwas flapsi-ger zu formulieren: Das Thema Cybersicherheit ist gekom-men, um zu bleiben und immer bedeutsamer zu werden.

2. Schlaglicht: Eben weil Cyberangriffe exponentiell wach-sen, werden auch immer häufiger kommunale Verwaltun-gen davon betroffen. Einer der größten Angriffe auf die öf-fentliche Verwaltung, die es in Deutschland bisher gab, fand bekanntlich in Nordrhein-Westfalen statt. In der Nacht auf den 31. Oktober 2023 wurden auf den Servern der Südwestfalen-IT, die über

100 Kommunen betreut, Ransomware aufgespürt und bereits verschlüsselte Dateien gefunden. Die Cyberkriminellen der Gruppe Akira forderten Lösegeld.

Nun hatten wir in Baden-Württemberg zum Glück noch kei-nen Cyberangriff auf kommunale Verwaltungen, der in sei-nen Auswirkungen dem gegen die Südwestfalen-IT ver-gleichbar gewesen wäre. Aber wir alle wissen: Selbst in „The Länd" kann es uns über kurz oder lang massiv erwischen. Erste Vorboten gab es schon. Darüber wird ja heute auch berichtet werden. Und dass wir in Baden-Württemberg bis-her eher glimpflich davongekommen sind, ist keine Garantie für die Zukunft.

3. Schlaglicht: Kommunen geraten nicht nur deswegen im-mer mehr ins Zielfeld von Cyberangriffen, weil diese expo-nentiell anwachsen. Die Anfälligkeit gerade von Kommunen für Cyberangriffe hängt natürlich auch damit zusammen, dass die Landkreise, Städte und Gemeinden über einen veri-tablen Schatz an wertvollen, sensiblen Daten verfügen. Sen-sible, wertvolle Daten, die ihnen von ihren Bürgerinnen und Bürgern anvertraut worden sind. Adressen, Identifizierungs-informationen, Bankdaten. Ein echtes Eldorado für Cyber-kriminelle.

Meine sehr verehrten Damen und Herren,

was wollte ich mit diesen drei Schlaglichtern zum Ausdruck bringen? Eigentlich nur das, was wir alle wissen, was aber bei all den sonstigen Herausforderungen des Alltagsge-schäfts manchmal aus dem Blickfeld gerät: Der Megatrend Cybersicherheit ist eine epochale Herausforderung. Er for-dert die einzelnen Staaten und die Weltgemeinschaft, Un-ternehmen und Gesellschaft – aber eben auch jede der 1.101 Städte und Gemeinden und jeden der 35 Landkreise in Ba-den-Württemberg.

Damit sind wir mitten im Thema angelangt: Was bedeutet der Megatrend Cybersicherheit für die baden-württembergischen Kommunen. Lassen Sie mich dazu sie-ben Thesen mit Ihnen teilen.

1. These: Für ihre Cybersicherheit ist die Kommune selbst verantwortlich.

Dies mag auf den ersten Zuruf hin etwas hart klingen. Aber so ist nun einmal unsere Verfassungsordnung gestrickt. Selbstverwaltungsgarantie, Subsidiaritätsprinzip – all das, was die kommunale Ebene ausmacht und, wie ich meine, auch stark macht, führt unweigerlich zu dieser Konsequenz: Für ihre Sicherheit ist die Kommune zunächst selbst verant-wortlich.

Auch das Gesetzesrecht weist eindeutig in diese Richtung. Das Cybersicherheitsgesetz des Landes nimmt die Kommu-nen von seinem Anwendungsbereich aus – und die Land-ratsämter in ihrem staatsbehördlichen Aufgabenfeld gleich dazu.

Bund und Länder verfolgen hier eine gemeinsame Linie. Man verzichtet darauf, das Thema Cybersicherheit in Bezug auf die Kommunen gesetzlich zu regeln. Stattdessen will man die Kommunen anstoßen, anreizen, stupsen, selbst etwas zu machen. To nudge heißt das auf Englisch. Deswegen spricht man von Nudging. Nudging statt Regulierung. Das ist der An-satz von Bund und Land.

Beispielhaft dafür ist der im Dezember vergangenen Jahres vom Land initiierte Stufenplan für mehr Cybersicherheit bei Kommunen. Dieser Stufenplan ist, anders als man vermuten könnte, kein Aktionsplan des Landes, um durch eigene Cy-bersicherheitssicherheitsmaßnahmen die Informationssi-cherheit im kommunalen Bereich zu erhöhen. Vielmehr handelt es sich bei dem Stufenplan um ein Hilfsinstrument für die Kommunen, mit dem sie für sich klären können, wo Sicherheitslücken bestehen und wo sie zusätzliche Sicher-heitsmaßnahmen treffen können. Der vom Land bereitge-stellte Stufenplan ist also lediglich ein Werkzeug. Es anzu-wenden, obliegt den Kommunen. Wenn sie es tun, werden sie von der Cybersicherheitsagentur des Landes unterstützt. Nudging statt Regulierung.

Entsprechendes gilt für die Bundesebene. Das Bundesamt für Sicherheit in der Informationstechnik, kurz: BSI, stellt viel Hilfreiches zur Verfügung, macht auf der Homepage aber zugleich unmissverständlich klar: Beratung könnt ihr von uns nicht erwarten.

Wie man es dreht und wendet. Es bleibt dabei. Für ihre Cy-bersicherheit ist die Kommune selbst verantwortlich.

2. These: Kommunale Cybersicherheit ist Chefinnen- und Chefsache.

Der grundsätzliche Umgang mit einem Megatrend, mit einer epochalen Herausforderung lässt sich nicht delegieren. Da-her müssen die kommunalen Spitzen die abschließende Ge-samtverantwortung für den Sicherheitsprozess überneh-men. Die politische Verantwortung haben Sie ja ohnehin.

Dies bedeutet, dass sie den Sicherheitsprozess initiieren müssen, die Erstellung einer IT-Sicherheitsleitlinie voran-treiben müssen und für deren regelmäßige Fortschreibung sorgen müssen.

Klar ist, dass damit keine fachliche Verantwortung verbun-den ist. Es geht um die organisatorische Verantwortung und Verortung.

Dies ist zugegebenermaßen viel verlangt. Aber es entspricht nun einmal der Größe der Herausforderung.

Daher: Kommunale Cybersicherheit ist Chefinnen- und Chefsache.

3. These: Zur kommunalen Cybersicherheit gehört es, die Mitarbeitenden mitzunehmen.

In der Fachwelt wird durchaus heftig darüber gestritten, was für die Cybersicherheit wichtiger ist: die IT und ihre Schutz-vorkehrungen oder aber die – neudeutsch – Awareness, die Sensibilität der Mitarbeitenden für das Cybersicherheits-Thema.

Wir Kommunale tun uns naturgemäß schwer mit solchen ideologischen Glaubenskriegen. Wir sind pragmatisch un-terwegs. Und wenn es nun einmal so ist, dass 95 % der Cy-bersicherheitsverletzungen auf menschliches Versagen zu-rückzuführen sind, dann gibt es doch eine starke Anscheins-vermutung dafür, dass es durchaus sinnvoll ist, die Mitarbei-terinnen und Mitarbeiter konsequent mitzunehmen, ausrei-chend zu schulen und immer wieder zu sensibilisieren.

Vor diesem Hintergrund würde ich daran festhalten: Zur kommunalen Cybersicherheit gehört es, die Mitarbeitenden mitzunehmen.

4. These: Nicht jede Kommune braucht bspw. ein Umwelt-managementsystem, aber jede Kommune braucht zwingend ein Informationssicherheitsmanagementsystem.

Durch ein solches Informationssicherheitsmanagementsys-tem wird gewährleistet, dass die Anforderungen der IT-Sicherheit systematisch erfüllt werden. Es geht darum, durch verbindliche Anweisungen, definierte Verantwort-lichkeiten und konsequentes Monitoring die Informationssi-cherheit dauerhaft zu gewährleisten und fortlaufend zu op-timieren.

Dabei ist es durchaus legitim, das Informationssicherheits-managementsystem allmählich, step by step zu entwickeln. Entscheidend ist nur, am Ball zu bleiben und den Anschluss nicht zu verlieren.

Natürlich gibt es Vorbehalte gegen solche Systeme. So sind sie beispielsweise immer auch ein Stück weit bürokratiean-fällig. Und Lorbeeren kann man sich damit auch nicht ver-dienen. There is no glory in prevention. Dennoch halte ich an der These fest:

Nicht jede Kommune braucht ein Umweltmanagementsys-tem, aber jede Kommune braucht zwingend ein Informati-onssicherheitsmanagementsystem

5. These: Jede Kommune braucht einen Plan B in der Tasche.

Cyberangriffe können ganz schnell die gesamte kommunale Organisation lahmlegen. In diesen Fällen steht das staatliche Grundversprechen auf dem Spiel, jederzeit für Ordnung, Si-cherheit und funktionierende Daseinsvorsorge zu gewähr-leisten. Deshalb braucht es einen klaren Notfallplan, der die Funktionsfähigkeit der Kommune und die Ausfallsicherheit der zentralen Geschäftsprozesse auch in solchen Krisenfäl-len gewährleistet.

Dabei kann man ein solches Notfallmanagement durchaus aufwachsend entwickeln. Auch hier gilt: Entscheidend ist, am Ball zu bleiben und den Anschluss nicht zu verlieren.

Aber klar ist: Jede Kommune braucht einen Plan B in der Ta-sche.

6. These: Durch Kooperation werden wir resilienter.

Gerade das Beispiel des Notfallmanagements zeigt, dass sich Kooperationen im Bereich der Cybersicherheit vielfach re-gelrecht aufdrängen. Denn natürlich macht es außeror-dentlich viel Sinn, sich vorab mit anderen Kommunen für den Fall zu committen, dass man aufgrund eines Cyberan-griffs vom Netz gehen muss. Dann kann die andere Kommu-ne, wenn entsprechende Vorbereitungen getroffen wurden, den Notbetrieb für die ausfallende Kommune übernehmen.

Dies ist nicht nur kein Widerspruch zur These 1, wonach die Kommune für ihre Cybersicherheit selbst verantwortlich ist. Es ist im Gegenteil Ausdruck gerade dieser Verantwortlich-keit der Kommune für ihre Sicherheit, wenn sie durch Ko-operationen ihre Cybersicherheit optimiert und dadurch auf einem höheren Level gewährleistet.

Die Kooperationen können dabei unterschiedlichster Art sein. Besonders bedeutsam ist natürlich unser Kooperati-onsverbund Komm.ONE. Komm.ONE ist nicht nur, aber ge-rade auch in Fragen der Cybersicherheit die Mutter aller Ko-operationen.

Daneben werden wir freilich zukünftig mehr noch als heute auch über ortsnähere Formen interkommunaler Zusam-menarbeit nachzudenken haben. Und dann gibt es ja auch noch Kooperationsformate wie etwa die Initiative digitale Landkreiskonvois, kurz: INDILAKO, auf die ich als Vertreter des Landkreistags ein klein wenig stolz bin, weil sich hier ei-ne besonders agile Form der Zusammenarbeit herausgebil-det hat.

So vielfältig die Formen der Kooperation sind, eines scheint mir unbestreitbar zu sein: Durch Kooperation werden wir resilienter.

7. und letzte These: Das Land nicht aus der Verantwortung entlassen.

Natürlich muss ich zum Schluss auf die Verantwortung auch des Landes zu sprechen kommen. Andernfalls hätte ich meinen Job als Vertreter der kommunalen Landesverbände einigermaßen verfehlt.

Worin liegt also die Verantwortung des Landes?

Erstens muss die Landesregierung nun möglichst schnell ihre vor mehr als vier Jahren gegebene Zusage einlösen, nämlich einen Cybersicherheitspakt mit den Kommunen abzuschlie-ßen. Dort muss geregelt werden, wie die Cybersicherheits-architektur im Verhältnis zwischen Land und Kommunen ausgestaltet wird und insbesondere auch welche Rollen die Komm.ONE einerseits, die Cybersicherheitsagentur Baden-Württemberg andererseits, in diesem Gefüge dauerhaft, nachhaltig und verlässlich einnehmen sollen. Es wäre schön, wenn das Land den Langsamkeitsrekord, den es beim Ab-schluss der Digitalisierungsvereinbarung aktuell aufstellt, beim Cybersicherheitspakt nicht noch toppen würde.

Zweitens geht es natürlich auch um das liebe Geld. Cybersi-cherheit hat ihren Preis. Angesichts der dramatischen Fi-nanzlage der Kommunen stellt sich sehr ernsthaft die Frage, wie viele Landkreise, Städte und Gemeinden in der Lage sind, diesen Preis zu zahlen. Bei den aktuellen Finanzver-handlungen gewinnt man nicht den Eindruck, dass das Land die Dramatik der kommunalen Finanzlage erfasst hätte bzw. sich überhaupt damit auseinandersetzen wollte. Umso wichtiger ist es, das Land immer wieder auch auf das Delta zwischen den kommunalen

Herausforderungen im Bereich der Cybersicherheit und der kommunalen Finanzausstat-tung hinzuweisen und Lösungen einzufordern.

Daher kann ich die 7. und letzte These auch nur nochmals dick unterstreichen: Das Land nicht aus der Verantwortung entlassen.

Meine sehr verehrten Damen und Herren!

Beim Thema Cybersicherheit geht es für die Kommunen um viel.

Denn wir werden als Kommunen unsere Leistungsfähigkeit schon wegen des demographischen Wandels und des damit verbundenen Fach- und Arbeitskräfteverlusts nur dann er-halten können, wenn die digitale Transformation unserer Verwaltungen gelingt. Genau diese unverzichtbare digitale Transformation aber wird durch Cyberangriffe massiv be-droht. Cybersicherheit ist daher die Voraussetzung dafür, dass kommunale Selbstverwaltung, wie wir sie kennen, auch morgen und übermorgen noch funktioniert.

Sich dafür einzusetzen, lohnt sich: Cybersicher zusammen – zusammen cybersicher – mit Ausrufe- statt mit Fragezei-chen.

Ich will allerdings nicht schließen, ohne mich zu bedanken. Ich tue dies ausdrücklich auch im Namen von Gemeindetag und Städtetag, von Präsident Steffen Jäger und dem Ge-schäftsführenden Vorstandsmitglied Ralf Broß.

Bedanken will ich mit bei der Komm.ONE und stellvertre-tend bei Ihrem Vorstandsvorsitzenden, William Schmitt, für diesen 2. Cybersecurity-Tag. Wenn es den Cybersecurity-Tag nicht schon gäbe, müsste man ihn glatt erfinden.

Ihnen allen alles Gute und Glück auf!