Anwaltsverband Baden-Württemberg
im Deutschen **Anwalt**Verein e. V.

Anwaltsverband Baden-Württemberg – Postfach 1221 – 70808 Korntal-Münchingen

Ministerium für Inneres, Digitalisierung und Migration
Baden-Württemberg
Herrn Matthias Pröfrock
Herrn Dr. Alfred Debus
Postfach 10 34 65

70029 Stuttgart

Geschäftsstelle beim Präsidenten:
RA Prof. Dr. jur. Peter Kothe
Johannes-Daur-Straße 10
70825 Korntal-Münchingen

Telefon 0711 / 2 36 59 63
Telefax 0711 / 2 55 26 55

E-Mail: info@av-bw.de
Internet: www.av-bw.de

Anschrift der Geschäftsführung:
Kathrin Eisenmann – Syndikusrechtsanwältin
Daimlerstraße 25
70372 Stuttgart

Telefon 0711 / 55 04 29 29
Telefax 0711 / 55 04 29 30
E-Mail: eisenmann@av-bw.de

03. November 2020

Per E-Mail: poststelle@im.bwl.de und Alfred.Debus@im.bwl.de!

Az. 7-0271.0/8
Entwurf eines Gesetzes zur Verbesserung der Cybersicherheit und Änderung anderer Vorschriften (Cybersicherheitsgesetz – CSG)
- Stellungnahme des Anwaltsverbandes Baden-Württemberg im Deutschen AnwaltVerein e.V.

Sehr geehrter Herr Pröfrock,
sehr geehrter Herr Dr. Debus,
sehr geehrte Damen und Herren,

für die Übermittlung des Gesetzentwurfs zur Verbesserung der Cybersicherheit und Änderung anderer Vorschriften mit Schreiben vom 22.09.2020 danken wir Ihnen. Der Anwaltsverband nimmt die Gelegenheit zur Stellungnahme gern wahr.

Der Anwaltsverband Baden-Württemberg e. V. ist der freiwillige Zusammenschluss der 25 örtlichen Anwaltvereine in Baden-Württemberg, die Mitglied im Deutschen Anwaltverein (DAV) sind. Er repräsentiert damit mehr als die Hälfte aller Kolleginnen und Kollegen in Baden-Württemberg und vertritt so als größte freiwillige Anwaltsorganisation dieses Bundeslandes die Interessen der Anwaltschaft in unserem Bundesland und – in Zusammenarbeit mit dem DAV – auch auf nationaler und internationaler Ebene.

1. Allgemeine Bewertung

Der Anwaltsverband Baden- Württemberg hat Verständnis für das politische Anliegen, auf die fortschreitende Digitalisierung vieler Prozesse in der Landesverwaltung, der Wirtschaft, aber auch bei Verbraucherhandeln und damit auf deren Gefährdung durch digitale Angriffe, wie Schadsoftware o. ä. mit der Errichtung einer Cybersicherheitsagentur für Baden-Württemberg (bei einem ganzheitlichen Ansatz) zu reagieren. Er erkennt dabei – wegen des Ziels, sich jeweils ein Lagebild in diesem Bereich zu verschaffen – Ähnlichkeiten zum Landesverfassungsschutz, aber hinsichtlich der geplanten Beratungs- und Prüfaufgaben zum Bundesamt für Sicherheit in der Informationstechnik (BSI). Aufgrund der beabsichtigten Befugnisse kommt der geplanten Cybersicherheitsagentur auch der Charakter einer speziellen Polizeibehörde zu, die sowohl präventiv zur Gefahrenabwehr, aber auch repressiv ermittelnd im strafrechtlichen Sinn tätig werden soll. Dies wird letztlich auch durch die Einbindung in den Geschäftsbereich des Innenministeriums sowie die besoldungsrechtliche Einstufung des zukünftigen Behördenleiters (Präsidenten) ähnlich einem Polizeipräsidenten zum Ausdruck gebracht. Die Befugnisse der geplanten Cybersicherheitsagentur würden also weit mehr umfassen als beispielsweise die des BSI.

Der Anwaltsverband ist deswegen skeptisch, ob eine klare Aufgabentrennung zu den Zuständigkeitsbereichen anderer Einrichtungen, etwa dem LfV, der BITBW oder dem BSI, gelingen kann. So betreibt beispielsweise schon das BSI die Entwicklung von Standards und Sicherheitsvorkehrungen und bietet Information und Beratung für Unternehmen und Verbraucher an.

Es ist richtig, eine primäre Zuständigkeit für Landesbehörden und ihnen nachgeordnete öffentliche Stellen vorzusehen, aber die gewonnen Erkenntnisse auch Unternehmen und Privatpersonen zur Verfügung zu stellen. So kann ein Mehrwert der für die Aufgabenerfüllung eingesetzten Steuermittel generiert werden.

Die explizite Berücksichtigung der verfassungsrechtlich oder einfachgesetzlich garantierten Unabhängigkeit weiterer öffentlicher Stellen als „Sonderstatus“ (§ 2 Abs. 2 CSG-E) wird seitens unseres Verbandes ausdrücklich begrüßt.

In der Gesetzesbegründung wird für den Laien zu viel fachspezifisches Wissen vorausgesetzt. So wäre es wünschenswert, die jeweils beteiligten Kreise, wie IT-Rat BW[1], BIT BW (Landesoberbehörde IT Baden-

[1] Der IT-Rat Baden-Württemberg setzt sich zusammen aus dem CIO (Beauftragter der Landesregierung für Informationstechnologie) als Vorsitzendem, den Amtschefinnen und Amtschefs der Ministerien sowie weiteren beratenden Mitgliedern. Er ist damit ressortübergreifend.

Württemberg im Geschäftsbereich des Innenministeriums), AK-IT[2], KG InfoSic[3], IT-Planungsrat[4] oder KoSt KRITIS[5], deren Zusammensetzung und Kompetenzen, kurz zu erläutern, damit der Bürger erkennen kann, wozu deren Stellung hier jeweils hilfreich sein kann. Die Begründung eines Gesetzes soll nicht lediglich den mit der Materie in der Regel vertrauten Abgeordneten des Landtages Sinn und Zweck der Normen erschließen, sondern auch dem Bürger die nötige Transparenz vermitteln und so die Akzeptanz erhöhen. Überdies ist nicht auszuschließen, dass sich Zusammensetzung und Kompetenzen der in Bezug genommenen Gremien/Institutionen im Laufe der Zeit ändern, so wie das z. B. beim IT-Planungsrat geschehen ist. Dann sollten sich aber auch mögliche Auswirkungen auf die Arbeit der Cybersicherheitsagentur bzw. den hiesigen Gesetzestext erkennen lassen.

Angesichts des ehrgeizigen Zeitplans für den Aufbau der Cybersicherheitsagentur noch in 2020 bzw. 2021 fragt der Anwaltsverband, ob überhaupt ausreichend Fachkräfte zur Verfügung stehen.

Der Anwaltsverband bemängelt, dass für die in § 5 CSG BW-neu geregelten Befugnisse der Cybersicherheitsagentur im Rahmen der Gefahrenabwehr – abgesehen von der Datenerhebung und -verarbeitung - in der Gesetzesbegründung keinerlei Beispiele genannt sind, an welche Anordnungen und Maßnahmen hier gedacht wird. Zwar ist das Verfahren mit Fristsetzung und Verhältnismäßigkeitsanforderungen näher beschrieben, aber nicht, was die Betroffenen erwarten könnte. § 7 CSG BW-neu spricht von Untersuchungsmöglichkeiten, aber kann die Gefahrenabwehr z. B. auch darin bestehen, dass eine Stelle geschlossen wird, um möglicherweise andere verbundene Stellen nicht zu infizieren?

Nachdem es nun schon einige Jahre Erfahrungen mit empfehlenswerten Maßnahmen gibt, z. B. seitens des BSI, kann erwartet werden, dass solche Maßnahmen auch beispielhaft in der Gesetzesbegründung aufgeführt werden.

2. Im Einzelnen

a) Zu § 2 CSG-E

Es erscheint kaum zielführend, im Rahmen der Begriffsbestimmungen mit Pleonasmen zu arbeiten. Nach § 2 Abs. 1 Satz 1 CSG-E ist unter einer öffentlichen Stelle eine Stelle zu verstehen, die einer

---

[2] Arbeitskreis Informationstechnik des IT-Rates Baden-Württemberg
[3] Koordinierungsgruppe Informationssicherheit des Landes Baden-Württemberg
[4] Der IT-Planungsrat ist das zentrale Gremium für die förderale Zusammenarbeit in der Informationstechnik. Der Vorsitz im IT-Planungsrat wechselt seit 2010 jährlich zwischen Bund und Ländern, wobei die Länder in alphabetischer Reihenfolge den Vorsitz übernehmen.
[5] Koordinierungsstelle kritische Infrastrukturen beim Innenministerium BW

bestimmten Gebietskörperschaft angehört oder unter der Aufsicht des Landes steht. Auch natürliche oder juristische Personen des Privatrechts sollen – die Wahrnehmung bestimmter Aufgaben vorausgesetzt hierunter fallen.

Der Begriff „Stelle" wird bei genauer Betrachtung gerade nicht definiert. Während etwa der Behördenbegriff in § 1 Abs. 2 LVwVfG durch die Aufgabenwahrnehmung der dort genannten Stelle konkretisiert wird, bedient sich der vorliegende Entwurf eines Pleonasmus. Dies ist nicht nur unbefriedigend, sondern birgt auch das Risiko von Missverständnisses. Wenn natürliche Personen – mithin Einzelpersonen – unter bestimmten Voraussetzungen als „Stelle" anzusehen sein sollen, stellt die Frage, ob auch einzelne Behördenbedienstete „öffentliche Stelle" in diesem Sinn sein können. Vorzugswürdig erscheint es deshalb, den Begriff der Stelle genauer zu definieren. Zu denken ist etwa an eine Organisationseinheit. Eine solche kann im privatrechtlichen Bereich durchaus durch eine Einzelperson verkörpert werden, während es im öffentlich-rechtlichen Bereich sicherlich einer organisatorischen Einheit innerhalb des hierarchischen Aufbaus bedarf, um die angesprochenen Aufgaben wahrnehmen zu können.

Überdies fällt auf, dass an Gebietskörperschaften, denen die „öffentlichen Stellen" zugeordnet oder angehören sollen, nur das Land sowie Gemeinden und Gemeindeverbände genannt sind. Zu fragen ist deshalb, weshalb Landkreise und Verbände wie etwa der Verband Region Stuttgart u. Ä. oder sonstige Zusammenschlüsse wie Zweckverbände o. Ä. nicht erwähnt werden. Es bedarf wohl keiner Vertiefung, dass auch diese vornehmlich Aufgaben der Daseinsvorsorge wahrnehmen. Weshalb ihnen ein Sonderstatus gemäß § 2 Abs. 2 Nr. 8 CSG-E zuzubilligen sein sollte, erschließt sich nicht, zumal es sich insoweit wohl nicht um Stellen des Landes i. S. der Gesetzesbegründung handelt.

b) Zu § 3 CSG-E - Aufgaben

Zu den Aufgaben der Cybersicherheitsagentur soll – ausweislich der Gesetzesbegründung – u. a. die Einflussnahme auf die Entwicklung von Sicherheitsvorkehrungen und Prüfwerkzeugen gehören. Aber auch die Entwicklung von kryptologischen und mathematischen Sicherungsverfahren, Kryptogeräten und -komponenten, Authentifizierungsverfahren und Zugriffskontrollverfahren soll die Cybersicherheitsagentur vorantreiben. Soweit Endprodukte dann von Unternehmen kommerziell vertrieben werden, sollen diese dafür an den Entwicklungskosten beteiligt werden.

Hier stellt sich die Frage, ob der Staat sich hier in nicht zulässiger Weise wirtschaftlich betätigen will. Politische Ziele lassen sich vielfach (direkter) über die regulative Ausgestaltung der Rahmenbedingungen und die Überwachung ihrer Einhaltung erreichen. Aus der wirtschaftlichen Tätigkeit des Staates können sich Wettbewerbsverzerrungen zu Lasten Privater ergeben. Ein Grund ist, dass

staatliche Stellen weniger stark als private Unternehmen dem Druck der Kapitalmärkte ausgesetzt sind. Infolgedessen können effizientere und innovativere Wettbewerber aus dem Markt ausscheiden.

Staatliche Wirtschaftstätigkeit kann für die Bürger/Verbraucher mit unmittelbaren Kosten verbunden sein. Im Vergleich zu Privaten unterliegen öffentliche Stellen oftmals geringeren Anreizen für effizientes Wirtschaften und beziehen bisweilen haushaltspolitische Erwägungen in ihre Entscheidungen ein. Gerade auf Monopolmärkten – wie hier einer entstehen würde - kann dies zu überhöhten Endkundenpreisen führen.

Die in der Begründung des Gesetzentwurfs vorgenommene Begrenzung etwa „auf Grundmuster oder Prototypen", während „die industrielle Entwicklung und Serienfertigung … allein der Wirtschaft" zugewiesen werden soll, findet sich so nicht im Gesetzeswortlaut. Die vermeintlich einschränkende Begründung wird sogleich wieder aufgeweicht, wenn es dort (S. 44) heißt:

> „Zu entwickeln und weiterzuentwickeln sind insbesondere kryptologische und mathematische Sicherungsverfahren, Kryptogeräte und -komponenten, Authentisierungsverfahren – etwa zur ‚digitalen Unterschrift' – Zugriffskontrollverfahren und Vorkehrungen zur Unterbindung der kompromittierenden Abstrahlung bei Geräten. Soweit Endprodukte mit informationstechnischen Sicherheitsvorkehrungen der Cybersicherheitsagentur kommerziell vertrieben werden dürfen, … hat die herstellende Person der Endprodukte die bei der Cybersicherheitsagentur angefallenen Entwicklungskosten aufgrund vertraglicher Vereinbarung zu erstatten."

Aus der Doppelrolle des Staates als Marktteilnehmer und Hoheitsträger ergibt sich ein erhöhtes Diskriminierungspotential gegenüber privaten Wettbewerbern. Aus den genannten Gründen ist es von entscheidender Bedeutung, dass die unternehmerische Tätigkeit des Staates, soweit möglich, im Wettbewerb erbracht wird.

Die wirtschaftliche Betätigung des Staates sollte dort, wo auch private Unternehmen Leistungen erbringen können, stets hinterfragt werden. Sie bedarf der besonderen Rechtfertigung. In den Entscheidungsprozessen über die wirtschaftliche Betätigung des Staates sollte der Gedanke der Subsidiarität stärker Berücksichtigung finden. Wenn die öffentliche Hand wirtschaftlich tätig wird, sollte sie ihre Beweggründe und die mit der wirtschaftlichen Betätigung verbundenen Vor- und Nachteile vor den Entscheidungen transparent und einer unabhängigen Überprüfung zugänglich machen.

Diese vorstehenden Ausführungen gelten auch für den Bereich der Zertifizierungen.

c) Zu § 4 CSG-E - Zentrale Koordinierungs- und Meldestelle

Dass die geplante Cybersicherheitsagentur die Aufgaben der zentralen Kontaktstelle übernimmt, entspricht § 8b BSIG.

Mit der eingeführten Meldepflicht (ab 01.01.2022) sollten gleichwertige Informationsrechte der Meldepflichtigen korrespondieren. Wenn sie schon so in die Pflicht genommen werden, sollten sie auch von den dadurch gewonnen Erkenntnissen unmittelbar und zeitnah profitieren können.

d) Zu § 5 CSG-E – Gefahrenabwehr

Die Eingriffsbefugnisse sollen offenbar bewusst hinter denen der Polizei (§ 3 PolG) oder der Sonderordnungsbehörden (vgl. etwa § 47 Abs. 1 Satz 2 LBO) zurückbleiben. Dies dürfte dem Umstand geschuldet sein, dass die Cybersicherheitsagentur gegenüber anderen öffentlichen Stellen tätig werden soll. Gleichwohl wirft die Formulierung Fragen auf:

Vermisst wird die in den sonstigen Eingriffsbefugnissen enthaltene Vorgabe des pflichtgemäß auszuübenden Ermessens.

Die vorherige Fristsetzung erinnert an die Verwaltungsvollstreckung, nämlich an die Androhung einer Vollstreckungsmaßnahme; sie ist nämlich nicht wie eine Anhörung i. S des § 28 LVwVfG formuliert.

Einerseits wird der Cybersicherheitsagentur die Befugnis eingeräumt, „die erforderlichen Anordnungen treffen und Maßnahmen“ zu ergreifen. Andererseits darf sie „Anordnungen treffen oder Maßnahmen vornehmen“ „nur im Einvernehmen mit der jeweils fachlich zuständigen obersten Landesbehörde oder im Einzelfall aufgrund Beschlusses des IT-Rates Baden-Württemberg“, und zwar auch dies nur nach vorheriger Fristsetzung. Dies erscheint zum einen kompliziert, zum anderen stellt sich die Frage, ob mit der Fristsetzung bereits die Erteilung des Einvernehmens für den Fall des fruchtlosen Verstreichens dieser Frist beantragt werden kann.

„Wenn zur Gefahrenabwehr sofortiges Handeln erforderlich ist“ – wenn also, polizeirechtlich gesprochen, Gefahr im Verzug ist -, soll die Präsidentin oder der Präsidenten der Cybersicherheitsagentur anordnen können, dass von der Einholung des Einvernehmens abgesehen werden kann. Nicht geklärt ist damit streng genommen, wer die Feststellung triff, ob sofortiges Handeln erforderlich ist. Vor allem vermissen wir eine Vertretungsregelung für den Fall, dass die Präsidentin oder der Präsident der Cybersicherheitsagentur nicht erreichbar ist. Die oder der Vertreter(in) im Amt wird nicht erwähnt; eine Delegationsmöglichkeit ist nicht vorgesehen.

Unklar ist, ob unterschiedliche Stellen gemeint sind, wenn einerseits von „der jeweils fachlich zuständigen obersten Landesbehörde“ gesprochen, deren vorherigen Einvernehmens etwaige Anordnungen und Maßnahmen bedürfen, andererseits aber von „der betroffenen obersten Landesbehörde“ die Rede ist, der die zu protokollierende Entscheidung über die Notwendigkeit sofortigen Handelns mitzuteilen ist.

Fraglich ist außerdem, ob der Antrag der betroffenen obersten Landesbehörde auf Überprüfung dieser Entscheidung durch den IT-Rat Baden-Württemberg i. S. eines Rechtsbehelfs aufschiebende Wirkung entfalten oder sich nur um eine „nacheilende“ Rechtmäßigkeitskontrolle handeln soll. Ersteres würde erfordern, dass die Präsidentin oder der Präsident der Cybersicherheitsagentur ihre bzw. seine Entscheidung für sofort vollziehbar erklärt, weil anderenfalls die Gefahr nicht effektiv abgewehrt werden könnte.

Ungeklärt ist schließlich, welche Maßnahmen die Behörde auf wessen Kosten anordnen kann; die hiermit zusammenhängenden Fragen stellen sich insbesondere bei einem Tätigwerden gegenüber Privaten:

- Soll dies Zutritts- und/oder Beschlagnahmerechte der Cybersicherheitsagentur umfassen?
- Soll sie berechtigt sein, ihrerseits Prüfsoftware auf die Server und Geräte der Betroffenen aufzuspielen?
- Soll die Cybersicherheitsbehörde „Stilllegungen“ ganzer IT-Systeme anordnen können und – bejahendenfalls – in welchem Umfang und für welche Zeiträume?
- Soll die Cybersicherheitsbehörde „Ersatzvornahmen“ durchführen können?
- Wie soll damit umgegangen werden, wenn die Cybersicherheitsagentur zu zögerlich handelt oder die falschen Maßnahmen ergreift? Mit anderen Worten: Haftet die Cybersicherheitsagentur für etwaige Versäumnisse?

Richtig ist, dass die Cybersicherheitsagentur bei der Wahrnehmung der ihr eingeräumten Befugnisse auf den Verhältnismäßigkeitsgrundsatz, den Schutz personenbezogener Daten und den Schutz geistigen Eigentums Rücksicht nehmen muss.

e) § 7 CSG-E – Untersuchung

Kritisch sieht der Anwaltsverband die Ausführungen in der Gesetzesbegründung, dass z. B. großen Konzernen und deren Zulieferern eher mit technischer Unterstützung geholfen werden soll als anderen Unternehmen oder gemeinnützigen Einrichtungen. Von solch großen Konzernen kann er-

wartet werden, dass sie durch das Vorhalten eigener ausreichender IT-Abteilungen und zeitgemäßer Fortbildung der dortigen Mitarbeiter selbst vorsorgen. Offensichtlich soll hier die Wettbewerbsfähigkeit von großen Unternehmen gestützt werden, wie man auch an dem Argument sieht, dass besonders auf ihre just-in-time-Organisation Rücksicht genommen werden soll. Gerade solche großen Unternehmen haben aber auch die Möglichkeit, ihre Ressourcen anders zu verteilen und so IT-Sicherheitsanforderungen gerecht zu werden.

Die aus Steuermitteln finanzierten Kapazitäten der Cybersicherheitsagentur in diesem Bereich sollten allen Unternehmen gleichermaßen offenstehen und gerade kleine und mittlere Unternehmen unterstützen.

f) § 8 CSG-E – Warnungen

Die Cybersicherheitsagentur kann nach § 8 CSG-E die Öffentlichkeit oder die betroffenen Kreise vor Gefahren für die Cybersicherheit - auch unter Angabe des Namens Herstellers oder Inverkehrbringers - warnen. Hiermit sind regelmäßig Eingriffe in den eingerichteten und ausgeübten Gewerbebetrieb nach Art. 14 GG und in die Berufsfreiheit nach Art. 12 GG verbunden.

Zu begrüßen ist, dass die von der Rechtsprechung geforderte gesetzliche Ermächtigungsgrundlage für solche Warnungen geschaffen wird. Es bleibt zu hoffen, dass sie von den Verantwortlichen dann auch maßvoll angewendet wird, um nachhaltige Schäden bei Unternehmen zu vermeiden. Haftungsrechtliche Fragen stellen sich nicht nur, falls sich eine Warnung der Cybersicherheitsagentur im Nachhinein unzutreffend herausstellt, sondern auch wenn sie im Einzelfall unverhältnismäßig ist. Ob die zweifellos gebotene Richtigstellung in derselben Form in der die Warnung erfolgte, als weitgehende Kompensation verstanden werden kann, erscheint indes mehr als fraglich. Der Schaden durch mit der Warnung erfolgten Imageverlust ist zu diesem Zeitpunkt bereits eingetreten. Als Anspruchsgrundlage kommen entgegen den Erläuterungen in der Begründung jedoch nicht nur Amtshaftungs- und Folgenbeseitigungsansprüche in Betracht, sondern auch Unterlassungsansprüche.

Der Anwaltsverband befürwortet auch die Normierung der Löschungsfrist; sie ist geboten, um ausweislich der Entscheidung

BVerfG, Beschluss vom 21.03.2018 – 1 BvF 1/13 –, BVerfGE 148, 40,

den Grundrechtsschutz der Betroffenen Rechnung zu tragen.

g) §§ 9, 12 CSG-E – Landesdatenschutzgesetz

Gegen den Vorrang des CSG-E vor dem Landesdatenschutzgesetz bestehen mit Blick auf den Gesetzeszweck des CSG-E keine grundsätzlichen Bedenken. Unklar erscheint indes das Verhältnis des § 12 CSG-E zu den Anforderungen des Landesdatenschutzgesetzes, insbesondere in Bezug auf den Grundsatz der Datensparsamkeit, der Zweckänderung u. ä.

h) § 10 CSG-E – Kernbereichsschutz

Der Anwaltsverband begrüßt die Aufnahme expliziter Regeln zum Kernbereichsschutz in den Gesetzestext.

Zweifel weckt jedoch die konkrete Ausgestaltung, wenn Fälle, in denen sich die Frage stellte, ob Daten aus dem Kernbereich privater Lebensgestaltungen erhoben wurden, der oder dem behördlichen Datenschutzbeauftragten der Cybersicherheitsagentur sowie einer oder einem weiteren Bediensteten der Cybersicherheitsagentur mit Befähigung zum Richteramt zur Kontrolle vorzulegen sind. Hier wird nicht deutlich, was die Aufgabe der oder des „weiteren Bediensteten der Cybersicherheitsagentur mit Befähigung zum Richteramt“ sein soll.

Zwar bestimmt § 5 Abs. 5 Satz 4 CSG-E, dass, „die nicht automatisierte Verarbeitung der Daten nach den Sätzen 1 und 2 … nur durch Bedienstete mit der Befähigung zum Richteramt angeordnet werden“ darf. Zum einen ist dies die – soweit ersichtlich - einzige Norm die konkrete Befugnisse auf Bedienstete mit der Befähigung zum Richteramt beschränkt; ob die dort angesprochenen personenbezogenen Daten zugleich zum Kernbereich privater Lebensführung zählen, ist damit noch nicht gesagt. Auch ergibt sich daraus nicht, dass die Entscheidung der Cybersicherheitsagentur zwingend von einer bzw. einem Bediensteten mit der Befähigung zum Richteramt zu treffen ist, was unseres Erachtens jedoch sinnvoll wäre.

Zum anderen legt die Formulierung, der zufolge ein(e) weitere(r) Bediensteter mit der Befähigung zum Richteramt hinzuziehen ist, nahe, dass es sich insoweit nicht um dieselbe Person handeln kann. Damit stellt sich aber die Frage, welche Befugnisse, diese(r) weitere Bedienstete haben soll. Denn die Letztentscheidung trifft die oder der behördliche Datenschutzbeauftragte, wenn – wie der Entwurf es vorsieht - die Löschung nachzuholen ist, sofern sie oder er der Entscheidung der Cybersicherheitsagentur widerspricht.

Oder soll – zum dritten - damit lediglich zum Ausdruck gebracht werden, dass die oder der Datenschutzbeauftragte der Cybersicherheitsagentur (ebenfalls) über die Befähigung zum Richteramt verfügen muss? Dann sollte dies explizit geregelt werden.

Überdies vermögen wir der Gesetzesbegründung hier nicht zu folgen. Angeblich sei es extrem unwahrscheinlich, dass der Cybersicherheitsagentur bei der Suche nach Gefahren kernbereichsrelevante Inhalte zur Kenntnis gelangen. Semantische Inhalte könnten nur Zufallsfunde sein. An anderer Stelle spricht die Gesetzesbegründung jedoch davon, dass eine Gefahrenquelle schädliche Anhänge zu E-Mails sein können. Wer tatsächlich einen Cyberangriff auf diese Weise plant, kann versuchen, das spätere Opfer erst mit einem unverfänglichen E-Mail-Verkehr oder Bilderaustausch zu ködern. Auch kann man sich die Durchsuchung eines möglicherweise von Schadsoftware befallenen Laptops, Smartphones o. ä. nur schwer vorstellen, ohne dass dem Suchenden dabei auch persönliche Daten des Betroffenen, z. B. des Mitarbeiters einer Behörde oder eines Unternehmens, zur Kenntnis gelangen.

Wenn es angeblich so selten vorkommt, dass der Kernbereich tangiert wird, werden die behördlichen Befugnisse gewiss nicht nachteilig eingeschränkt, wenn der Kernbereichsschutz an dieser Stelle verstärkt wird.

i) § 11 CSG-E – Schutz von Zeugnisverweigerungsrechten

Der Anwaltsverband begrüßt die Aufnahme des Verwertungsverbots von Erkenntnissen, die bei von den Zeugnisverweigerungsrechten nach §§ 53, 53a StPO geschützten Personen gewonnen werden.

Die konkrete Formulierung erscheint jedoch missverständlich. § 11 Satz 5 CSG-E soll gewiss – insoweit § 9a Abs. 4 PolG vergleichbar – eine Ausnahme zu § 11 Sätze 1 bis 4 CSG-E darstellen, bezieht sich bei genauer Betrachtung jedoch nur auf den unmittelbar vorangegangenen Satz 4. Es erscheint deshalb vorzugswürdig entweder zu formulieren:

> „Sätze 1 bis 4 gelten nicht …“

oder § 11 Sätze 1 bis 4 CSG-E zu § 11 Abs. 1 CSG-E zusammenzufassen und § 11 Satz 5 als § 11 Abs. 2 CSG-E wie folgt zu fassen:

> „ Absatz 1 gilt nicht, sofern Tatsachen die Annahme rechtfertigen, dass die zeugnisverweigerungsberechtigte Person die Gefahr für die Cybersicherheit oder für den Bestand oder die Sicherheit des Staates oder Leib, Leben oder Freiheit einer Person oder für bedeutende Sach- und Vermögenswerte verursacht hat.“

j) § 15 CSG-E – Berichtspflichten

Der Anwaltsverband hält einer Erweiterung der Berichtspflichten für geboten; so sollte die Pflicht zur jährlichen umfänglichen Unterrichtung über die Ausübung der eingeräumten Befugnisse, den Erkenntnissen zur Bedrohungslage und zu technischen Weiterentwicklungen auch gegenüber dem Innenausschuss des Landtags und gegenüber der bzw. dem Landesdatenschutzbeauftragten bestehen. Wenn die bzw. der Landesdatenschutzbeauftragte aus zutreffenden Erwägungen bei der Evaluation zu beteiligen ist, gebietet es die Sachnähe, sie bzw. ihn bereits in die Berichtspflichten einzubeziehen.

3. Zu Art. 9 – Überprüfung der Auswirkungen dieses Gesetzes

Richtig ist es, eine Überprüfung der Auswirkungen des Cybersicherheitsgesetzes nach drei Jahren vorzusehen. Der Einsatz der veranschlagten Haushaltsmittel und von mehr als 80 Personalstellen sollte auf seine Effektivität hin untersucht werden. Insbesondere sollte sich bis dahin zeigen, welche „Konkurrenzverhältnisse“ zu bereits bestehenden Stellen bestehen, damit Doppelstrukturen abgebaut werden können. Es sollte auch untersucht werden, ob die geplanten Hilfestellungen für die mit diesem Gesetz Begünstigten tatsächlich eine wertvolle Unterstützung bei der Herstellung einer möglichst großen Cybersicherheit darstellen.

Die Aufarbeitung digitaler Angriffe ist meist recht komplex und aufwändig. Es sollte geklärt werden, inwieweit eine solche Cybersicherheitsbehörde über ausreichend technische und personelle Kapazitäten verfügt, um die gewünschten Untersuchungen durchführen, die Funktionsfähigkeit informationstechnischer Systeme wiederherstellen zu können sowie Standards und Maßnahmen durchzusetzen.

Wir würden uns freuen, wenn unsere Hinweise Eingang in das weitere Gesetzgebungsverfahren finden würden und stehen für weitere Gespräche gern zur Verfügung.

Mit freundlichen Grüßen

Prof. Dr. Peter Kothe
Präsident