HESSISCHER LANDTAG

Stenografischer Bericht
(ohne Beschlussprotokoll)

öffentliche Anhörung

84. Sitzung – Innenausschuss

15. Mai 2023, 10:03 bis 11:48 Uhr

Anwesend:

Vorsitz: Christian Heinz (CDU)

CDU

Alexander Bauer
Andreas Hofmeister
Uwe Serke
Frank Steinraths

BÜNDNIS 90/DIE GRÜNEN

Markus Hofmann (Fulda)
Torsten Leveringhaus
Lukas Schauder

SPD

Karin Hartmann
Heike Hofmann (Weiterstadt)
Rüdiger Holschuh
Marius Weiß

AfD

Dirk Gaw
Klaus Herrmann

Freie Demokraten

Dr. h.c. Jörg-Uwe Hahn
Thomas Schäfer (Maintal)

DIE LINKE

Torsten Felstehausen

Fraktionslos

Walter Wissenbach

Fraktionsassistentinnen und -assistenten:

CDU:	Johannes Schäfer
BÜNDNIS 90/DIE GRÜNEN:	Dr. Frederik Rachor
SPD:	Lena Kreutzmann
Freie Demokraten:	Julia Bayer

Landesregierung, Rechnungshof, etc.

StS Stefan Sauer, HMdIS

Marc-André Link (M 3), HMdIS

ROR Martin Keller, HRH

Anzuhörende:

Hessischer Städtetag	Referentin Dr. Anja Wiesmeier
Hessischer Beauftragter für Datenschutz und Informationssicherheit	Herr Prof. Dr. Roßnagel Frau Horlbeck Herr Dr. Bruhn
Universität Speyer	Univ.-Prof. Dr. David Roth-Isigkeit
EBS Universität für Wirtschaft und Recht	Prof. Dr. Matthias Friehe
Universität Bremen	Prof. Dr. Dennis Kenji-Kipker
Universität des Saarlandes Rechtsinformatik	Prof. Dr. Christoph Sorge
Universität Darmstadt Fraunhofer-Institut für Sichere Informationstechnologie SIT Fachbereich Informatik, Technische und Nationales Forschungszentrum für angewandte Cybersicherheit ATHENE	Prof. Dr. Michael Waidner
Goethe-Universität Frankfurt am Main Fraunhofer-Institut für Sichere Informationstechnologie SIT Institut für Informatik, und Nationales Forschungszentrum für angewandte Cybersicherheit ATHENE	Prof. Dr. Haya Shulman
ekom21 KGRZ Hessen	Olaf Orth Leiter Fachbereich Recht und Verträge
Evolution Security GmbH	Geschäftsführer Benjamin Mejri Lars Günther
Fraport AG	Alexander Döhne
Stadt Kassel Personal- und Organisationsamt Informationssicherheitsbeauftragter	Jens Lange
LOAD e. V.	Caroline Krohn

Protokollführung: Diane Busam, VA Claudia Lingelbach

Öffentliche mündliche Anhörung

Gesetzentwurf
Landesregierung
Hessisches Gesetz zum Schutz der elektronischen Verwaltung (Hessisches IT-Sicherheitsgesetz – HITSiG)
– Drucks. 20/10752 –

hierzu:

Stellungnahmen der Anzuhörenden
– Ausschussvorlage INA 20/75 –

(Teil 1 verteilt am 08.05.23, Teil 2 am 11.05.23)

Vorsitzender: Meine sehr geehrten Damen und Herren! Ich begrüße Sie herzlich zur 84. Sitzung des Innenausschusses des Hessischen Landtags. Ganz besonders willkommen heiße ich alle, die als Sachverständige und Anzuhörende heute unter uns sind. Vielen Dank für Ihre Zusagen und Ihre Bereitschaft, hier gleich zu dem einzigen Punkt des heutigen Tages, dem IT-Sicherheitsgesetz, mündlich vorzutragen. Die Drucksache ist Ihnen bekannt und liegt Ihnen vor.

Gleichfalls liegen dem Ausschuss alle schriftlichen Stellungnahmen der Anzuhörenden vor, sodass der Inhalt vorausgesetzt werden kann. Das heißt, als Ermahnung an die Anzuhörenden: Sie brauchen nicht noch einmal mündlich vorzutragen, was Sie schriftlich eingereicht haben. Bitte beschränken Sie sich vielmehr auf Ausführungen in gedrängter Form, vielleicht noch einmal auf die wesentlichen Punkte zugespitzt, die Ihnen ganz besonders wichtig sind. Es wäre gut, wenn sich diese Ausführungen in einem zeitlichen Rahmen von ungefähr fünf Minuten bewegen würden. Nach den einzelnen Blöcken gibt es immer Gelegenheit für Nachfragen aus den Reihen der Abgeordneten, sodass wir eher versuchen, hier ins Gespräch zu kommen, als lange Monologe und Ausführungen zu hören. Denn zum Lesen sind hoffentlich alle Abgeordneten in der Lage. Jedenfalls haben wir rechtzeitig alle Stellungnahmen zugeleitet bekommen.

Nach diesen Eingangsbemerkungen können wir loslegen. Die Landtagsverwaltung hat die Anhörung freundlicherweise in drei Blöcke gegliedert. Wir fangen gleich mit Block 1 an.

Frau **Dr. Wiesmeier:** Ich möchte meinen Ausführungen zum Gesetzentwurf einen grundlegend übergeordneten Gedanken vorwegschicken, und zwar dass die IT-Sicherheit oder Aufgaben und Maßnahmen zur IT-Sicherheit einen gesamtstaatlichen Charakter haben. Das bedeutet: Bund, Länder und Kommunen müssen hier eng zusammenarbeiten und haben auch ein gemeinsames Interesse daran, dass ein gewisses Sicherheitsniveau angestrebt wird.

Wenn wir diesen Gedanken voranstellen – und ich denke, wir sind uns hier im Raum alle einig, dass wir diesen Gedanken teilen können; er ist auch beim Gesetzentwurf bei der Problemstellung

aufgegriffen worden – und konsequent weiterdenken, dann ist dieser Gedanke aus unserer Sicht in dem Gesetzentwurf nicht ausreichend genug berücksichtigt.

Der Gesetzentwurf, den wir grundsätzlich positiv bewerten, ist aus unserer Sicht nicht weit genug in dem Sinne, dass die Kommunen im Rahmen der dort genannten Maßnahmen eng genug mitgenommen werden. Die Kommunen haben ja nicht nur selbstverwaltende Aufgaben, sondern nehmen auch staatliche Aufgaben wahr. Aus unserer Sicht ist es nicht sinnvoll, wenn bei der Aufgabenerfüllung auf staatlicher Ebene unterschiedliche Sicherheitsniveaus zugrunde liegen, wenn also einmal die Kommunen und einmal das Land die Aufgabe bearbeiten.

Deshalb wäre es aus unserer Sicht wünschenswert, wenn das Zentrum für IT-Sicherheit viel enger mit den Kommunen zusammenarbeiten würde – anders als in dem Gesetzentwurf enthalten –, dass das Zentrum für IT-Sicherheit also z. B. gemeinsame Sicherheitsstandards entwickelt, dass ein stärkerer Austausch mit den Kommunen erfolgt, dass das Zentrum für IT-Sicherheit eine zentrale Instanz darstellt, die auch IT-Sicherheitskompetenzen bündelt. Im Gesetzentwurf ist öfter mal die Rede davon, dass die Kommunen auf dieses Zentrum zugehen können und dass ihnen geholfen werden kann, wenn Kapazität vorhanden ist. Ich denke, dieses „Können“ und „wenn Kapazität da ist“ sind nicht im Sinne des Gesamtkonzepts, dass man eng zusammenarbeitet.

Deshalb würden wir uns hier wünschen, dass das Zentrum auch für die Kommunen mehr Aufgaben übernehmen kann. Die Kommunen sind bereit, die Kommunen haben großes Interesse an IT-Sicherheit. Die Kommunen sind auf ihrer Ebene teilweise noch nicht genug finanziell ausgestattet. Wenn das Zentrum da entsprechende Aufgaben übernehmen würde, wären auch die Kommunen bereit, da mitzuarbeiten.

Neben dieser finanziellen Unterstützung, die die Kommunen dafür benötigen, würden wir es auch befürworten, dass das Zentrum für IT-Sicherheit weiter finanziell oder noch mehr ausgestattet wird. Das ist nötig, wenn auch noch eine stärkere Einbindung der Kommunen erfolgen soll. Wir würden uns freuen, wenn Sie die Gedanken aufgreifen würden.

Vorsitzender: Wir kommen zum Hessischen Beauftragten für Datenschutz und Informationssicherheit. Ich habe ihn schon gesehen. Herr Prof. Dr. Roßnagel, Sie haben das Wort.

Herr **Prof. Dr. Roßnagel:** Der Gesetzentwurf ist zu begrüßen. IT-Sicherheit ist auch ein Thema für den Datenschutz. Insofern unterstützen wir alle Bemühungen, die zur Verbesserung der IT-Sicherheit führen.

IT-Sicherheit kann aber in Konflikt mit dem Datenschutz geraten, wenn personenbezogene Daten verarbeitet werden. Insofern ist ein Ausgleich zwischen dem Ziel der IT-Sicherheit und dem Ziel der informationellen Selbstbestimmung notwendig. Ich denke, dass der Ausgleich in dem Gesetzentwurf gelungen ist. Wir haben hier Regelungen, die gestufte Befugnisse vorsehen, die je nach

steigender Eingriffsintensität auch zunehmende Anforderungen stellen. Dadurch ist es möglich, dass wir IT-Sicherheit und Datenschutz erreichen.

Wichtig in dem Zusammenhang sind die Regelungen zur strengen Zweckbegrenzung, zur automatisierten Erhebung und Auswertung von Daten, zur Anonymisierung und Pseudonymisierung, die kurzen Zeiträume für die vorgesehene Speicherung, die Löschungsvorgaben, die technisch-organisatorischen Maßnahmen. Für mich konkret ist auch hilfreich, dass Kontrollen durch unsere Behörde möglich sind und dass an mehreren Stellen darauf hingewiesen wird, dass die Datenschutz-Grundverordnung und das HITSiG uneingeschränkt Geltung beanspruchen.

Diese ausgeglichenen Ergebnisse waren möglich durch einen vorbildlichen Einbezug meiner Behörde in die Vorbereitung des Entwurfs. Wir waren zeitig und umfassend immer beteiligt. Unsere Änderungsvorschläge wurden überwiegend berücksichtigt und umgesetzt. Ich möchte mich ausdrücklich für die enge Abstimmung und den konstruktiven Austausch zu diesem Gesetzentwurf bedanken.

Zwei Punkte möchte ich noch ansprechen. Der erste Punkt betrifft § 17, die Information der betroffenen Personen. Dort wird in Satz 1 eine Interessenabwägung vorgesehen: die Interessen der Betroffenen auf Transparenz mit den Interessen der verantwortlichen Stellen. Eine solche Interessenabwägung sehen Art. 13 und 14 der Datenschutz-Grundverordnung nicht vor. Die Rechte der Betroffenen können zwar eingeschränkt werden, z. B. nach Art. 23 Buchstaben c und d. Das ist in Satz 2 von § 17 erfolgt. Aber in § 17 Satz 1 ist eine Regelung getroffen, die meines Erachtens mit der Datenschutz-Grundverordnung so nicht vereinbar ist.

Das kann man jetzt noch im Gesetzgebungsprozess entsprechend korrigieren. Wenn man es nicht tut, ist es auch nicht schlimm, weil diese Regelung dann dem Anwendungsvorrang der Datenschutz-Grundverordnung unterfällt und nicht anwendbar ist. Daher kann man es sich herussuchen, ob man vorher reagiert oder hinterher dann gesagt bekommt, dass die Regelung nicht anwendbar ist.

Der zweite Punkt ist ein rein formaler. Er betrifft die Adressaten der datenschutzrechtlichen Erlaubnisse. Wir haben in § 7 eine Regelung, die die Datenverarbeitung ermöglicht, aber nur für das Zentrum für Informationssicherheit. Die anderen Stellen, die in § 1 genannt sind, sind weder in § 7 noch in §§ 8 bis 11 genau benannt. Sie werden aber in § 12, wenn es um die Zuständigkeit geht, als Stellen vorausgesetzt, die von diesen Erlaubnissen Gebrauch machen können. Hier könnte man also unter Umständen in der Begründung zu § 12 noch darauf hinweisen, dass diese Stellen in § 1 nach der Generalklausel des HITSiG, also § 3, die Erlaubnis haben, diese Daten zu verarbeiten, sodass es dann, wenn später die Frage ist, wer von den Erlaubnissen Gebrauch machen darf, zu keiner Verwirrung kommt. Ich denke, es würde der Rechtssicherheit dienen, wenn man hier eine entsprechende Ergänzung einfügt.

Vorsitzender: Jetzt gibt es Gelegenheit für die Abgeordneten für Nachfragen an Frau Dr. Wiesmeier und Herrn Prof. Roßnagel. Wünscht jemand das Wort?

Abg. **Heike Hofmann (Weiterstadt):** Ich darf Sie alle recht herzlich von Bijan Kaffenberger, unserem digitalpolitischen Sprecher, grüßen, der sehr gern bei der Anhörung dabei gewesen wäre, aus persönlichen Gründen – er ist Vater geworden – leider nicht dabei sein kann, sie aber recht herzlich grüßen lässt und gemeinsam mit uns trotzdem die Anhörung vorbereitet hat.

Ich habe eine Frage an Frau Wiesmeier vom Hessischen Städtetag. Sie haben hier auf die notwendige Zusammenarbeit, insbesondere des Zentrums für IT-Sicherheit, mit den Kommunen hingewiesen. Da habe ich die ergänzende Frage an Sie, ob die Kommunen vom Gesetz her noch stärker in den Geltungsbereich aufgenommen werden sollten, also wie man Ihr Begehren, das ja sehr nachvollziehbar ist, gesetzlich noch mal konkretisieren kann.

Die zweite Frage ist, ob IT-Sicherheit dann auch kommunale Pflichtaufgabe sein müsste und wie dies im Einklang mit der kommunalen Selbstverwaltung stünde.

Vorsitzender: Ich schaue noch mal die Abgeordnetenkollegen an. – Es gibt keine weiteren Wortmeldungen. Dann machen wir jetzt die Antwortrunde.

Frau **Dr. Wiesmeier:** Vielen Dank für die Nachfragen. In dem Gesetzentwurf sind die Akteure, die umfasst sind, enthalten. Die Kommunen sind auch enthalten. Aber wenn es – ich sage mal so – ums Eingemachte geht, was jetzt z. B. Standards anbelangt, dann heißt es: Für die Kommunen wird es empfohlen. Das bedeutet natürlich: Die Kommunen können es machen. Wir wissen aber alle, dass die Kommunen zum Teil nicht genug ausgestattet sind, um dies machen zu können. Deshalb würden wir, auch wenn Sie auf die kommunale Selbstverwaltung hinweisen, die uns sehr, sehr heilig ist, an dieser Stelle eine Pflicht begrüßen, damit die Kommunen die Möglichkeit haben, eine entsprechende finanzielle Ausstattung zu bekommen. Wie gesagt, wir haben alle ein Interesse, ein möglichst hohes Sicherheitsniveau zu erhalten. Wir haben mitbekommen, dass es IT-Sicherheitsvorfälle gibt. Das ist für das gesamte Land sehr, sehr unangenehm. Wir sehen es so: Die Kommunen übernehmen eine Verantwortung, das Land übernimmt eine Verantwortung. Demnach ist es für uns sinnvoll, wenn hier eine entsprechende Verpflichtung dahinter stehen würde.

Vorsitzender: Damit sind wir mit Block 1 schon durch. Wir kommen zu Block 2 unserer Liste. Von der Universität Speyer spricht Herr Universitätsprofessor Roth-Isigkeit.

Herr **Prof. Dr. Roth-Isigkeit:** Ich wollte zu dem Gesetzentwurf drei kurze Fragen thematisieren. Die erste Frage ist: Braucht man das überhaupt? Also braucht das Land eine solche Regelung, wenn wir doch gleichzeitig sehen, dass wir im Bereich der Cybersicherheit immer eine Tendenz zur Zentralisierung haben? Wir haben eine Zentralisierung auf Bundesebene, und auf der anderen Seite haben wir auch eine Zentralisierung in Europa. Das heißt, wir haben einen zunehmenden Ausbau einer europäischen Cybersicherheitsverwaltung.

Dann sagt der Gesetzentwurf in meinen Augen richtig, dass die Lücke da ist, die Hessische Landesverwaltung zu schützen. An der Stelle muss man sagen: Für diesen ganz konkreten Anwendungsbereich ist der Gesetzentwurf meiner Meinung nach erforderlich und so auch vernünftig gemacht.

Die zweite Frage, die sich daran anschließt, ist: Wie baut man das in die Architektur der Landesverwaltung, des Ministerialsystems ein? Nun ist es so, dass das geplante Zentrum relativ intensive ressortübergreifende Kompetenzen aufweist. Es scheint zunächst mal so, als ob es das Beste wäre, diese ressortübergreifenden Kompetenzen nahe beim Innenministerium anzusiedeln, also nahe an der Behörde zur Gefahrenabwehr. Nun hat aber die Cybersicherheit eigentlich eine ganz andere Struktur als die klassische Gefahrenabwehr. Wir haben gesehen: Es sind keine lokalen Gefahren, sondern Gefahren, die weitestgehend aus dem Ausland kommen, bei denen die Zuordnung auch schwierig ist.

An dieser Stelle hätte sich in meinen Augen die Frage gestellt, ob es nicht besser gewesen wäre, dieser besonderen Bedrohungslage mehr gerecht zu werden und eine eigene Behörde, eine etwas unabhängigere Struktur einzurichten, als sie direkt in das Innenministerium zu integrieren. Man könnte auch darüber nachdenken, ob man nicht eine besondere parlamentarische Verantwortlichkeit vorsieht. Gerade beim Landesdatenschutz hat das ja sehr gut funktioniert. Das heißt, man hat eine Behörde, die direkt mit dem Parlament kommuniziert und damit etwas zu tun hat. Von der Aufgabe her wäre das meines Erachtens besser gewesen.

Warum wäre das besser gewesen? Das ist die dritte Frage. Wir haben in den Ressorts ein Problem der politischen Verantwortlichkeit. Für eine ressortübergreifende Aufgabe gibt es in der Hessischen Verfassung eigentlich gar nicht so wirklich Raum, weil es die Struktur ist, dass die Minister, Ministerinnen ihre Ressorts in eigener Verantwortung leiten.

Wenn nun eine in ein anderes Ressort integrierte Behörde die politische Verantwortlichkeit für Vorfälle übernimmt, die in einem Ressort wie z. B. dem Gesundheitsressort vorkommen können, wo es zu Datenproblemen kommen kann, dann verschieben wir die Grundarchitektur des Ministerialsystems. Das mag jetzt in diesem Fall noch verschmerzbar sein, weil die Cybersicherheit eine so komplexe Aufgabe ist. Aber wir müssen, glaube ich, strukturell in den Gesetzgebungsvorhaben ein bisschen aufpassen, dass wir nicht die gesamte Struktur des ministerial organisierten Verfassungsstaats verändern, indem wir ressortübergreifende Kompetenzen in einzelnen Ressorts ansiedeln.

Herr **Prof. Dr. Friehe:** Ich möchte mich im Wesentlichen auch darauf beschränken, auf meine schriftlichen Ausführungen zu verweisen und einfach noch mal die zwei Punkte deutlich zu machen, die ich ausgeführt habe, einfach, den Gesetzentwurf noch mal konkret anzuschauen: Was will der Gesetzgeber hier eigentlich machen? Ein Teil ist die Einführung der zentralen Stelle für IT-Sicherheit.

Über die Andockung habe ich auch eine Bemerkung gemacht. Da kann man sicherlich streiten, aber das ist letztendlich eine politische Entscheidung. Ich habe mich ein bisschen gefragt, ob das nicht der Punkt wäre, wofür auch mal das Digitalministerium zuständig sein könnte, von dem nicht ganz klar ist, wie und in welchem Umfang es eigentlich besteht, weil es bisher eben nicht so gut mit Kompetenzen ausgestattet ist. Ich sehe aber durchaus auch Anknüpfungspunkte in den Innenbereich. Die Gefahrenabwehr ist erst mal grundsätzlich eine Aufgabe des Innenministeriums. Daher würde ich sagen, dass die Zuordnung auch nicht völlig verkehrt oder so ist.

Das, was jetzt eben zu einer parlamentarischen Aufgabe geäußert wurde, das also irgendwie im Bereich des Parlaments anzuordnen, wenn ich das richtig verstanden habe, kann ich nicht ganz nachvollziehen. Ich glaube, da wäre es nicht richtig aufgehoben. Es mag sein, dass man hier mit diesen ressortübergreifenden Aufgaben ein bisschen – ich will mal sagen – die Struktur innerhalb des Ministerialsystems auf die Probe stellt. Aber wenn man das jetzt an den parlamentarischen Bereich anknüpfen würde, dann würde gewissermaßen die Trennung zwischen Exekutive und Legislative auf die Probe gestellt. Das würde aus meiner Sicht für erheblich mehr Probleme sorgen und wäre auch verfassungsrechtlich nicht unproblematisch.

Daher würde ich sagen: Es ist schon richtig bei der Exekutive aufgehoben. In welchem Ressort das ist – das kann auf Dauer auch durch die entsprechende Geschäftsverteilung, wenn da noch mal Anpassungsbedarf besteht, geändert werden.

Ansonsten ist das Gesetz vor allem aus dem Gedanken heraus entstanden, dass mit der IT-Sicherheit auch Grundrechtseingriffe verbunden sein können. So verstehe ich den zweiten Teil des Gesetzes, der die entsprechenden Ermächtigungsgrundlagen enthält. Es wird auch Art. 10 GG zitiert. Es wird das Recht auf informationelle Selbstbestimmung zitiert, was gar nicht zitationspflichtig ist. Aber das steht auf einem anderen Blatt. Das scheint hier in Hessen üblich zu sein. Da hatten wir schon mal einen vergleichbaren Fall. Es schadet auch nicht, das Grundrecht zu zitieren.

Den Punkt, den ich hier noch machen möchte und auch in der schriftlichen Ausarbeitung gemacht habe, ist der, dass man sich auch erst mal anschauen müsste, wo genau die Grundrechtseingriffe überhaupt liegen. Es wird jetzt von allen anderen – ich will mal sagen – als selbstverständlich vorausgesetzt, dass wir es hier auf jeden Fall mit Grundrechtseingriffen zu tun haben. Das mag auch in bestimmten Bereichen so sein. Aber das scheint mir gar nicht so der typische Fall im Rahmen dessen zu sein, was da jetzt bei der Cyberabwehr passiert. Denn es geht ja erst mal um

die Durchsicht der regierungsinternen Kommunikation. Wenn ich jetzt mal ganz klassisch da herangehe und mir die Frage stelle, ob durch die Auswertung der Protokolldaten von einer dienstlichen E-Mail in Art. 10 GG eingegriffen wird, dann sage ich: Nein. Denn Art. 10 GG schützt den Fernmeldeverkehr zwischen Bürgern und nicht die Innerregierungskommunikation. Einen Eingriff in Art. 10 GG sehe ich hier, wenn überhaupt, nur in Ausnahmekonstellationen, beispielsweise wenn private E-Mails von dienstlichen Accounts versendet werden. Es gibt sicherlich Fälle, wo das so ist. Aber das scheint mir gar nicht so sehr der typische Fall zu sein. Diesen Punkt unterstreiche ich deswegen so sehr, weil in der öffentlichen Wahrnehmung, wenn so ein Gesetz mit allen möglichen Eingriffsermächtigungen präsentiert wird, gelegentlich der Eindruck entsteht, dass jetzt in alle möglichen Rechte des Bürgers eingegriffen werde und alle möglichen ganz neuen Befugnisse geschaffen würden. Das scheint mir gerade nicht der Fall zu sein. Das wäre ein falsches Verständnis, dass wir jetzt hier ein Gesetz haben, das intensiv in Grundrechte des Bürgers eingreift. – So weit vielleicht. Ich freue mich auf Ihre Nachfragen.

Herr **Prof. Dr. Kenji-Kipker:** Mit dem Entwurf für ein Hessisches IT-Sicherheitsgesetz werden die umfangreichen Befugnisse des Hessen CyberCompetenceCenters im Zuständigkeitsbereich des Hessischen Ministeriums des Inneren und für Sport, das als zentraler Ansprechpartner zum Thema Cybersicherheit in Hessen fungiert, an eine Rechtsgrundlage geknüpft, was gemessen am skizzierten Aufgaben- und Befugnisumfang sinnvoll, sachgerecht und meiner Meinung nach auch juristisch notwendig erscheint, insbesondere auch deshalb, weil es bislang an einer umfassenden Rechtsgrundlage für Befugnisse und die Datenzugriffe in Hessen fehlt.

Vor diesem Hintergrund ist dementsprechend auch der durch die Landesregierung vorgelegte Gesetzentwurf zu sehen, der vorangehend das Ziel verfolgt, meiner Meinung nach aber noch unter verschiedenen systematischen und inhaltlichen Mängeln leidet. Ich werde diese jetzt in Kürze aufzählen. Das ist aber nicht als abschließend zu verstehen.

Zunächst beginnen diese Mängel meiner Meinung nach in den Begriffsbestimmungen, die teils dem BSI-Gesetz entlehnt sind und ohne ersichtlichen Grund abgewandelt werden. Aber auch die generelle Frage, was wir unter einer Sicherheitslücke verstehen wollen – das ist ja ein wichtiger Begriff, der zurzeit auch im Umsetzungsgesetz von NIS 2 noch mal angepasst und abgewandelt wird.

In ontologischer Hinsicht sollte meiner Meinung nach eine Klarstellung vorgenommen werden, ob wir jetzt von Informationssicherheit; IT-Sicherheit oder Cybersicherheit sprechen wollen, wie es beispielsweise auch der Gesetzgeber in Baden-Württemberg mit einer vergleichbaren Regelung getan hat.

Im Rahmen der Grundsätze der Informationssicherheit stellt sich mir die Frage, weshalb nur für technische Maßnahmen der Stand der Technik maßgeblich sein soll und an der Stelle nicht auch die organisatorischen Maßnahmen einbezogen werden, wie es in vergleichbaren bundesrechtlichen Vorschriften ebenfalls der Fall ist.

Außerdem sollte die Rolle des ISB und die staatliche Gewährleistungsverantwortung der IT-Sicherheit überdacht werden. So finden sich keinerlei Hinweise auf eine hinreichende Qualifikation, die Konkretisierung seines Tätigkeitsbereichs im Hinblick auf wesentliche Änderungen an IT-Systemen und letzten Endes die Folgen seiner Beteiligung, also beispielsweise im Sinne eines Vetorechts, was man hier andenken könnte, falls bestimmte Änderungsvorschläge der IT-Infrastruktur grundlegende Sicherheitsbedenken seinerseits zur Folge haben.

Ergänzend wäre in diesem Zusammenhang eine Begründungspflicht der Dienststellen im Allgemeinen anzudenken, sollten sie den Empfehlungen des CISO nicht folgen beziehungsweise eigene Maßnahmen zur Cybersicherheit ergreifen.

Die Rollen in der Zusammenarbeit des Zentrums für Informationssicherheit und der Hessischen Zentrale für Datenverarbeitung sollten deutlich klarer definiert und auch gegeneinander abgegrenzt werden. Dazu gehört zum einen die Zusammenarbeit mit privaten Stellen. Gerade auch im Bundesbereich haben wir gesehen, dass die Bildung solcher Public Partnerships sehr wichtig ist, weil Cybersicherheit letzten Endes Informationsaustausch bedeutet. Informationsaustausch setzt ein entsprechendes Vertrauen voraus. Zum anderen braucht es aber genauso die Herstellung einer gesetzlich verankerten Informationsparität zwischen HZD und dem Zentrum für Informationssicherheit.

Es sollte meiner Meinung nach auch ausdrücklich in den Gesetzeswortlaut aufgenommen werden, dass Erkenntnisse im Zusammenhang mit der Informationssicherheit unverzüglich zu teilen sind.

Ein großer Knackpunkt und auch ein Problem an dieser gesetzlichen Regelung sind meiner Meinung nach die Vorschriften zur Datenverarbeitung. Meiner Meinung nach leiden diese an gravierenden systematischen und inhaltlichen Mängeln und sollten deshalb einer grundlegenden Überprüfung und Überarbeitung unterzogen werden. Wir haben bereits einige datenschutzrechtliche Fragestellungen im Rahmen dieser Anhörung angesprochen. Meiner Meinung nach ist es zurzeit so, wenn man einen Blick in diesen Entwurf wirft, dass die Vorschriften mehr Rechtsunsicherheit als Rechtssicherheit bieten. Es ist meiner Meinung nach auch verhältnismäßig unklar, in welchen Fällen welcher Tatbestand gilt. Auch hier der Verweis auf das Cybersicherheitsgesetz Baden-Württemberg, wo das meiner Meinung nach deutlich besser gelöst ist. Das bietet hier deshalb auch wertvolle Anknüpfungspunkte.

Systematisch fragwürdig ist überdies, weshalb sich in einer Vorschrift zur Datenverarbeitung eine inhaltlich weit gefasste Befugnisgrundlage zur Beseitigung von Schadprogrammen findet. In den Datenverarbeitungsvorschriften finden sich im Übrigen in der gegenwärtigen Fassung keine hinreichenden Vorgaben, die Datensicherheit und Datenschutz in einen angemessenen Ausgleich bringen. Denn auch Metadaten, die zu Zwecken der IT-Sicherheit ausgewertet werden können – das wird hier eben auch vorgeschlagen –, können einen Personenbezug entfalten.

Darüber hinaus haben wir verschiedene begriffliche Schwierigkeiten. So ist auch von anonymisierten personenbezogenen Daten die Rede, was ich inhaltlich auch etwas irreführend finde.

Die Datenschutzvorgaben sind hier insgesamt noch deutlich klarer zu formulieren und gegenwärtig meiner Meinung nach mangelhaft. Das betrifft sowohl die Eingriffsgrundlagen als auch die übermäßige Einschränkung datenschutzrechtlicher Betroffenenrechte.

Insgesamt empfehle ich deshalb, das Gesetz systemisch klar in Datenschutzvorschriften und Eingriffs- und Auswertungsbefugnisse zu untergliedern, das heißt, die Vorschriften voneinander zu trennen, die gegenwärtig zusammengefasst sind, um eine vernünftige behördliche Arbeitsgrundlage zu schaffen und die widerstreitenden Interessen in einen verfassungskonformen Ausgleich zu bringen.

Herr **Prof. Dr. Sorge:** Ich halte das Gesetz im Grundsatz für überaus begrüßenswert und in der Systematik auch erst einmal gut gelungen. Deshalb sind meine Anmerkungen doch eher kleinteilig und beziehen sich auf einzelne Normen.

Ich möchte trotzdem eine allgemeine Bemerkung voranstellen, nämlich den Umgang mit Sicherheitslücken. Es ist in der Fachdiskussion mittlerweile ein großes Thema und auch allgemein anerkannt, dass Sicherheitslücken, die einer Firma oder einer Behörde bekannt werden, offengelegt werden sollten. Ich hielte es für einen gesamtgesellschaftlichen Beitrag zur IT-Sicherheit, wenn auch das Land da mit gutem Beispiel vorangehen könnte und man entsprechend eine gesetzliche Regelung zur Offenlegung von Sicherheitslücken in einem verantwortungsvollen Prozess aufnehmen würde. Man spricht von einem „Coordinated Vulnerability Disclosure“-Prozess, bei dem sichergestellt wird, dass die Offenlegung auch keine Sicherheitsprobleme mit sich bringt.

Zu einigen einzelnen Normen: Ich werde jetzt nicht meine gesamte Stellungnahme vorlesen, sondern nur die aus meiner Sicht wichtigsten Punkte ansprechen.

Das ist einmal eine begriffliche Sache, dass eine Verarbeitung von Protokolldaten vorgesehen ist, die sich im Prinzip auf Kommunikationsprotokolle beziehen, aber so, wie ich die Normen verstehe, eigentlich eindeutig etwas anderes gemeint ist, nämlich dass Daten einer Protokollierung, also sogenannte Logdateien, was schon protokolliert ist, ausgewertet werden dürfen. Da habe ich entsprechend eine Änderung, Anpassung an den Begriff „Protokollierungsdaten“ aus dem BSI-Gesetz empfohlen.

Zu den Begriffen habe ich auch anzumerken, dass hier im Gesetzentwurf Informationstechnik und IT-Sicherheit, was ja nicht genau das Gleiche wie Informationssicherheit ist, geregelt sind. Das heißt, die nicht technischen Aspekte – jemand druckt etwas aus und lässt das irgendwo liegen – sind nach meiner Lesart zunächst nicht mit einbezogen. Es wäre zu überlegen, ob man das ändern will.

Ich habe weiterhin anzumerken, dass in § 7, insbesondere Abs. 2, wo eine Grundlage für die Verarbeitung von sensiblen personenbezogenen Daten in sogenannten besonderen Kategorien vorgesehen ist, aus meiner Sicht die Anforderungen der DSGVO an eine solche Regelung nicht

erfüllt sind, weil dort eine Konkretisierung verlangt wird, die aber nicht ausreichend gegeben ist. Das heißt, an dieser Stelle könnte man europarechtlich in Probleme kommen.

Weiterhin ein – ich will fast sagen – Trend der IT-Sicherheit, aber auch schon seit einigen Jahren, ist, dass man Datenverkehr irgendwo im Netz auf einer Firewall oder ähnlichen Systemen entschlüsselt. Das ist in Unternehmensnetzen durchaus gängig. Dazu müssen die Endsysteme mitwirken. Das heißt, man muss Konfigurationsänderungen beispielsweise auf den einzelnen Arbeitsplatzgeräten vornehmen, und dann kann Datenverkehr entschlüsselt werden. Der Gesetzentwurf geht offenbar auch davon aus, dass das passiert. Denn es wird ausdrücklich von verschlüsselter Kommunikation und Kopfdaten, die da ausgewertet werden sollen, gesprochen. Ich würde es aber für wünschenswert halten, das tatsächlich explizit zu regeln, wenn man das wirklich machen will, was nicht unüblich wäre. Aber es könnte für die Anwender durchaus überraschend sein. Also sollten sie wenigstens darüber informiert werden, wenn das passiert. Natürlich ist dann auch abzuwägen, inwieweit das gemeinsam mit einer Privatnutzung von IT-Systemen oder mit so Dingen wie Bring your own Device funktioniert, wobei ich nicht weiß, ob das im Landesnetz praktiziert wird.

Weiterhin habe ich in meiner Stellungnahme einige technische Klarstellungen zu § 9 empfohlen, die ich nicht im Einzelnen aufzählen will, aber für durchaus wichtig halte, weil ansonsten einige Missverständnisse entstehen könnten. Ein zentrales Missverständnis – das hat der Herr Kipker auch schon angesprochen – ist das Verhältnis Pseudonymisierung, Anonymisierung, wie es in den §§ 10 und 11 vorkommt. Man hat den Eindruck, dass pseudonymisierte Daten als nicht mehr personenbezogen angesehen werden oder auch als ausreichend anonymisiert. Das ist nicht zwingend so. Eine Pseudonymisierung, die dem Stand der Technik entspricht, ist auch nicht trivial, weshalb ich empfehlen würde, dazu eine Richtlinie durch das zu schaffende Zentrum erarbeiten zu lassen, die dann auch bindend sein könnte.

Weiterhin würde ich noch eine Regelung der datenschutzrechtlichen Verantwortlichkeit in § 12 empfehlen, das Verhältnis zwischen Zentrum und anderen Beteiligten am Landesdatennetz.

Und schließlich ist auch das Sicherheitskonzept, das in § 15 angesprochen wird, sehr wenig konkretisiert. Auch da wäre es durchaus denkbar, noch einige inhaltliche Vorgaben zu machen, beispielsweise entsprechend den Empfehlungen des BSI.

Damit bin ich am Ende meiner Punkte. Wie gesagt, ich habe noch vieles schriftlich aufgeschrieben. Aber es hat ja keinen Sinn, das alles zu wiederholen.

Vorsitzender: Dann haben wir noch die gemeinsame Stellungnahme von Herrn Prof. Michael Waidner und Frau Prof. Shulman. – Wer trägt vor? Beide? Bitte schön.

Herr **Prof. Dr. Waidner:** Das werden tatsächlich wir beide machen. – Zum einen teilen wir uns das. Wir haben vier Punkte. Ich werde zwei erklären, meine Kollegin Haya Shulman die anderen beiden. Vorneweg möchte ich mich aber bedanken für die Gelegenheit. In der Stellungnahme haben wir sehr viele lobende Worte für den Gesetzentwurf gefunden. Die könnte ich jetzt gerade wiederholen. Das werde ich nicht, sie gelten aber trotzdem. Wir wollen die Stellungnahme um vier Punkte ganz kurz ergänzen.

Punkt 1: Das Gesetz – es geht um das Thema Ausnahmen – definiert eine ganze Reihe von Einrichtungen, die von den Regelungen des Gesetzes inklusive Meldepflichten mehr oder weniger ausgenommen sind. Das sind neben Gerichten, Staatsanwaltschaft und dem Datenschutzbeauftragten auch die Schulen – ganz am Anfang – und dann die Hochschulen des Landes. Klammer auf: Wir sind beide keine Juristen. Daher verzeihen Sie mir bitte, dass wir einfach logisch denken und jetzt nicht sagen: Es gibt grundsätzliche verfassungsrechtliche Bedenken, warum es nicht geht.

(Vereinzelt Heiterkeit)

Vielmehr kommt jetzt ein Wunsch jenseits aller juristischen Betrachtungen. Ich denke nämlich, zur Verbesserung der Cybersicherheit sollten auch für diese Einrichtungen entsprechende Angebote und Empfehlungen gemacht werden. Das wird auch gemacht. Aber tatsächlich denke ich, man sollte auch Vorgaben machen. Angriffe auf diese Einrichtungen sind für das Land genauso gefährlich wie auf alle anderen Einrichtungen des Landes.

Gerade die Hochschulen des Landes waren in letzter Zeit vermehrt Opfer von Cyberangriffen. Alle erinnern sich an den Fall der Universität Gießen, denke ich. Sehr oft wird die IT von Hochschulen auch dazu verwendet, wiederum Cyberangriffe auf andere Einrichtungen zu fahren. Ich denke, das ist ein wichtiger Punkt.

Generell sollten also alle Teile der Landesverwaltung, zu der ich jetzt auch die Hochschulen rechne, also auch die Goethe-Universität und die Uni Darmstadt, Angebote zur Verbesserung der Cybersicherheit bekommen. Das war Punkt 1.

Bei Punkt 2 geht es um die Kompetenzen des CISO. Das wurde gerade schon mal angesprochen. Die Bündelung der Kompetenzen hier an einem Zentrum für Informationssicherheit unter der Leitung eines unabhängig aufgestellten CISO ist – das sagt die ganze Cybersicherheitsforschung – ein unverzichtbares Element jeder modernen Cybersicherheitsorganisation. Eine der Grundregeln ist aber, dass die Funktion des CISO ein sehr umfassendes Informationsrecht gegenüber dem CIO und allen ausführenden Stellen – der CIO des Landes, aber auch die HZD – haben muss. Darüber hinaus muss der CISO bei allen Entscheidungen, die einen Einfluss auf die IT-Sicherheit haben können, auch ein Vetorecht haben. Das heißt, Entscheidungen, die sich negativ auf die Cybersicherheit auswirken, sollte der CISO eigentlich verhindern können. Das ist jetzt die Lehrbuchmeinung.

Für CISOs der Ministerien wird im Entwurf festgelegt, dass diese bei allen wichtigen Dingen ihres Hauses zumindest mal ins Benehmen gesetzt werden müssen. Besser wäre natürlich Einvernehmen. Mir wurde jetzt nicht ganz klar, ob das auch für den Landes-CISO gilt. Ich nehme es mal an. Aber das könnte man vielleicht deutlicher sagen. Es muss auf jeden Fall auch für den CISO sowie für den Landes-CIO, die HZD usw. gelten.

Damit bedanke ich mich erst mal recht herzlich. Für die anderen beiden Punkte übergebe ich an meine Kollegin.

Frau **Prof. Dr. Shulman:** Auch ich möchte mich herzlich für die Gelegenheit zur Kommentierung des Gesetzentwurfs bedanken.

Punkt 3 auf unserer Liste ist die Cybersicherheitsarchitektur des Landes. Die Cybersicherheit der Landesverwaltung hängt langfristig entscheidend davon ab, dass im Land eine moderne IT und Cybersicherheitsarchitektur umgesetzt werden. Dies umfasst die gesamte IT des Landes und der HZD, aber natürlich auch die aller Dienstleister des Landes. Dementsprechend sollte das Zentrum für Informationssicherheit auch für die fortlaufende Entwicklung und Umsetzung einer solchen Cybersicherheitsarchitektur verantwortlich sein. Stichworte sind hier einerseits die Einführung Phishing-resistenter Authentifikation, feingranulares und restriktives Rechtemanagement, feingranulare Überprüfung von Zugriffsrechten und flächendeckende Verschlüsselung.

Andererseits gehören hierzu auch Strategien zur Mitigation und deren Umsetzung, also z. B. das Patching von Schwachstellen und die Kapselung durch Segmentierung und Virtualisierung. Schließlich gehört hierzu auch eine umfassende Strategie zu Threat Intelligence, also die Erstellung eines verlässlichen umfassenden und detaillierten Lagebilds für das Land. Hierzu gehören beispielsweise regelmäßige Scans der IT des Landes, seiner Dienstleister, aber auch Darknet-Analysen zur Aufdeckung kompromittierter Konten und anderer Kompromittierungen. Unter anderem gehören hierzu auch Fragen, ob externe Dienstleister oder ob Cloud-Dienste verwendet werden und was auf einer Cloud und was auf On Premise self-gehostet wird.

Punkt 4 auf unserer Liste ist ein umfassender Zugriff auf Cybersicherheitsdaten. § 8 beschränkt die Cybersicherheitsanalyse auf sechs Typen von Protokolldaten. Hier sollte unbedingt mit einer offenen Liste oder allgemeinen Definition gearbeitet werden, da ansonsten eine wirklich effektive Analyse nicht garantiert werden kann. Beispielsweise beinhaltet die vorliegende Liste keine Protokolldaten, sogenannte Intrusion Detection Systeme, SCIM-Systeme oder Anwendungen wie SAP.

Der Gesetzestext ist hinsichtlich der Analyse von Inhaltsdaten zudem zu sehr auf Schadsoftware fokussiert. Neben Schadsoftware gibt es auch andere gefährliche Payloads. Inhaltsdaten beispielsweise sind Nachrichten, die so konstruiert sind, dass der sie verarbeitende Server zum Absturz gebracht wird, oder auch Nachrichten, die einen Cyberangreifer zum Ausleiten gestohlener Informationen verwendet.

Vorsitzender: Dann kommen wir jetzt zu unserer Fragerunde.

Abg. **Dr. h.c. Jörg-Uwe Hahn:** Ich wollte den Hessischen Datenschutzbeauftragten fragen, was er von der doch sehr umfassenden und grundsätzlichen Kritik an diesem Gesetzentwurf, die Herr Prof. Kenji-Kipker hinsichtlich der Aussagekraft der nicht ganz ordentlich genutzten datenschutzrechtlichen Vorgaben vorgetragen hat, hält.

Vorsitzender: Herr Prof. Roßnagel ist noch da. Eigentlich hatten wir ihn eben schon halb entlassen. Aber er ist freundlicherweise geblieben. Dann kann er sich gleich noch äußern.

Abg. **Heike Hofmann (Weiterstadt):** Ich habe zunächst eine Frage an Prof. Kenji-Kipker. – Sie haben sehr detailliert auf – ich will es mal so formulieren – Regelungslücken oder Optimierungsmöglichkeiten und -bedarfe hingewiesen. Ich habe noch mal eine Frage zu § 2 Nummer 4 des Gesetzentwurfs. Sie haben dort den rechtlichen Begriff der „Sicherheitslücke“ problematisiert und haben in Ihrer Stellungnahme formuliert, er sei „verbrannt“. Da die konkrete Nachfrage an Sie: Welchen Formulierungsvorschlag hätten Sie?

Dann habe ich zwei, drei Fragen an Prof. Waidner bzw. Prof. Shulman, anknüpfend an Ihre Stellungnahme, auch die, die Sie eben abgegeben haben. Sie haben geschrieben, dass die Umsetzung so erfolgen solle, dass die neu geschaffenen Strukturen nahtlos in die Cybersicherheitsarchitektur Deutschlands integriert werden. Vielleicht können Sie das noch mal konkretisieren?

Die zweite Frage: Sie regen auch die Vernetzung mit der Cybersicherheitsforschung im Gesetz an oder sagen, diese solle stärker betont werden. Können Sie das noch mal konkretisieren?

Abg. **Alexander Bauer:** Herr Vorsitzender, meine Frage geht auch an Prof. Kenji-Kipker. – Sie hatten angeregt, dass das Gesetz in Anlehnung an das baden-württembergische Gesetz eine Begriffsdefinition voranstellt. Jetzt habe ich mal nachgeschaut. Die definieren hier alle möglichen Fachbegriffe – Informationstechnik, Sicherheit der Informationstechnik, Kommunikationstechnik. Wo ist der Mehrwert? Klar kann man das machen, aber die Differenzierung der jeweiligen Begrifflichkeiten ist aus Ihrer Sicht erforderlich, weil es da Begriffsunschärfen gibt oder weil Begriffe falsch verwendet werden. Warum sollte man in einem Gesetz die fachlichen Begriffe erläuternd vorwegstellen? Können Sie mir das noch mal kurz erklären?

Abg. **Torsten Felstehausen:** Ich habe eine Frage an Herrn Prof. Dr. Dennis Kenji-Kipker und Herrn Prof. Dr. Christoph Sorge. Sie hatten beide angesprochen, dass Sie es befürworten würden, wenn in diesem Gesetz auch geregelt ist, dass Datensicherheitslücken unverzüglich offengelegt werden, nachdem sie erkannt worden sind. Das ist eine Diskussion, die schon relativ lange geführt wird. Wie könnte das in diesem Gesetz verarbeitet werden, und welche zentralen Vorteile würde dieses Verfahren bringen? Wenn Sie zur Abwägung für uns darstellen könnten: Welche Gefahren sind gegebenenfalls damit verbunden?

Abg. **Marius Weiß:** Ich habe eine Frage an Herrn Prof. Friehe von der EBS. In Ihrer Stellungnahme auf S- 2 im dritten Absatz in der Mitte heißt es – ich zitiere –:

> Andererseits besteht in Hessen seit 2019 ein „Digitalministerium“, das bisher über keinen „echten“ Geschäftsbereich verfügt. Hier bestünde die Chance, das Digitalministerium jenseits von Fototerminen bei innovativen Unternehmen mit echten eigenen Verwaltungskompetenzen auszustatten.

Da wäre meine Frage: Welche Verwaltungskompetenzen sollte das Digitalministerium nach Ihrer Vorstellung an dieser Stelle übernehmen?

Abg. **Thomas Schäfer (Maintal):** Als Nichtjurist hätte ich da noch mal eine Frage in Richtung Herr Prof. Waidner und Frau Prof. Shulman, weil Sie ja eben angesprochen haben, dass die Schulen, Hochschulen mit dem Gesetzentwurf nicht abgedeckt worden sind. Inwieweit sehen Sie die Verbindung zwischen Landes- bzw. kommunalen Institutionen zu Unternehmen, Dienstleistern, die für die Kommunen Aufgaben unternehmen – beispielsweise kommunale Unternehmen – durch dieses Gesetz ausreichend abgedeckt, dass da auch die Regelungen getroffen sind? Es gibt durchaus auch außerhalb der jeweiligen Verwaltung Zuarbeit oder IT-Verknüpfungen, die da hineinragen.

Vorsitzender: Wir beginnen mit der Antwortrunde. – Zunächst Herr Prof. Roßnagel zur Frage von Herrn Dr. Hahn.

Herr **Prof. Dr. Roßnagel:** Ich würde die Antwort gern in drei Teile gliedern. Der erste Teil betrifft die Punkte, die Herr Kipker aus Sicht der IT-Sicherheit getroffen hat. Dazu würde ich mich jetzt nicht äußern, weil wir für die Datenschutzfragen zuständig sind.

Die beiden anderen Punkte betreffen den Datenschutz. Das sind Hinweise darauf, dass mehr Rechtssicherheit erreicht werden könnte, indem die Befugnisse anders gegliedert werden, und

dass man sich stärker an dem Cybersicherheitsgesetz in Baden-Württemberg orientiert. Das mag sein. Wir haben uns darauf fokussiert, die Vorlagen, die uns immer gemacht wurden, die wir immer rechtzeitig bekommen haben, die wir uns genau anschauen konnten, zu besprechen. Wir haben uns deswegen die grundsätzliche Systematik des Gesetzes angeschaut und diese erst einmal so akzeptiert, weil diejenigen, die sich mit der Entstehung des Gesetzes intensiv befasst haben, da auch eine Fülle von Überlegungen hineingesteckt haben. Man kann natürlich jetzt alles weglegen und kann sagen: Wir nehmen das aus Baden-Württemberg und ziehen das ganz neu auf.

Das verbindet sich jetzt mit dem dritten Punkt, den ich ansprechen wollte, nämlich die Feststellung, dass kein ausreichender Ausgleich mit dem Datenschutz stattgefunden hat. Dem würde ich widersprechen. Deswegen erschien es uns jetzt auch nicht notwendig, alles in die Tonne zu treten und ein ganz neues Gesetz vorzuschlagen. Vielmehr kann ich feststellen, dass wir mehrere Entwürfe bekommen haben – es ist ein längerer Prozess gewesen, das Gesetz zu entwickeln. Wir haben alle Entwürfe mit den Autoren des Gesetzes intensiv besprochen und haben unsere jeweiligen Stellungnahmen abgegeben. Allen Punkten, die wir zur Verbesserung angemerkt hatten, ist nachgekommen worden. Außer bei § 17 – das ist der letzte Punkt, den wir wirklich als Problem sehen – sind die Lösungen, die man gefunden hat, in meinen Augen vertretbar.

Herr **Prof. Dr. Friehe:** Herr Weiß hatte an mich die Frage adressiert, wie es mit der Zuordnung ist. Da muss ich erst mal klarstellen, dass das sozusagen gar keine Frage ist, die hier durch das Gesetz geklärt werden kann. Denn das ist ja das Zusammenspiel vom Gesetz und dem Geschäftsverteilungsplan der Landesregierung. In dem Gesetz ist es so, dass der CISO – – Hier steht nicht „Innenministerium“ drin, sondern „das für die IT und Cybersicherheit in der Landesverwaltung zuständige Ministerium“, und das ist eben nach dem derzeitigen Geschäftsverteilungsplan das Innenministerium. Wenn ich jetzt hier nichts Grundlegendes übersehen habe, gibt es gar keinen Bereich, den man gesetzgeberisch benennen könnte. Denn dieser Geschäftsverteilungsplan der Landesregierung sieht eben keine eigene Nummer für das Digitalministerium vor. Vielmehr kommt das Digitalministerium nur in verschiedenen Fußnoten dieses Geschäftsverteilungsplans vor, während die anderen Ministerien jeweils einen ausformulierten Geschäftsverteilungsplan haben. Ich hatte mir hier nur die ‚Anmerkung erlaubt, dass man, wenn man so ein Digitalministerium haben will, darüber nachdenken könnte, dass man dort nicht nur Fragen des Digitalen bündelt, wo man über Konzepte nachdenkt, mal Unternehmen besucht und so, sondern dort auch die Verwaltungsaufgaben, die anfallen, reinsetzt.

Das würde bedeuten, dass man darüber nachdenken könnte, die IT-Sicherheit und die Cybersicherheit, die jetzt im Innenministerium angesiedelt sind, dort anzudocken. Natürlich ist das Innenministerium ein großes und mächtiges Ministerium, das nicht so gerne Kompetenzen abgibt. Aber auf der anderen Seite haben wir ja ein Ministerium – ich will mal sagen – im Aufbau, das sich vielleicht noch ein bisschen finden muss. Das würde dann den politischen Willen voraussetzen, dieses Ministerium dauerhaft auch mit entsprechenden Kompetenzen zu versehen, auszustatten und aufzubauen.

Wie gesagt, das muss man aber auch nicht machen. Es wird ja auch politisch darüber gestritten, ob man überhaupt ein Digitalministerium braucht. Es ist jedenfalls – das will ich abschließend auch noch mal deutlich machen – nicht so, dass es im Innenministerium in irgendeiner Weise an einer sachlich falschen Stelle aufgehoben wäre. Das ist überhaupt nicht so. Vielmehr ist IT-Sicherheit Teil der Frage der öffentlichen Sicherheit und Ordnung und gehört damit natürlich auch als besonders spezieller Bereich zu einem Kernbereich des Innenbereichs.

Das ist letztlich einfach eine politische Entscheidung, ob man sagt: Das ist dann da auch richtig aufgehoben, oder ob man sagt: Nein, das ist so eine spezielle Aufgabe. Dafür will man perspektivisch ein anderes Ministerium sozusagen errichten und entsprechend ausstatten, was dann voraussetzen würde, dass man an anderer Stelle vielleicht Kompetenzen wegnimmt. Vielleicht so viel.

Herr **Prof. Dr. Kenji-Kipker:** Erst einmal zum Begriff der Sicherheitslücke. Das ist ein Thema, das uns insbesondere seit letztem Jahr bewegt. Ich habe mich auch umfassendst damit auseinandergesetzt. Eine Sicherheitslücke ist technisch zu verstehen. Sie kann nicht politisch, geostrategisch oder ähnlicher Art verstanden werden. Das ist eine technische Sicherheitslücke. Das gibt die Rechtsprechung des Bundesverfassungsgerichts her, und das gibt auch die Gesetzesbegründung zu den IT-sicherheitsgesetzlichen Vorschriften im Bund her. Wenn man das klarstellen wollte, dann sollte man erwähnen, dass eine Sicherheitslücke ausschließlich technische Hintergründe hat.

Im Bund wird das Ganze zurzeit aufgeweicht. Mit der Umsetzung der NIS-2-Richtlinie ist man nämlich dabei, eine politische Warnmöglichkeit bzw. eine politische Bewertung der Sicherheitslücke einzuführen. Das schadet meiner Meinung nach dem Verständnis von IT-Sicherheit. Denn IT-Sicherheit ist in erster Linie ein technischer Begriff. Wenn wir ein politisches Verständnis der Sicherheitslücke einführen würden, dann wäre der Rechtsunsicherheit Tür und Tor geöffnet. Das würde letzten Endes auch möglicherweise Klagen nach sich ziehen. Davon kann ich an der Stelle nur ganz dringend abraten.

Zur Differenzierung der Begrifflichkeiten bzw. zum Thema Definition: Wir haben ja jetzt eine Definition in diesem Gesetzentwurf drin. Meiner Meinung nach ist es besonders wichtig, ein einheitliches Begriffsverständnis zu haben. Da kann man so ein bisschen auch an die Frage der Sicherheitslücke anknüpfen. Eine Sicherheitslücke ist ein technischer Begriff, wie ich schon gesagt habe. IT-Sicherheitsrecht ist generell ein technisches Thema. Das heißt also, die Regelungsintentionen können durchaus unterschiedlich sein. Aber die Begrifflichkeiten, mit denen wir uns befassen, sind oftmals ähnlich. Wenn wir definieren, dann müssen wir natürlich nicht alles 1 : 1 neu definieren. Wenn wir aber bestimmte Begriffe umdefinieren, was ja auch vorgenommen wird und was ich in meiner Stellungnahme auch angemerkt habe, dann sollten wir zumindest begründen, warum diese Begriffe letzten Endes umdefiniert werden.

In vielerlei Hinsicht ist es sicherlich auch möglich, auf bundesrechtliche Definitionen zu verweisen, sodass nicht für jeden Einzelfall eine eigenständige Definition im hessischen Gesetz vorgenommen werden muss. Das ist also nicht zwingend notwendig.

Was wir brauchen, ist ein einheitliches systematisches Verständnis. Denn sonst führt das Ganze zu Auslegungsschwierigkeiten. Die Bedrohungslagen sind in technischer Hinsicht im Land und im Bund dieselben. Da macht es keinen Sinn, unterschiedliche Definitionen zu verwenden, ohne das zu begründen.

Das Thema Schwachstellenmanagement: Ja, das ist ein wichtiges Thema. Das ist ein Dilemma. Das ist eine offene Diskussion. Das wurde auch in der Anhörung des Digitalausschusses im Bundestag im Januar ganz umfassend behandelt, ohne dass man bislang zu einer Lösung gekommen ist. Wir reden schon jahrelang über Themen wie Hackback, „Aktive Cyberabwehr“, „Digitale Gegenschläge“. Das hängt letzten Endes alles so ein bisschen damit zusammen, wo Schwachstellen gefunden werden, wie sie verwaltet werden, wer sie bekommt und wie sie letzten Endes genutzt werden.

Wie gesagt, das ist ein Dilemma. Es geht hier um die Abwägung zwischen unterschiedlichen verfassungsrechtlichen Positionen. Eine absolute These zu vertreten, dass generell eine unbedingte Offenlegung von Schwachstellen zu erfolgen hat, wird man wahrscheinlich aus der rechtlichen Perspektive – nicht aus der politischen Perspektive – nicht möglich machen können, weil immer auch widerstreitende Grundrechte da sind.

Es gibt zum Thema Schwachstellenmanagement schon umfassende wissenschaftliche Vorarbeiten. So hat z. B. die Stiftung Neue Verantwortung ein Papier dazu erarbeitet, in dem ein Prozess vorgeschlagen wird, wie ein solches Schwachstellenmanagement aussehen könnte, dass man eben auch schaut, welche Relevanz, Kritikalität eine solche Schwachstelle besitzt. Gegebenenfalls werden weitere Stakeholder einbezogen, um diese Schwachstelle zu bewerten und dann letzten Endes eine Entscheidung zu haben: Wird die Schwachstelle offengelegt? Wird sie nicht offengelegt? Wird sie für weitere Zwecke genutzt? Da kann ich einfach noch mal anregen, sich die entsprechenden wissenschaftlichen Veröffentlichungen anzuschauen.

Sicherlich, wenn man das Thema jetzt in Hessen angehen möchte, dann wäre das vorbildlich. Das könnte vielleicht auch sogar eine Ausstrahlungswirkung auf die Bundesdebatte in diesem Bereich haben. Es wäre durchaus zu begrüßen, wenn wir da auch zu verbindlichen Regelungen gelangen würden, weil dann solche Themen wie Hackback, „Digitale Gegenschläge“ sicherlich auf ein vernünftigeres juristisches Fundament gestellt würden.

Herr **Prof. Dr. Sorge:** Ich bin ja auch zum Thema „Umgang mit Schwachstellen bzw. Sicherheitslücken“ angesprochen worden. Meine Auffassung ist schon, dass man im Grundsatz, von dem es im Einzelfall Ausnahmen geben mag, zur Offenlegung von Schwachstellen kommen sollte aus der schlichten Überlegung heraus: Wenn eine Schwachstelle beispielsweise in einer Behörde

bekannt wird oder durch eine Behörde gefunden wird, dann kann auch jemand Drittes diese Schwachstelle finden und damit eventuell nicht verantwortungsvoll umgehen. Das heißt, er könnte sie auf dem Schwarzmarkt verkaufen. Es gibt tatsächlich einen Markt für Schwachstellen. Damit wird natürlich das Sicherheitsniveau gesamtgesellschaftlich reduziert, wenn keine Möglichkeit besteht, die Schwachstelle zu beheben.

Der Hinweis auf eine Offenlegung einer Schwachstelle kann natürlich auch Unternehmen, die die Software hergestellt haben, dazu motivieren, diese Schwachstellen schneller zu beheben. Das heißt jetzt nicht, dass man sofort, in dem Moment, in dem man eine Schwachstelle findet, sie offenlegen soll oder muss. Denn natürlich kann eine sofortige Offenlegung auch Sicherheitsprobleme verursachen, weil Dritte sofort die Gelegenheit haben, die Schwachstelle auszunutzen, die sie vorher vielleicht nicht kannten.

Deshalb ist es in der Community relativ gängig, dass man Schwachstellen koordiniert meldet, auch eine Absprache mit Stakeholdern trifft und die Information auf jeden Fall an das Unternehmen gibt, das die entsprechende Software beispielsweise programmiert hat, und nach einer gewissen Frist, die ausreichen sollte, um den Fehler zu beheben, an die Öffentlichkeit geht, damit alle Betroffenen, die das System einsetzen, ihre eigenen Systeme überprüfen können, überlegen können, wie schnell sie reagieren müssen usw. Es sollte also ein koordinierter Prozess sein. Den könnte auch das Zentrum für Informationssicherheit koordinieren, dass man die entsprechende Kompetenz jetzt nicht mehr bei jeder einzelnen Behörde vorhalten muss. Das heißt, die einzelne Behörde könnte die Schwachstelle an das Zentrum melden, das dann den weiteren Prozess abstimmt, beispielsweise mit dem betroffenen Unternehmen, und sicherstellt, dass die Schwachstelle zeitnah behoben wird und dann alle Stakeholder informiert werden.

Herr **Prof. Dr. Waidner:** Vielleicht eine kleine Vorbemerkung: Da wir ja sozusagen die beiden Informatiker im Hause sind – die anderen professoralen Kollegen sind, glaube ich, Juristen –, möchte ich das nur bestätigen und unterstützen. In der Wissenschaft sagt man: Bei Schwachstellen muss der Fokus auf dem Beheben sein, also nicht auf dem Veröffentlichen – das muss man nicht unbedingt, aber die Hersteller müssen informiert werden. Dass der Fokus auf dem Beheben liegt, das ist unbestritten.

Das passt auch ganz gut zu der ersten Frage von Frau Hofmann zu der Sicherheitsarchitektur und was wir damit gemeint haben. Auf der einen Seite ist Hessen in Deutschland unter den Ländern relativ weit, was Cybersicherheit betrifft. Das muss man einfach honorieren. Der Bund bemüht sich natürlich auch. Es gibt das BSI-Gesetz. Es gibt das BSI. Es gibt das Vorhaben, aus dem BSI eine zentrale Stelle zu machen, die dann auch mehr Verantwortung für die Länder übernimmt. Dementsprechend muss man einfach sagen: Egal, wie jetzt das hessische Gesetz aussieht, es muss irgendwie zu dem passen, was im Bund passiert. Das ist nun mal ein bisschen schwierig. Man muss im Kopf behalten, dass das vereinheitlicht wird. Hessen soll beim besten Willen nicht auf ein Mittelmaß herunternormiert werden oder so. Aber man muss es irgendwie

hinbekommen, dass das alles zusammenhängt. Wie gesagt, das BSI-Gesetz, NIS 2 wurden gerade schon erwähnt usw., das ist einfach eine gewisse Herausforderung. Das ist in diesem Sinne keine Kritik an dem, wie es im Gesetz steht oder wie es in Hessen gemacht wird, sondern einfach der Hinweis auf eine große Herausforderung.

Da wir auch schon über Schwachstellen und Melden gesprochen haben, auch da ganz kurz den Hinweis, dass es lustigerweise zwischen Recht und Technik, glaube ich, gerade unterschiedliche Interpretationen gibt, wie politisch der Begriff der IT-Sicherheitsschwachstelle ist. Das Recht hat vielleicht die eine Meinung. In der Forschung, die sich mit vertrauenswürdiger IT beschäftigt, ist schon allgemein anerkannt: Das Vertrauen in IT ist keine technische Eigenschaft, nicht nur eine technische Eigenschaft, sondern ist ganz massiv auch eine politische Eigenschaft. Das muss man einfach im Blick behalten. Zu sagen, IT-Sicherheit sei ein rein technischer Begriff, stimmt so aus Sicht der Technik originellerweise nicht. Vielmehr ist das auch ein politischer Begriff. Das muss man unter einen Hut bekommen. Das hat jetzt mit dem Gesetz vielleicht auch wieder eher wenig zu tun. Aber das muss man einfach im Blick behalten.

Ich kann noch etwas zur zweiten Frage von Frau Hofmann, was die Forschung machen könnte, sagen. Das ist eigentlich relativ einfach. Hessen ist tatsächlich der Vorreiter im Bereich Forschung in Deutschland. Ohne Eigenlob betreiben zu wollen, aber mit ATHENE in Darmstadt, der TU Darmstadt, der Goethe-Universität sind wir weit vor allen Bundesländern, auch vor befreundeten Bundesländern ganz im Westen – gar keine Frage.

Ich würde mir wünschen, dass aus dieser Vorreiterstellung, die wir haben, im Gesetz auch zur Geltung kommt, auch ausgedrückt wird, dass man manche Dinge machen könnte. Cybersicherheit entwickelt sich sehr schnell voran. Es muss technologieoffen sein und muss offen sein für neue Dinge. Oft kommen in der Forschung neue Dinge früher als in der Industrie. Darauf muss man zugreifen können. Auch das ist wieder keine Kritik. Tatsächlich arbeiten wir eng mit dem HMdIS, mit Hessen3C zusammen. Das funktioniert eigentlich ganz gut. Aber man könnte da für das Land deutlich mehr machen. Das überfrachtet jetzt vielleicht ein bisschen das Gesetz. Aber wenn es darum geht: „Wie kann das Land beispielsweise – – Frau Shulman hat gesagt, man muss für alle Landesstellen dringend Threat Intelligence anbieten. Da ist die Forschung viel weiter als die Industrie. Da könnten wir mit Forschungsmitteln dem Land sehr weit unterstützend entgegenkommen und Hilfe anbieten, was man in der Industrie gar nicht einkaufen kann und auf die Art und Weise vielleicht auch in die hessische Industrie Dinge reinbringen. Da wird jetzt also quasi nicht nur an das Gesetz gedacht, sondern da geht es ganz allgemein um Cybersicherheit in Hessen. – Das war, glaube ich, die Antwort auf die zweite Frage von Frau Hofmann.

Frau **Prof. Dr. Shulman**: Ich möchte nur noch etwas ergänzen. Ich stimme natürlich allem zu. Warum ist aber die Vernetzung mit der Forschung wichtig? In unserer Forschung sehen wir das Ökosystem von Kriminellen und Hackern. Sie entwickeln sich stets. Sie warten nicht. In der Forschung untersuchen wir und sicherlich auch andere Forscher im Bereich der Cybersicherheit, die

technisch arbeiten, dieses Ökosystem. Wir untersuchen die Werkzeuge, die die Kriminellen entwickeln, die Angriffsvektoren. Das ist sehr wichtig, um Angriffe zu verhindern. Es ist wichtig, zu wissen, was sie machen. Was sind die Kompromittierungen, was sind die Probleme?

Wir arbeiten eng mit dem Land Hessen, aber nicht nur mit Hessen, und natürlich mit der Industrie zusammen. Wir bekommen ganz oft Feedbacks, wie viele Angriffe wir verhindert haben, weil wir im Voraus wissen, was die Angreifer vorhaben, oder wir wissen, dass es eine Lücke gibt, oder wir wissen, dass es eine Intrusion gibt, also dass sie im Netz sind.

Angriffe passieren viel früher, als wir sie wahrnehmen. Wenn wir merken, dass Angriffe stattfanden, dann ist es viel zu spät. Der eigentliche Angriff war schon vorher. Es dauert typischerweise ein paar Tage bis ein paar Wochen, bis die Kriminellen diesen Angriff dann ausnutzen. Wenn die Systeme verschlüsselt oder Daten gestohlen sind, dann merken wir, dass ein Angriff stattgefunden hat. Aber genau in dieser Zeit kann man den Angriff verhindern. In dieser Zusammenarbeit mit der Forschung kann man diese Intelligence bekommen. Aber nicht nur. Man kann auch neue Strategien entwickeln. Man kann Cybersicherheitsarchitekturen entwickeln. Wir sehen, dass das sehr wichtig ist, dass die Behörden, die Industrie und das Land ganz eng mit der Wissenschaft, mit der Forschung zusammenarbeiten.

Zur zweiten Frage: Für die Dienstleister muss das Gesetz genauso gelten. Sie bieten Dienste für Schulen, Hochschulen, Industrie, Behörden. Die Dienstleister werden oft angegriffen. Über Angriffe auf Dienstleister können auch alle Kunden des Dienstleisters angegriffen werden. Das sind die sogenannten Lieferkettenangriffe. Solche Angriffe kommen oft vor. Z. B. vor Kurzem, vor etwa einem Jahr, gab es einen Angriff auf das Kaseya-Unternehmen. Durch diesen Angriff konnten Kriminelle ganz viele Kunden von Kaseya angreifen. Das heißt, dass natürlich Dienstleister eine ganz wichtige Infrastruktur sind, für die das Gesetz genauso gelten muss.

Vorsitzender: Vielen Dank. – Das war die Antwortrunde. Dann können wir mit dem dritten Block weitermachen. Hier beginnen wir entgegen der Reihenfolge auf dringende Bitte von Frau Krohn mit LOAD e. V.

Frau **Krohn:** Vielen Dank, dass Sie LOAD heute in der Anhörung auch anhören wollen. Unsere schriftliche Stellungnahme ist aufgrund einer späten Vertretungsregelung durch meine Person ein bisschen verspätet gekommen. Die bekommen Sie natürlich im Nachgang. Ich möchte hier nur ein paar Punkte herausarbeiten.

Das Allererste ist, dass es sehr erfreulich ist, dass wir hier einen sehr breiten Konsens darüber haben, dass wir in der Digitalisierung der Verwaltung sehr stark auf Datenschutz und Datensicherheit achten wollen und dass hier eine Verbesserung vonnöten ist. Das haben wir auch anerkannt. Das ist auch wirklich sehr, sehr gut, auch die intensive Auseinandersetzung damit, auch

die technische Auseinandersetzung vorbehaltlich der Dinge, denen wir zustimmen, die Herr Prof. Kenji-Kipker auch schon gesagt hat, dass es viele Ungenauigkeiten gab.

Wir haben uns sehr intensiv mit dem Gesetz auseinandergesetzt und haben hinterher an vielen Stellen mehr Fragen als Antworten gehabt. Deswegen gibt es ein paar Themen, bei denen wir noch mal aus der Zivilgesellschaft heraus – also jenseits der juristischen Betrachtung – darauf hinweisen möchten, wo es bereits sehr breite Diskussionen gibt. Das ist eben schon angeklungen. Im Hinblick auf die Erstellung des Gesetzes haben wir Anzeichen dafür, dass man die Auseinandersetzung mit den aktuellen großen Debatten und dem, was aktuell auf Bundes- und Länderebene nicht gut läuft, ein bisschen vermisst. Jedenfalls scheint das Gesetz an vielen Stellen das zu zementieren, was gerade breit auf Bundes- und anderen Länderebenen diskutiert wird.

Ich möchte dafür vier Beispiele nennen und das gerne so formulieren – für Sie hoffentlich ein bisschen unterhaltsamer –, dass ich Ihnen vier Aspekte nennen werde, bei denen ich Ihnen prognostiziere, dass unser Vorhaben, die IT-Sicherheit für Hessen zu verbessern, scheitern wird.

Das Erste, bei dem wir ein prognostiziertes Problem ausgemacht haben, ist die fehlende Einbettung von Bund und Ländern. Alle, die sich damit beschäftigen, kennen das sogenannte Cyber-Wimmelbild der Verantwortungsdiffusion. Das ist eine sehr intensive Arbeit der Stiftung Neue Verantwortung – ich sehe schon einige lächeln; ich habe es hier auch als Fußmatte dabei; wenn das jemand sehen möchte; das war die einzig angemessene Größe. Wir wissen jedenfalls, dass es eine Vielzahl von Institutionen gibt auf kommunaler, auf Länder-, auf Bundes-, auf europäischer Ebene, die miteinander im Widerstreit sind, wo wir jeden Tag Kompetenzgerangel sehen, bei denen wir jeden Tag sehen, dass Informationspflichten, dass sozusagen Kompetenzüberlastungen sich miteinander verhaken. Und es gibt keinen größeren Feind der Sicherheit der Bürgerinnen und Bürger, als wenn sich solche Behörden oder nachgeordneten Behörden und Institutionen mehr miteinander streiten, als für eine Sicherheit für die Bürgerinnen und Bürger zu sorgen.

Jetzt ist LOAD, wie Sie vielleicht wissen, ein Verein für liberale Netzpolitik, der sich ganz stark den Rechten der Bürgerinnen und Bürger verpflichtet fühlt und auch staatliche Befugnisse gerne auf ein Mindestmaß verringern möchte, einfach auch um staatliche Übergriffe auf Rechte der Bürgerinnen und Bürger einzuschränken. Und hier sehen wir wirklich ein Übermaß an bereits vorhandenen Institutionen.

Jetzt ist klar: Im aktuellen Cyber-Wimmelbild der Verantwortungsdiffusion gibt es schon das Hessen3C. Es ist die gute Nachricht, dass kein weiteres Kästchen hiermit entsteht, sondern einfach die Rechtsgrundlage dafür entsteht. Aber nichtsdestotrotz vermissen wir hier eine gesamte Strategie, bei der Bundes- und Länderinitiativen mal orchestriert werden.

Das ist der Grund, warum wir auch hier voraussehen, bei aller Mühe, die wir uns jetzt geben, die Begriffe richtig klarzuziehen und all solche Dinge, dass keinem in der Sicherheit geholfen ist, wenn wir hier nicht einmal sehr, sehr klar zwischen Bund und Ländern eine Kommunikation aufmachen und sagen, wer eigentlich was macht.

In diesem Zusammenhang komme ich zu meinem Punkt 2: Die Rolle des BSI. Wir waren einigermaßen bestürzt darüber, dass das BSI in diesem Gesetz zwar Erwähnung findet, aber all das, was das BSI die letzten Jahre und Jahrzehnte an Vorschlägen, an Grundlagen, an Leitlinien und dergleichen erarbeitet hat, hier eine vage Empfehlung ist. Wir haben hier im Gesetz noch keine wirkliche Verschärfung der Verpflichtung, gerade für die Landesverwaltung, sich mit den Leitlinien, die erprobt und bewährt sind, sozusagen verpflichtend auseinanderzusetzen, sie auch zu auditieren und einmal festzulegen, dass das hier der Standard ist, der für alle verbindlich ist. Ich vermisse ganz häufig in Debatten, in neuer Gesetzgebung zur IT-Sicherheit oder Cybersicherheit, dass wir hier einfach auch noch mal auf Rechtsdurchsetzung bestehen. Es ist ein wichtiger Aspekt, wie wir hier beispielsweise auch mit dem BSI kooperieren wollen.

Da haben wir auch eine Debatte auf Bundesebene, die wirklich sehr, sehr viele Probleme im Management der Cybersicherheit in Deutschland offenbart hat, nämlich die Frage nach der Unabhängigkeit des BSI. Die zieht sich auf Länderebene fort, wenn wir solche Zentren errichten, bei denen klar ist: Hier ist ein Ministerium, und dieses Ministerium greift sich die Kompetenz für diese Institution, und die ist nicht unabhängig.

Das ist auch gleichzeitig unser Punkt 3. Ich kann Ihnen mein Wort darauf geben – auch als LOAD-Vorstand –, dass eine Institution, die den Zweck verfolgt, unser aller Sicherheit zu erhöhen, scheitern wird, wenn sie politisch gesteuert ist, weil die politische Steuerung mit der Expertensteuerung technischer Art häufig kollidiert. Und der politischen Steuerung darf nicht der Vorzug gegeben werden.

Ich glaube, es ist extrem wichtig, sich mal die Entwicklung auf Bundesebene der letzten Monate anzuschauen, auch bei den Personalwechseln beim BSI, um einmal sehr, sehr deutlich zu sehen, was hier eigentlich passiert, wenn es sozusagen in der Sache Unstimmigkeiten gibt, die politisch ausgetragen werden. Das hilft uns in unserer gesamten Cyberlage, die ja auch, wie schon richtig gesagt wurde, international vernetzt ist, überhaupt nichts.

Das ist der Grund, warum wir ganz dringend appellieren und sagen: Dieses Gesetz sollte viel, viel intensiver an die BSI-Strukturen, die BSI-Vorschläge herangeführt werden und gleichzeitig unabhängiger von der Exekutive werden. Ich stimme dem Kollegen von der EBS auch nicht zu, dass das in die Exekutive gehört. Ich stimme dem Kollegen aus Speyer zu, dass ich denke, dass so ein Zentrum dann erfolgreicher sein könnte, wenn es einen ähnlichen Status hätte wie unser Landesbeauftragter für Datenschutz, der ja von der Regierung vorgeschlagen und vom Landtag gewählt wurde. So muss das eigentlich sein. Es muss eine öffentliche Kontrolle geben, und diese Kontrolle ist in diesem Gesetz einfach nicht verankert. Die haben wir vermisst, auch in den Formulierungen, die da sagen: Wenn es sozusagen Kompetenzerhöhungen gibt und Grundrechtseingriffe verschärft werden, dann bedarf es einer richterlichen Genehmigung aufseiten des Ministeriums. Ganz ehrlich, als Bürgerrechtlerin wünsche ich mir deutlichere Kontrollmechanismen, die einfach Zugriffsrechte einschränken. Ich betrachte mit Sorge abermals die angekündigte Beschneidung von Grundrechten, weil wir seit dem 11. September 2001 eine kontinuierliche Beschneidung von Grundrechten in unserer Sicherheitsgesetzgebung sehen. Deswegen ist die Grundforderung von LOAD einmal ganz grundsätzlich ein Moratorium von Sicherheitsgesetzen,

bevor wir nicht eine Überwachungsgesamtrechnung angestellt haben. Denn hier sehen wir eine Tendenz, die wir umkehren müssen.

Zum Schluss erlauben Sie mir, eine ganz pragmatische Erfahrung anzuführen, die Sie natürlich nicht davon abhalten sollte, ein Gesetz zu machen, weil Sie natürlich mit dem Gesetz Normen herstellen. Ich bitte dafür um Entschuldigung, aber ich finde, es muss hier bedacht werden. Wir haben hier ein Gesetz, das sagt: Wir haben eine Institution, die eingerichtet wird, um den genannten Stellen zu helfen. Die genannten Stellen sind aber nicht entbunden davon, sich selbst zu helfen. Das heißt, hier bauen wir sozusagen Parallelstrukturen, ohne dass die Zugriffsrechte des Zentrums für Informationssicherheit näher bestimmt sind. Ich weiß halt nicht, wann bei einem Cybervorfall tatsächlich jemand das Kommando übernimmt angesichts der verschobenen Verantwortungen.

Aber ungeachtet dessen sind wir uns ja auch alle einig, dass wir zurzeit einen massiven Fachkräftemangel haben. Jetzt haben wir abermals das Problem, dass, wenn dieses Zentrum am Ministerium angekettet ist, wir TVöD-Vergütungen haben. Jetzt frage ich Sie, wie Sie bei den Aufgaben, die Sie sich in diesem Gesetz überlegt haben, das Personal finden wollen, natürlich in Konkurrenz zu den anderen Ministerien, das diese Aufgaben überhaupt bewältigen kann, wenn Sie sich die Marktpreise angucken und wenn Sie sich anschauen, wie ein Wirtschaftsunternehmen solche Expertise vergütet. Wenn es Ihnen gelänge, in dieser Organisation nach Marktpreisen zu bezahlen, hätten Sie eine Organisation, die fünf bis sieben Personen groß wäre, und das ohne Assistenzen, weil diese nicht mit budgetiert sind. Ich kann Ihnen nur sagen: Wir haben dann ein Zentrum, das entweder qualitativ den Aufgaben nicht gewachsen sein wird – vielleicht personell schon; keine Ahnung –, aber wir haben definitiv ein Problem. Denn selbst wenn wir das Problem beheben, haben wir noch ein quantitatives Problem, weil wir es mit fünf bis sieben Personen nicht schaffen, das zu erfüllen, was dieses Gesetz hier erwartet.

Ich warne davor, da auch die Erwartungen an dieses Gesetz zu hoch zu schrauben und zu sagen: Es müsste noch dieses und müsste noch das und müsste noch forschen und müsste noch verteilen und koordinieren usw. Wenn wir sagen: Wir brauchen eine Institution, die die Landesverwaltung sicherer macht, dann lassen Sie uns eine Institution gründen, die die Landesverwaltung sicherer macht und keine eierlegende Wollmilchsau.

Herr **Orth:** Ich bedanke mich auch im Namen der ekom für die Einladung, heute hier unsere Stellungnahme in kurzen Worten noch mal auf den Punkt zu bringen. Ich versuche, das auch kurz zu machen.

Als IT-Dienstleister der Verwaltung in Hessen ist IT-Sicherheit unser Tagesgeschäft. Wir kämpfen natürlich auch immer mit den strukturellen Schwierigkeiten, die wir heute hier auch im Plenum gehört haben, mit unklaren Rechtsgrundlagen, technischen Herausforderungen, personellen Herausforderungen.

Ich möchte aber trotzdem für ekom21 sagen, dass wir grundsätzlich der Auffassung sind, dass die stärkere politische Verankerung auch der IT-Sicherheit im Landesrecht eine sehr große Signalwirkung und daher auch eine grundsätzliche Bedeutung für ekom21, für die Bürger und natürlich auch für die Verwaltung hat, sei sie im staatlichen Bereich oder im Kommunalbereich.

In unserer Stellungnahme haben wir im Wesentlichen zwei Punkte aufgegriffen, die für uns als IT-Dienstleister und in unserer Rolle als ekom wichtig sind: einmal die gesetzliche Strukturierung in § 1, welcher gliedert zwischen Landesverwaltung, mittelbarer Landesverwaltung mit Rechts- und Fachaufsicht – also, das ist nicht ganz so scharf, wenn ich es richtig in Erinnerung habe – und den Gemeindeverbänden und Gemeinden und den Schulen. Als ekom21 sind wir uns nicht ganz sicher, was der Gesetzgeber in der Einordnung mit uns vorhat. Denn wir sind ein Zwischending. Die Rechtsaufsicht ist nach dem Datenverarbeitungsverbundgesetz dem Land zugewiesen. Wir sind aber ein kommunaler Zweckverband. Dementsprechend sind wir mehr auf der kommunalen Seite eingeordnet. Das würde auch bedeuten, dass dort ganz andere Rechtsfolgen im Gesetz angeknüpft sind. Aber die gesetzgeberische Vorgabe dafür ist uns nicht so ganz klar. Wo sollen wir uns dort einsortieren? Der Staatsgerichtshof hat in den Neunzigerjahren entschieden, dass die ekom kein Gemeindeverband ist. Daher tendieren wir hier für eine klare gesetzgeberische Einordnung und auch für den Wunsch der ekom, dass wir sagen: Wir zählen aufgrund unserer Mitgliederstruktur zu den kommunalen Einrichtungen in Nummer 3.

Als Beispiel, wo sich diese Einordnung auch wirklich auswirkt, habe ich die Regelung in dem Gesetz gesehen, in dem § 1 Nummer 3 HITSiG, die nicht für Nummer-3-Stellen gilt, sondern nur für Stellen nach Nummer 1 und 2. Daher, denke ich, ist es ganz besonders wichtig, dass auch da eine Einordnung stattfindet.

Der zweite Punkt, der uns aufgefallen ist: Das Gesetz spricht ja von Verwaltungstätigkeit. IT – das haben wir heute gehört – ist ein generelles Strukturelement. Wir fragen uns: Was bedeutet es eigentlich, wenn eine Behörde gerade keine Verwaltungstätigkeit im klassischen Sinn ausübt, also IT-Infrastrukturprozesse und -systeme wie Netze, Firewalls usw. nutzt, wo einerseits Verwaltungstätigkeit ausgeübt wird, also Anträge genehmigt, bearbeitet werden, aber auch Dinge wie das Verkaufen von Holz, z. B. durch Hessen Forst als Eigenbetrieb, durchgeführt werden? Ich kann mir gut vorstellen – ich kenne die Landesverwaltung nicht so gut –, dass letztlich am Ende des Tages dasselbe Netz benutzt wird, derselbe Rechner, nämlich der Hessen-PC, mit denselben IT-Sicherheitseinstellungen. Und das Gesetz spricht eigentlich von Verwaltungstätigkeit. Da, finde ich, ist es nicht ganz präzise. Auf der operativen Ebene kann man das nicht trennen. Man kann nicht Verwaltungstätigkeit von anderer Tätigkeit, von den in § 1 genannten Stellen trennen. Das wäre, glaube ich, eine Überforderung der IT.

Das waren aus unserer Sicht die wichtigsten Punkte. Vielen Dank, dass ich die heute hier vortragen durfte.

Herr **Mejri:** Grundlegend sehe ich durch die Gesetzgebung eine Verbesserung der Sicherheitslage für Hessen, die Kommunen und Institutionen. Der Hintergrund, warum ich das so sehe, sind der schnellere Austausch, verbesserte Kooperationsmöglichkeiten, aber auch erhöhte Koordinierung im Verbund. Das gilt für das Zentrum für Informationssicherheit, das angebundene CERT vom HMdIS, aber auch das H3C.

Mit begünstigend trifft das Ganze natürlich auch für das Lagebild mit ein. Es gibt Abwehrmöglichkeiten durch klare Befugnisse bei Auswertung und Erkennung von Sicherheitsrisiken, Schwachstellen und Schadprogrammen, der Aufbau notwendiger Befugnisse und Kompetenzen zur Abwehr von Sicherheitsrisiken, Schwachstellen und Schadprogrammen.

Wie kann das Ganze zwischen dem Zentrum und dem BSI funktionieren? Höhere Verarbeitungsgeschwindigkeit, qualifiziertere Auswertung, Fallnähe und niedrigere Reaktionszeiten durch Behörden. Die Reaktionsfähigkeit muss mit Befugnissen und Handlungsfähigkeiten gekoppelt sein. Zentrale Handlungen sollten von zentraler Stelle erfolgen. Qualifiziertes Personal muss geschaffen werden, vertraute, bewährte Prozesse müssen eingebunden werden.

Warum benötigen wir diese Gesetzgebung zum aktuellen Zeitpunkt? Ein gutes Beispiel dafür aus Hessen ist die Stadt Rodgau, die aktuell mit 50.000 Einwohnern nicht mehr in der Verfügbarkeit ist, wo alle Ämter nicht mehr funktionieren, die Kommune selbst überhaupt keinen Überblick darüber hat, wie sie sich selbst schützt, weder über die Schutzperimeter noch über die Warnungen, die im allgemeinen Bereich veröffentlicht wurden. Deshalb sitzen wir z. B. auch heute hier.

Kommunen können sich nicht selbst schützen. Dienstleister des Bundes haben ein zu niedriges Schutzniveau. Das haben wir jetzt bei der Materna festgestellt, genauso wie bei der ENIT sowie bei anderen Bund-Dienstleistern sozusagen. Viele Empfehlungen, aber keine klaren Handlungen durch Befugnisse. Die Cybercrimeaktivitäten werden nicht frühzeitig erkannt, und ihre Zahl steigt immer weiter an. Die Städte werden natürlich immer weiter durch diese Akteure bedroht und scheinen auch dieses Schutzniveau nicht halten zu können, unabhängig davon, ob sie dafür selbst verantwortlich sind oder ob es die aktuellen Institutionen von uns sind.

Wo sehen wir Bedenken? Es gibt Sachen, wo wir ganz klar sagen: Die müssen kritisch berücksichtigt oder auch hinterfragt werden. Da geht es einmal um die Datensicherheit und den Datenschutz, ganz besonders bei der Schadcodeanalyse, wenn wir über die Auswertung von personenbezogenen Daten reden. Ganz klar: Wenn so ein Schadcode analysiert wird, und dort kommen hundertfach personenbezogene Daten, die von den Angreifern – ich sage mal – exfiltriert wurden, dann muss auch geklärt werden, wie so ein Prozess erfolgen kann, um diese Daten sinnvoll und sicher auszuwerten. Im Moment ist es noch nicht so. Es wird zwar von Pseudonymisierung und Anonymisierung gesprochen, dies muss aber klarer definiert werden.

Keine falsche Nutzung der Gesetzgebung zum Missbrauch von Schwachstellen oder Sicherheitsanfälligkeiten: Wie vorhin vom Kollegen aus Aachen schon erläutert, findet eine leichte Aufweichung dieser Gesetzgebung statt. Hier benötigen wir Zuverlässigkeit in der Gesetzgebung, eine gewisse Transparenz im Umgang und befürworten auch Projekte und Programme im Bereich

Responsible Disclosure, die natürlich auch gesetzlich in irgendeiner Form mit eingebunden werden müssen, um diesen Prozess sinnvoll abzubilden.

Wir dürfen da nicht die US-Behörden als Vorbild nehmen, die Schwachstellen über ein, zwei Jahre zurückhalten, währenddessen die Opfer geschädigt werden, in der ersten Instanz die Unternehmen selbst über die Hersteller, aber auch die, die in dritter Instanz dahinterstehen und als Dritte geschädigt werden und vielleicht nichts direkt mit einem Angriff zu tun haben, wenn wir über Sicherheitslücken reden, die als Multiplikator wirken können.

Wir benötigen eine Verpflichtung für die Kommunen, damit ein gewisses Schutzniveau gehalten werden kann, damit ein Grundschutz eintrifft, eine gewisse Perimetersicherheit da ist und auch eine Verpflichtung, diesen Warnmeldungen in irgendeiner Form nachzugehen.

Dabei stellen wir uns auch eine Förderung für die Kommunen vor, weil die im Moment überhaupt nicht wissen, wie sie sich vor diesen Cyberangriffen schützen sollen und wie sie dieses Schutzniveau aufbauen sollen.

Möglichkeiten zur Amtshilfe und Kooperation: Dabei stellen wir uns Reaktionsmöglichkeiten vor, eine gewisse Verantwortung, die im Hintergrund getragen wird über die Gesetzgebung, aber auch eine gewisse Identifikation, die in diesen Prozessen stattfindet. Hier sollte konkretisiert werden. Aktuell ist die Gesetzgebung an dieser Stelle noch etwas schwammig definiert.

Weniger Handlungsempfehlungen und mehr klare Befugnisse ohne ausnutzbare Nachteile, um proaktiv zu agieren: Bestes Beispiel ist das H3C im Moment. Tagtäglich bekommen sie Fälle auf den Tisch, in denen sie handeln könnten, in denen sie Angriffe verhindern könnten, das aber aktuell aufgrund mangelnder Befugnisse nicht können. Wenn wir eine zentrale Stelle hätten, die mit solchen Bereichen kommuniziert, dann könnten wir dort natürlich diese Kommunikation einfacher aufbauen und etablieren, um etwaige Institutionen, aber auch Kommunen besser zu schützen.

Klärung der Rahmenbedingungen für Einbindung von Dienstleistern zur Gefahrenabwehr: Wir reden in der Gesetzgebung ganz klar davon, Dienstleister einzubinden oder auch nutzen zu können über die Institution. Dort muss eine klare Definition erfolgen, wie und in welchen Fällen diese Dienstleister angebunden werden können. Gewisse Use Cases sollten zumindest irgendwie vordefiniert sein, damit man weiß, wie diese genutzt werden können.

Wir brauchen eine Parallelisierung von Gesetzen außen herum. Denn allein diese Gesetzgebung wird nicht ausreichen. Wir werden an anderen Stellen Gesetze anpassen müssen oder werden sie mit einbeziehen müssen. An vielen Stellen haben wir auch im Bereich Datenschutz oder in anderen Bereichen gehört, dass es noch inkompatibel mit der Gesetzgebung und der Formulierung zum aktuellen Zeitpunkt ist.

Es muss eine Klärung von Kompetenzen erfolgen mit Bezug auf die Behörden und Institutionen, damit nicht immer dieses Kompetenzgerangel im Lagebild stattfindet und die Leute ganz klar zugewiesen werden oder auch wissen, wo die Bereiche sind, wo sie agieren können.

Wir benötigen qualifiziertes Personal. Wir können die schönste Institution aufbauen, wenn wir aber nicht das qualifizierte Personal ausbilden und auch die Anreize für das qualifizierte Personal schaffen, dann werden wir an dieser Stelle nicht weit kommen. Denn dann sitzen in so einem Lagebildzentrum drei bis fünf Leute, die diesen Anforderungen nicht gerecht werden, wie wir eben hier von linker Seite schon gehört haben. – Danke schön. Ich denke, damit habe ich alles gesagt.

Herr **Döhne:** Als Vertreter der Wirtschaft habe ich den Gesetzentwurf natürlich aus einem anderen Blickwinkel gelesen und kommentiert. Letztendlich sehe ich sehr viel Positives in dem Entwurf, z. B. die Bündelung der Kompetenzen im Zentrum für Informationssicherheit, aber auch die Klärung von Rollen und Verantwortlichkeiten. Auch natürlich das Angebot des CERT, seine Dienstleistung Privatunternehmen anzubieten, sehe ich grundsätzlich sehr positiv, wobei ich da ähnlich skeptisch bin, ob das von den Personen am Ende quantitativ und qualitativ überhaupt geleistet werden kann.

Meine weiteren Kommentierungen betreffen eher ein bisschen die operative Anwendbarkeit von verschiedenen Paragrafen und decken sich eigentlich fast 1 : 1 mit den Ausführungen der Professoren Waidner und Shulman. Auch ich sehe hier, dass man sich in manchen Paragrafen deutlich zu sehr einschränkt, beispielsweise mit reinem Verweis auf Schadprogramme, weil viele Angriffsarten dadurch direkt erst mal ausgeschlossen sind und nicht in den Paragrafen integriert sind. Viele Angriffe können aber ohne Schadprogramme genauso stattfinden.

Genauso das Thema „Protokollierung, Protokolllogs, Systemlogs“, das habe ich in meinem Kommentar aufgeführt. Die Nennung von sechs Systembereichen, für die protokolliert werden soll, greift meines Erachtens deutlich zu kurz, weil Applikationen, andere Intrusion Prevention Systeme und Ähnliches komplett außen vor sind. Darüber sollte man wirklich noch mal nachdenken: Will man das so explizit ausführen, oder kann man das etwas offener formulieren?

Eine Fragestellung betrifft in § 18 noch das Thema. Ich frage mich, warum man aus der Meldepflicht so viele Institutionen herausnimmt, gerade z. B. die Hochschulen. Wir haben in der Vergangenheit gesehen, dass gerade in diesem Bereich sehr viele Angriffe stattgefunden haben. Ich glaube, man nimmt sich eine gute Datengrundlage über Angriffe und über ein Lagebild, wenn man solche Stellen komplett von einer Meldepflicht ausschließt.

Das kann zusammengefasst einfach schon das gewesen sein, was ich eingereicht habe. Viel mehr brauche ich gar nicht ergänzen.

Herr **Lange:** In meiner Funktion als Informationssicherheitsbeauftragter der Stadtverwaltung Kassel sind meine Betrachtungen des Gesetzentwurfs aus dieser Sichtweise auf die kommunalen Aspekte fokussiert. Ich bin also so etwas wie der IT-Sicherheitshausmeister einer Kommunalverwaltung. Daher erst mal Danke dafür, dass diese kommunale Basis hier auch gehört wird.

Deutschlandweit sind 2023 bereits 13 IT-Sicherheitsvorfälle öffentlich bekannt geworden, davon drei in Hessen. Die Betonung liegt durchaus auch auf „öffentlich bekannt geworden“. Wir wissen nicht, welche anderen Fälle noch unbekannt sind. In meiner Stellungnahme stehen noch zwölf IT-Sicherheitsvorfälle. Wir haben aber gerade vor vier Tagen den Landkreis Ludwigsburg mit über 500.000 Einwohnern als neuen kommunalen IT-Sicherheitsvorfall zu verzeichnen. Im Jahr 2022 waren es 18 in Deutschland insgesamt, und 2021 sogar 32 Vorfälle in Kommunalverwaltungen. Ein tatsächliches kommunales Lagebild zur Informationssicherheit ist jedoch nicht bekannt.

Auf der anderen Seite müssen wir feststellen, dass 86 % der hessischen Kommunen nicht mehr als 20.000 Einwohner haben, 60 % nicht mehr als 10.000 Einwohner. Es gibt daher leider nur Vermutungen, wie diese bei der IT-Sicherheit tatsächlich aufgestellt sind.

Ich habe sechs Punkte ausgemacht, die meiner Meinung nach im Gesetzentwurf für die kommunale Ebene fehlen oder nicht ausreichend berücksichtigt wurden. Diese Punkte sind ein Kompromiss, wo die Verhandlungsgegner dabei zum einen mein Sachverstand waren und zum anderen die Realität. Es ist einfach, einen verbindlichen Mindeststandard – z. B. Standardabsicherung nach IT-Grundschutz – zu fordern, es ist aber unrealistisch, wenn in diesem Spannungsfeld das böse K-Wort auf der einen Seite und nur Eigenerklärungen für die Akte auf der anderen Seite in der Umsetzung erfolgen. In diesem Zusammenhang sind diese sechs Punkte für mich ein realistischer Weg, in diesem Spannungsfeld für die kommunale Ebene etwas zu bewirken.

Darüber hinaus freue ich mich, dass Frau Dr. Anja Wiesmeier, Frau Simran Mann und Herr Prof. Dr. Christoph Sorge ähnliche Aspekte für die kommunale Ebene benannt haben und auch ähnliche Dinge empfehlen. – Ich danke für die Aufmerksamkeit.

Vorsitzender: Dann gäbe es jetzt für die Abgeordneten Gelegenheit, Nachfragen an diese fünf Persönlichkeiten zu stellen.

Abg. **Heike Hofmann (Weiterstadt):** Ich habe zunächst eine Frage an die Evolution Security GmbH, anlehnend an die Stellungnahme des Städtetags. Sie haben einige Punkte aus Ihrer praktischen Erfahrung – Umgang, Unterstützung der Kommunen – gebracht. Mich würde noch mal der Punkt „Aus- und Fortbildung der Kommunalbeamten oder Mitarbeiter“ aus Ihrer Expertise interessieren. Es ist – Sie haben es angerissen – eine zentrale Aufgabe, da immer auch auf der kommunalen Seite aus- und fortgebildet zu sein. Was wünschen Sie sich das sozusagen aus praktischer Sicht?

Herr Lange, Sie haben jetzt ja sehr straff berichtet. Sie haben eine Meldepflicht für Kommunen von IT-Sicherheitsvorfällen und die Pflicht für Kommunen zur Erstellung einer Leitlinie zur Informationssicherheit gefordert. Verstehe ich Sie richtig, dass Ihnen da der Gesetzentwurf nicht weit genug geht?

Und die zweite Frage: Würde das von Ihnen geforderte System zur Meldung von IT-Sicherheitsvorfällen für Kommunen mehr Licht ins Dunkelfeld der IT-Sicherheitsvorfälle bringen?

Vorsitzender: Dann schaue ich noch mal in den Kreis der Abgeordneten, ob es noch Nachfragen gibt. – Das ist nicht der Fall. Dann haben zur Antwort zunächst die Evolution Security GmbH und dann Herr Lange das Wort.

Herr **Mejri:** Grundlegend würde ich erst mal dazu sagen, dass man dem natürlich mit Schulungen und Workshops entgegenwirken sollte. Aber das allein reicht nicht. Das heißt, auch vom Bund aus, auch von Hessen aus muss natürlich über die Ministerien eine gewisse Awareness an die einzelnen Kommunen herangetragen werden, damit sich diese dem überhaupt erst mal bewusst werden. Denn wenn ich z. B. in einzelne Kommunen hineingehe und frage, ob dort Schulungen stattgefunden haben, dann ist es in den meisten Fällen so, dass sie sich dem noch nicht mal bewusst sind. Um erst mal dieses Bewusstsein aufzubauen, kann man denen nicht einfach Schulungen aufzwängen, sondern man muss erst mal eine gewisse Sensibilisierung über das Land betreiben, über das Bundesland, sage ich jetzt mal, damit das auch bei den jeweiligen Kommunen ankommt, weil die meistens erst dann aufwachen, wenn die ganze Stadt – ich sage jetzt mal – nicht mehr verfügbar ist oder komplett verschlüsselt wurde. – Beantwortet das die Frage?

Abg. **Heike Hofmann (Weiterstadt):** Das wäre ein eigenes abendfüllendes Thema. Aber ich glaube, die Botschaft ist angekommen, dass man erst mal so eine Art Boden bereiten muss und dann ansetzen muss, aber auch mit Unterstützung des Landes. So habe ich Sie jetzt verstanden, oder?

Herr **Mejri:** Richtig. Ansonsten wären sie sich ja jetzt schon im Klaren, dass sie Schulungen machen müssten und würden das tun. Das tun sie aber im Moment gerade nicht. Deshalb ist es wichtig, dass das in irgendeiner Form über das Land kommuniziert wird.

Herr **Lange:** Grundsätzlich sehe ich genau in diesen zwei Punkten, die ja zwei meiner sechs Punkte sind, Defizite. Sie sind also nicht in dem Gesetzentwurf enthalten. Eine Meldepflicht halte

ich für fundamental. Denn nur wenn ich weiß, wie die Lage ist, kann ich auch entsprechende Maßnahmen daraus ableiten und Vorsorge treffen.

Bereits in der Cybersicherheitsstrategie 2013 des Bundes war aufgeführt, dass das kommunale Lagebild einen weißen Fleck darstellt und dass das BSI aufgefordert war, dort entsprechend ein Lagebild zu erstellen. Das BSI war dazu nicht in der Lage. Das hat sicherlich auch viel mit unseren föderalen Strukturen – Bund, Länder und Kommunen – zu tun. Daher halte ich diese Meldepflicht für unbedingt notwendig. Ich glaube auch, dass die Strukturen dafür an der Zentralstelle möglich sind, zumal die ja auch für die Landesbehörden aufgebaut werden müssen.

Das Zweite: Die Forderung einer Leitlinie für Informationssicherheit auch bei den Kommunen habe ich deswegen mit aufgenommen, damit sich auch die Kommunen und die Behördenleitungen zu dem Thema Informationssicherheit positionieren. Das heißt, ich würde gar nicht mal fordern, dass dort von vornherein ein Mindeststandard vorgegeben wird. Das wäre sicherlich wünschenswert. Ich halte das aber durchaus für nicht ganz realistisch. Doch ist es wichtig, dass die Behördenleitungen der Kommunen verstehen, welche Pflichten und welche Notwendigkeiten bei der Informationssicherheit bestehen. Und sie müssen sich über eine Leitlinie zu diesem Thema positionieren. Damit entsteht auch gleichzeitig eine Sensibilisierung.

Vorsitzender: Es gibt zwei weitere Wortmeldungen, einmal von Herrn Felstehausen und dann von Herrn Gaw.

Abg. **Torsten Felstehausen:** Meine Frage geht an Frau Krohn von LOAD e. V. In Ihrer Stellungnahme empfehlen Sie, die Zusammenarbeit mit Polizei, Strafverfolgungsbehörden und – ich nehme mal an – auch dem Landesamt für Verfassungsschutz, wie Sie schreiben, sehr genau zu spezifizieren. Ich kann mir dabei jetzt zwei Szenarien vorstellen. Das eine ist, dass sich aus einem IT-Sicherheitsvorfall ein Strafverfolgungsinteresse ergibt. Das ist sozusagen die eine Variante, wo dann der IT-Sicherheitsvorfall selbst zum Gegenstand von Strafverfolgungsermittlungen gemacht wird, um die Verursacher möglicherweise ihrer Strafe zuzuführen. Das andere wäre aber natürlich, dass sich die Polizei oder das LfV den Kompetenzen der neuen Stelle bemächtigt und dort sozusagen im Rahmen von – wie könnte man das nennen? – einer Sicherheitspartnerschaft dann tätig wird.

Können Sie uns mal Ihre Vorstellung beschreiben, wie man dort eine Firewall einrichten müsste? Denn aus der Sicht von Bürgerrechten, aus der Sicht einer verantwortungsvollen Netzpolitik müsste dort ja genau so etwas eingerichtet werden.

Abg. **Dirk Gaw:** Ich habe eine weitere Frage zu dem Thema Schulungen. Wie hoch schätzen Sie denn den Aufwand ein, um zunächst einmal ein gewisses Niveau, also Qualitätsniveau zu erreichen? Dann ist es wahrscheinlich auch ein fortlaufender Prozess. Es ist ja nicht irgendwann abgeschlossen. Es muss wahrscheinlich ständig wiederholt werden, um das dann auch zu halten.

Frau **Krohn:** In der Tat ist das ein sehr wichtiges Thema. Ich habe eben noch gedacht, ich ärgere mich, dass ich das nicht selbst angesprochen hatte, weil das natürlich auch mit dem, was der Kollege von der EBS vorhin gesagt hat, sehr zusammenhängt, dass es gar keine Notwendigkeit zu geben scheint, darauf zu verweisen, dass wir sozusagen aus den Grundrechten zitieren müssen in diesem Gesetz. Das ist so interessant, weil uns bei unserer Lektüre genau das alarmiert hat. Wenn sich der Gesetzgeber hier überlegt hat, darauf zu verweisen, dass wir per se Grundrechtseinschränkungen vornehmen, dann haben wir daraus gelesen, dass das tatsächlich auch die Absicht ist. Wenn das die Absicht ist, ist natürlich die Frage, an welcher Stelle. Denn wir haben heute auch schon verschiedentlich gehört, wenn wir nach Schadsoftware scannen usw., werden uns natürlich auch personenbezogene Daten offenbart. Das passiert ja, okay. Aber das ist halt nicht der Normalfall. Wenn allerdings aus der Behörde – – Das war meine letzte Anmerkung, was die Behörde eigentlich tun soll, oder an welcher Stelle sie, um mich selbst noch mal zu zitieren, eine eierlegende Wollmilchsau werden soll. Wir, LOAD, verwahren uns ganz entschieden dagegen, dass wir hier Polizeiarbeit oder erweiterte Polizeiarbeit machen, um tatsächlich eine Umgehung der Regelung zu finden, dass sich Polizeiarbeit auch nicht mit nachrichtendienstlicher Tätigkeit und dergleichen diffundieren soll.

Wir haben im Moment die Debatte mit Palantir, wo wir sehen, dass Daten sozusagen über Umwege so diffundiert werden, dass diese Aufteilung der Sicherheitsbehörden nicht mehr gewährleistet ist. Wir haben das vorher schon mal gesehen bei der Einrichtung der ZITiS, dieses zentralen Instituts für – – Ich muss mal gucken, wie das ausgeschrieben wird. Aber die ZITiS ist eben so eine komische Nicht-Behörde, die nicht nur Sicherheitslücken offenlässt, sondern tatsächlich die Trennung von Polizei und Nachrichtendiensten aufweicht. Das ist der Grund, warum bei uns hier die Alarmglocken angegangen sind, dass wir gesagt haben: Haben wir es hier mit einem Institut zu tun, das versucht, Schlupflöcher zu finden für Dinge, die Polizeiarbeit möglicherweise erleichtern, aber aus bürgerrechtlicher Sicht nicht diskutabel sind?

Herr **Mejri:** Zum Aufwand für die Schulungen: Dort hat man verschiedene Abhängigkeiten. Man hat einmal das Finanzielle. Man hat einmal das Personal. Man hat einmal die Zeit und natürlich auch das Wissen, was man benötigt. Jetzt ist es so: In den Kommunen existiert dieses Personal nicht, um die Ressource selbst aufzubauen, um sich selbst in diesem Bereich zu schulen. Da sind wir schon wieder bei dieser Klärung für externe Dienstleister oder aber auch für die Verantwortung des CISO, der dann hinzugezogen wird, um gegebenenfalls diese Leute in den Kommunen abzuholen.

Anders wird es wahrscheinlich nicht funktionieren, weil wir jetzt schon wissen, dass die Leute in den Kommunen mit ihrem Personal am Anschlag sind, wo man die Leute nicht mal für irgendwie ein, zwei Tage abziehen kann, um sie dann in solche Schulungen zu überführen. Das heißt, man müsste sich auch auf Landesebene hinsetzen und entscheiden, wie man das zukünftig regeln will und was eine sinnvolle Mechanik dahinter ist, um das diesen Kommunen über Externe zukommen zu lassen.

Da ist dann auch wieder die Frage: Hat man im Bundesland die Ressource, oder muss man gegebenenfalls wieder auf externe Bereiche zugreifen, die dieses Wissen haben, die die Zeit aufbringen können, um diese jeweiligen Kommunen dann auch – ich sage mal – auf das Schutzniveau anzuheben, wie Schulungen, Workshops oder Awarenessveranstaltungen?

Vorsitzender: Die Frage ist auch beantwortet. Es liegen keine weiteren Fragen an die Anzuhörenden vor. Ich darf Ihnen allen noch mal ganz herzlich für die Mitwirkung heute danken. Den einen oder anderen sehen wir bestimmt bei anderen Gelegenheiten wieder.

Die Sitzung ist geschlossen.

Beschluss:
INA 20/84 – 15.05.2023

Der Innenausschuss hat zu dem Gesetzentwurf eine öffentliche mündliche Anhörung durchgeführt.

Wiesbaden, 1. Juni 2023

Protokollführung: Vorsitz:

Claudia Lingelbach Christian Heinz