Redner zu nachfolgendem Tagesordnungspunkt

Erster Vizepräsident Tobias Reiß
Staatsminister Albert Füracker
Abg. Florian Köhler
Abg. Dr. Stefan Ebner
Abg. Benjamin Adjei
Abg. Tobias Beck
Abg. Florian von Brunn
Abg. Andreas Jurca

Erster Vizepräsident Tobias Reiß: Ich rufe **Tagesordnungspunkt 1 b** auf:

Gesetzentwurf der Staatsregierung
zur Änderung des Bayerischen Digitalgesetzes und des Gesetzes über die Bayerische Landesstiftung (Drs. 19/2591)
- Erste Lesung -

Begründung und Aussprache werden miteinander verbunden. Die Staatsregierung hat 14 Minuten Redezeit. Zugleich eröffne ich die Aussprache. Die Gesamtredezeit der Fraktionen beträgt 29 Minuten. – Ich erteile Herrn Staatsminister Albert Füracker das Wort.

Staatsminister Albert Füracker (Finanzen und Heimat): Lieber Herr Präsident, sehr geehrte Damen und Herren, Kolleginnen und Kollegen! Es geht um die sichere IT-Infrastruktur und die Cyberabwehr. Das sind große Themen für unsere staatliche Verwaltung sowie für die Strafverfolgung, die Kommunen und die Unternehmen. In Bayern haben wir einen hohen Digitalisierungsgrad in unserer Verwaltung. Deswegen haben wir uns schon längst entschlossen, einen besonderen Weg zu gehen. Bayern hat als erstes Bundesland eine eigene Fachbehörde eingerichtet.

Schon im Jahr 2017 wurde das Landesamt für Sicherheit in der Informationstechnik eingerichtet. Das kommt uns heute zugute. Das LSI arbeitet sehr erfolgreich. Mittlerweile hat es 150 Mitarbeiterinnen und Mitarbeiter. Das LSI hat die Aufgabe, staatliche Behörden vor Cyberangriffen zu schützen. Wir treten auch als hoch kompetente Unterstützer und Berater für die Kommunen und Betreiber kritischer Infrastrukturen auf. Das LSI ist gleichsam das Pendant zum BSI, dem Bundesamt für Sicherheit in der Informationstechnik. Mittlerweile hat es sich in Bayern etabliert. Ich bin sehr froh, dass wir es haben.

Im Übrigen gibt es viel zu tun. Das LSI analysiert im Sicherheitsmonitoring täglich 2,5 Milliarden Datensätze. Täglich werden 1,4 Millionen E-Mails mit Schadcode gefiltert. Das LSI hat bereits Ende 2023 mit den Angeboten rund 94 % der Kommunen er-

reicht. Warum ist es jetzt so bedeutsam? – Durch die Neuerung, die jetzt in eine gesetzliche Form gebracht werden muss, müssen wir nicht bei null beginnen. Stattdessen kommen wir mit einer Ergänzung des Digitalgesetzes zurecht. Es geht um die Umsetzung der sogenannten NIS-2-Richtlinie. Das ist natürlich etwas für Feinschmecker. Es handelt sich um eine Richtlinie der Europäischen Union, die nichts anderes zum Ziel hat, als das gemeinsame Cybersicherheitsniveau in der EU zu stärken. Diese Richtlinie betrifft vor allen Dingen Unternehmen und muss vorrangig durch den Bund umgesetzt werden. Das ist wahr. Der Bund führt jedoch im Rahmen der Gesetzgebung eine Länder- und Verbändeanhörung durch. Die zeitliche Perspektive ist unklar. Für uns ist das – das sage ich in aller Offenheit – nicht entscheidend. Wir müssen in jedem Fall, wie jedes andere Bundesland auch, unsere eigene Gesetzgebung anpassen.

In den Anwendungsbereich der Richtlinie fallen auch die öffentlichen Verwaltungen. Im Übrigen hat der Bund für die bayerischen Behörden keine Gesetzgebungskompetenz. Deswegen machen wir uns unabhängig von der Zeitschiene des Bundes auf den Weg und setzen die NIS-2-Richtlinie in Landesrecht um. Die Notwendigkeit einer gesetzlichen Regelung besteht. Wir passen bereits bestehende Vorschriften zur IT-Sicherheit einfach an. Es besteht eine hohe Übereinstimmung. Im Hinblick auf die NIS-2-Richtlinie besteht anders als bei vielen anderen EU-Richtlinien kein Anlass, in großes Geschrei zu verfallen. Die Regelung ist nicht ideal und sehr auf Unternehmen zugeschnitten. Unser Gesetzentwurf befasst sich mit der Umsetzung insbesondere für die Verwaltungen.

Wir machen eine Eins-zu-eins-Umsetzung. Wir praktizieren kein Gold Plating von EU-Recht, wie es der Bund so gerne betreibt. Das kann man dem Gesetzentwurf nicht nachsagen. Wir sind gut aufgestellt. Ich sprach es an. Wir müssen aber die EU-Vorgaben erfüllen. Die EU verlangt, in Zukunft in jedem Land ein Computer Security Incident Response Team einzurichten. Meine Damen und Herren, das hört sich toll an, das haben wir aber schon längst. Früher hieß das bei uns Bayern-CERT, jetzt heißt es LSI.

Das ist also kein Problem. Die Fachbehörde LSI existiert. Wir werden die Aufgaben dieser Aufsichtsbehörde im LSI bündeln, wie es die Richtlinie fordert. Durch unser bereits hohes Sicherheitsniveau werden wir zusätzliche Bürokratie auch in Grenzen halten können. Eine gute Zusammenarbeit zwischen dem LSI und dem BayernServer ist vorhanden.

Wir haben vor, die europarechtlich vorgegebenen Aufsichts- und Durchsetzungsbefugnisse gegenüber allen erfassten Behörden im LSI zu bündeln. Fazit: Die Entscheidung, das LSI zu gründen, war eine wirklich wichtige und zukunftsweisende Entscheidung. Somit ist die Umsetzung der Richtlinie keine große Herausforderung für uns. Wir haben eine gewisse Vorreiterfunktion. Im Hinblick auf die IT-Sicherheit sage ich immer: Es geht nicht darum, dass sich jemand als zuständiger Minister hinstellt.

(Toni Schuberl (GRÜNE): Wo ist der Digitalminister?)

Wenn man für die IT-Sicherheit des Freistaats Bayern Verantwortung trägt, stellt sich jeden Tag die Frage: Was kann man machen, damit die IT-Sicherheit intensiver gewährleistet ist? Insoweit ist die Zuständigkeit in meinem Geschäftsbereich für das Landesamt für Sicherheit und Informationstechnik von jeher gegeben. Diese werden wir auch wahrnehmen. Wir können zusagen, alles Menschenmögliche zu tun, aber zu versprechen, dass niemandem irgendetwas passieren könnte, wäre vermessen. Das mache ich sicher nicht. Aber ich kann zusagen, dass wir das aus unserer Sicht Menschenmögliche tun, um die IT-Sicherheit bei uns zu gewährleisten.

Wir habe noch ein Update für die Bayerische Landesstiftung an dieses Gesetz angehängt. Dabei geht es darum – ich würde sagen, dass das mehr eine Formalie ist –, dass die Bayerische Landesstiftung, wie es auch während der Pandemie der Fall war, in Sitzungen in Form von Video- und Telefonkonferenzen handeln und Beschlussfassungen im Umlaufverfahren durchführen kann. Während der COVID-Pandemie sind gute Erfahrungen damit gemacht worden. Deswegen besteht der Wunsch, dass man das Ganze in Gesetzesform fixiert. Das können wir gerne machen.

Es gibt eine weitere Änderung, und zwar für die Rechnungslegung der Bayerischen Landesstiftung: Es gilt künftig eine Frist von 9 statt bisher 6 Monaten. Das gilt auch für alle anderen Stiftungen in Bayern.

Diese Änderungen machen die Bayerische Landesstiftung agiler, schaffen überflüssige Sonderregelungen ab und entbürokratisieren gleichsam. Es ist daher aus meiner Sicht kein Problem, sowohl der Änderung des Digitalgesetzes als auch der Regelung zur Landesstiftung zuzustimmen. Das Ganze kommt jetzt dann in die Ausschüsse. Ich bitte um eine positive Beratung, eine positive Beschlussfassung und somit Zustimmung zum Gesetzentwurf.

(Beifall bei der CSU und den FREIEN WÄHLERN)

Erster Vizepräsident Tobias Reiß: Danke, Herr Staatsminister. – Der nächste Redner ist der Kollege Florian Köhler.

(Beifall bei der AfD)

Florian Köhler (AfD): Sehr geehrter Herr Vizepräsident, sehr geehrte Kollegen, sehr geehrte Damen und Herren auf der Besuchertribüne! Das Ziel des vorgelegten Gesetzes ist es, ein hohes Cybersicherheitsniveau in der EU und ihren Mitgliedstaaten zu gewährleisten. Im Wesentlichen wird die NIS-2-Richtlinie der Europäischen Union auf Landesebene umgesetzt. Bayern hat bei der Umsetzung tatsächlich einen sehr geringen Umsetzungsspielraum. Der Freistaat hat mit dem Landesamt für Sicherheit in der Informationstechnik – LSI – bereits den Grundstein gelegt, das wurde eben schon angesprochen. Der Freistaat hat bereits eine entsprechende Behörde gegründet. Diese wird nun in einigen Fällen – ich sage mal – mit mehr Befugnissen ausgestattet. Wobei ich sagen muss, dass diese Ausdrucksweise ein bisschen zu hoch gegriffen ist. Im Wesentlichen sorgt die Novellierung erst mal für mehr Klarheit, um angemessene Reaktionen auf Angriffe sicherzustellen. Neben deutlicheren Formulierungen bei Rechtsbegriffen und neben ein paar redaktionellen Änderungen gibt es zusätzliche sprachli-

che Angleichungen. Wir sind immer ein Freund von klaren, bestimmten und unmissverständlichen Formulierungen.

Im Fokus steht auch das bereits angesprochene Computer Security Incident Response Team. Auch das wurde bereits vom Freistaat eingerichtet und untersteht dem LSI. Eine wesentliche Änderung bezieht sich auf die Speicherfrist von Protokolldaten, die das LSI erhebt: Diese soll von 12 auf 18 Monate verlängert werden – aber auch darüber kann man diskutieren. Auf der einen Seite sehen wir durch die Verlängerung der Speicherfristen von Protokolldaten eine gewisse Praktikabilität, aber auf der anderen Seite könnte das auch zu einem Datenschutzproblem führen, insbesondere im Hinblick auf personenbezogene Daten.

Wir müssen uns noch ein finales Urteil über das dreistufige Meldeverfahren bilden; denn die Einführung neuer Melde- und Berichtspflichten könnte den Verwaltungsaufwand erheblich erhöhen, ohne dass klare Mehrwerte entstehen.

Im Gegensatz zur Staatsregierung sehen wir durchaus, dass die EU-Richtlinie am Ende des Tages wahrscheinlich für einen erhöhten Verwaltungsaufwand insgesamt sorgen wird, ganz zu schweigen davon, was auf die Unternehmen zukommen wird. Dafür ist – das ist bereits angesprochen worden – der Bund, also die Ampel zuständig. Vermutlich wird das also noch schlechter gemacht für Unternehmen.

Die noch nicht verabschiedeten Rahmenbedingungen auf Bundesebene könnten zu weiteren notwendigen Anpassungen und möglicher Rechtsunsicherheit führen. Aber wie der Herr Minister gerade schon gesagt hat, müssen wir abwarten und Tee trinken, und anschließend können wir entsprechend reagieren.

Die Regelungen des Stiftungsgesetzes sind an sich sehr praxisorientiert. Ich nenne nur als Beispiel die Ermöglichung von Umlaufbeschlüssen. Das ist durchaus sinnvoll.

Zum Schluss bleibt noch die Kostenfrage: Obwohl die Änderungen als kostenneutral dargestellt werden, werden versteckte Kosten gerade beim LSI bzw. den anderen Ver-

waltungsbehörden durch notwendige Schulungen und Infrastrukturmaßnahmen entstehen. Das ist einfach so. Wir werden die Argumente im Ausschuss genau analysieren und uns dann eine abschließende Meinung bilden.

(Beifall bei der AfD)

Erster Vizepräsident Tobias Reiß: Vielen Dank. – Der nächste Redner ist der Kollege Dr. Stefan Ebner.

Dr. Stefan Ebner (CSU): Herr Präsident, meine sehr verehrten Kolleginnen und Kollegen, sehr geehrte Damen und Herren! Ich möchte meine Rede heute mit etwas Positivem beginnen, weil wir heute Bayern sicherer machen können. Wir können heute Bayern cybersicherer machen. Das ist wichtig, weil die Cyberkriminalität jedes Jahr weiter zunimmt. Jedes dritte Unternehmen in Deutschland ist in den letzten zwei Jahren Opfer von Cyberattacken geworden. Der wirtschaftliche Schaden ist enorm: Er liegt bei 150 Milliarden Euro pro Jahr. Deswegen müssen wir in unserer digitalen Welt verteidigungs- und wehrfähiger werden. Bayern wird täglich angegriffen. Bayern muss sich täglich verteidigen, aber nicht nur Bayern, sondern auch Deutschland und Europa. Deswegen haben der Europäische Rat und das Europäische Parlament richtig entschieden, die Cybersecurity in unserem Heimatkontinent auf ein neues, höheres Niveau zu heben.

Meine Damen und Herren, die Menschen und die Unternehmen erwarten zu Recht, dass sie vor Einbruch, Diebstahl, Sabotage und Erpressung geschützt werden. Sie erwarten das nicht nur in der analogen Welt, sondern auch in der digitalen Welt. Ich will betonen, dass die Europäische Volkspartei – die EVP – unter dem Vorsitz von Manfred Weber dieses Thema federführend vorangetrieben hat, damit Europa stärker vor Cyberangriffen geschützt wird.

Wir sehen im Übrigen auch, dass die Thematik ein gutes Beispiel dafür ist, wie wichtig europäische Zusammenarbeit ist. Ich will eine Randbemerkung in die rechte Richtung machen, zu Ihrem Freund Björn Höcke. Dieser sagt, dieses Europa muss sterben.

(Zuruf von der AfD: Die EU! Mein Gott!)

Nein, dieses Europa wird nicht sterben, ganz im Gegenteil. Auf europäischer Ebene müssen wir dafür sorgen, dass wir die Menschen noch stärker schützen. Gerade solch große Probleme und Herausforderungen sind europäisch zu lösen; sie können nur europäisch gelöst werden.

Ich komme nun zurück zur Mitte Europas, zurück nach Bayern. Unser Staatsverständnis ist klar, unser Staatsverständnis heißt: Sicherheit und Ordnung für die Bürger herstellen. Bayern ist exzellent aufgestellt – der Minister hat das ausführlich dargestellt – mit IT-Spezialistinnen und -Spezialisten, bei der Polizei, beim Verfassungsschutz, bei der Justiz und beim Landesamt für Sicherheit in der Informationstechnik. Dieses Landesamt macht seit sechs Jahren einen ganz tollen Job bei der Abwehr von Cybergefahren. Ich möchte das Ganze konkret machen: Im Jahr 2022 sind 4.000 Angriffe auf das Bayerische Behördennetz unternommen worden. Das sind im Durchschnitt 11 Angriffe pro Tag. Wir werden heute lange tagen, wahrscheinlich bis 23 Uhr. Das heißt, bis zum Ende unserer Sitzung werden wahrscheinlich 5 Angriffe auf das Bayerische Behördennetz erfolgen. Das Gute dabei ist, dass es bei den Angriffen wahrscheinlich genauso sein wird wie bei den letzten 4.000 Mal, dass kein einziger dieser Angriffe durchkommen wird.

Deswegen möchte ich an dieser Stelle den 150 IT-Sicherheitsexpertinnen und -experten am Landesamt für Sicherheit in der Informationstechnik, die Bayerns IT schützen, ein herzliches Dankeschön aussprechen. Auf dem Cyberschlachtfeld sind sie die Cyberarmee des Freistaates.

(Beifall bei der CSU)

Ja, so ist es: Bayern nimmt eine Vorreiterrolle beim Thema Cybersecurity ein. Das ist das bayerische Staatsverständnis von Ordnung und Sicherheit. Das gilt analog, und das gilt digital.

Meine Damen und Herren, diese Art von Politik ist deswegen so wichtig, weil wir uns nicht sicher sein können, dass wir alle in der Politik an einem gemeinsamen Strang ziehen. Ich schaue wieder zu Ihnen nach rechts, meine Damen und Herren von der AfD. Mit Ihnen ist kein glaubwürdiger Kampf gegen die Cyberkriminalität zu führen. Bei Ihnen weiß man nicht, auf welcher Seite Sie stehen. Die Mehrheit der Cyberangriffe kommt aus China, Russland, Nordkorea und dem Iran. Das heißt, ein Drittel der Cyberangriffe kommt aus Staaten, die gegen den Westen gerichtet sind. Ich frage Sie: Wie soll denn eine politische Partei glaubwürdig im Kampf gegen Cyberangriffe aus China und Russland sein, wenn einige Leute seit Monaten im Verdacht stehen, sich genau von diesen Ländern schmieren zu lassen?Ich frage mich schon ernsthaft, wie so eine Partei in ihrem Namen behaupten kann, sie sei für Deutschland.

(Florian von Brunn (SPD): Abstieg für Deutschland: AfD!)

Meine Damen und Herren, so wenig, wie Sie eine Alternative sind, so wenig sind Sie offenbar für Deutschland. Meine Damen und Herren, aber unabhängig davon ist es die ureigenste Aufgabe politischer Verantwortungsträger, enge Verbindungen ins Ausland aufzubauen, Verbindungen zu pflegen oder auszubauen.

(Florian von Brunn (SPD): Alles andere, aber nicht für Deutschland! – Widerspruch bei der AfD)

Das müssen dann Verbindungen im Interesse des eigenen Landes und nicht im Interesse der anderen sein. Im globalen Cyberkampf braucht es Soldaten und keine Söldner, meine Damen und Herren.

Wir sprechen aber über den Kampf gegen Cyberkriminalität. Da würde man sich auch ein bisschen mehr Engagement vom linken Rand des Parlaments wünschen. Nehmen wir die GRÜNEN: Ähnlich wie bei vielen anderen Themen sind die GRÜNEN manchmal zu naiv, ein bisschen zu zurückhaltend, ein bisschen zu bürokratisch, ein bisschen zu langsam. Man sieht es auch: Das Gesetz muss bis zum 17. Oktober 2024 in natio-

nales Recht umgesetzt werden. Auf Bundesebene ist in dem Bereich immer noch nichts entstanden.

(Florian von Brunn (SPD): Das stimmt doch überhaupt nicht! Sie sind nur nicht informiert! Das ist das Problem!)

Wären manche Grüne im Kampf gegen Cyberattacken engagierter, könnte man Viren und Trojaner zu einer Tüte drehen, meine Damen und Herren.

(Florian von Brunn (SPD): Meine Güte!)

Aber Hacker lösen sich nicht in Rauch auf. Hackern muss man das Handwerk legen, meine Damen und Herren.

Lassen Sie mich zum Schluss kommen: Mit der heutigen Debatte und der Ersten Lesung beschließen wir noch mehr Sicherheit für Bayern. Wir setzen eine EU-Richtlinie um. Wir setzten sie eins zu eins um, das heißt, ohne ein Mehr an Bürokratie und ohne Extras. Der Freistaat rüstet sich und präpariert sich, und das alles unter dem Dach des Staatsministers der Finanzen und für Heimat Albert Füracker. Bei ihm ist das Thema Cyberkriminalität in besten Händen. Ich bitte Sie, diesen Gesetzentwurf zu unterstützen.

(Beifall bei der CSU – Zuruf des Abgeordneten Martin Böhm (AfD))

Erster Vizepräsident Tobias Reiß: Vielen Dank, Herr Kollege. – Als Nächstem erteile ich dem Kollegen Benjamin Adjei das Wort.

Benjamin Adjei (GRÜNE): Herr Präsident, liebe Kolleginnen und Kollegen! Beim Finanzminister ist das Thema Cyberkriminalität in besten Händen – nur ärgerlich, dass wir einen Digitalminister haben. Lieber Fabian, ich bin mir aber sicher: Du versuchst auch irgendwie dein Bestes, in internen Gesprächsrunden bei der Digitalisierung mal etwas bewegen zu können; denn die Digitalisierung in Bayern und in Deutschland schreitet immer weiter voran. Wir wollen, wie ihr in der Staatsregierung es euch auf die

Fahnen geschrieben habt, unsere Staatsverwaltung modernisieren und digitalisieren. Dann müssen wir natürlich dafür sorgen, dass die Verwaltung am Ende resilient gegenüber Angriffen von außerhalb ist und ihnen standhalten kann, um die Staatsverwaltung zu sichern, aber auch die Bürgerinnen und Bürger zu schützen.

Gerade ist schon ausgeführt worden: Die Zahl der Angriffe nimmt zu. Das BSI hat für das letzte Jahr eine Steigerung der Zahl der Angriffe um 28 % gemessen, vor allem aus dem Ausland. Die Angriffe kommen weniger von innen heraus, sondern mehr aus dem Ausland, insbesondere aus China und Russland. Da ist es wichtig und richtig, dass die EU sich jetzt auf den Weg macht, das Thema Cybersecurity mit der NIS-2-Richtlinie zu stärken. Die EU möchte flächendeckend hohe Standards ansetzen. Dabei muss sie die verschiedenen Regelungen in den Mitgliedstaaten der Europäischen Union harmonisieren; denn ich glaube, auch mit Blick auf Unternehmen ist es ganz essenziell, dass es nicht in jedem Land andere, sondern einheitliche, gleiche und gute Regeln gibt. Hier ist der Bund auf dem Weg. Er ist etwas verspätet, das stimmt, aber er ist auf dem Weg, das umzusetzen. Die Bayerische Staatsregierung setzt auf Landesebene das um, was hier umzusetzen ist.

Lieber Albert Füracker, ich habe es bei der Haushaltsdebatte schon gesagt: Natürlich lobe ich auch das, was in Bayern gut läuft. Damals habe ich auch das LSI hervorgehoben. Das ist eine Errungenschaft des Freistaates, die es in keinem anderen Bundesland gibt. Jetzt hat es sich wieder bewährt, weil viele der Regelungen, die eingeführt werden müssen, sehr einfach durch kleine Gesetzesänderungen ohne das Einführen neuer Behörden und Strukturen umgesetzt werden können. Ich habe selber schon das Bayern-CERT am LSI besucht. Das ist wirklich eine sehr gute Institution. Entsprechend gut ist es, das weiterzuführen und auszubauen.

Bei allem Lob gibt es aber natürlich auch ein bisschen Kritik: Die richtet sich nicht rein an die Bayerische Staatsregierung, sondern eigentlich an den IT-Planungsrat insgesamt. Die Bundesländer haben sich nämlich entschieden, nicht alles aus der NIS-2-Richtlinie umzusetzen, insbesondere die Kommunen nicht mit aufzunehmen. Das

halte ich für einen großen Fehler. Die Kommunen sind das Rückgrat unserer Staatsverwaltung. Insbesondere, wenn es um die Digitalisierung der Kommunal- oder der Staatsverwaltung geht, wird sehr viel von den Kommunen umgesetzt werden müssen. Gleichzeitig nehmen die Angriffe auf Kommunen massiv statt.

(Bernhard Pohl (FREIE WÄHLER): Zu!)

– Sie nehmen massiv zu. Das BSI hat letztes Jahr 27 Angriffe auf Kommunalverwaltungen gemessen. 6 Millionen Menschen in Deutschland leben in diesen betroffenen Kommunen. Das ist die Hälfte der bayerischen Bevölkerung. Das muss man sich wirklich mal vorstellen, wie viele Menschen allein im letzten Jahr betroffen waren. Ich schaue mir die Steigerungsraten an: Die werden in den nächsten Jahren massiv zunehmen. Ich glaube, es wäre insbesondere mit Blick auf die Daseinsvorsorge fatal, hier die Kommunen jetzt komplett rauszunehmen und zu sagen: Nein, wir geben euch nicht die hohen Sicherheitsstandards und die Auflagen und natürlich dann, damit verbunden, auch nicht die Unterstützung bei der Umsetzung.

Ich selber stamme aus dem Landkreis Miesbach. Vielleicht kennt der eine oder andere das Krankenhaus Agatharied. Das arbeitet nämlich im Moment analog, offline. Warum arbeitet es analog und offline? – Weil es vor zwei Wochen Opfer eines großen Cyberangriffs geworden ist. Es ist das einzige Kreiskrankenhaus in dem Landkreis und auch noch Mitversorgungskrankenhaus für die benachbarten Landkreise. Die müssen im Moment alles analog machen, weil alle Systeme, übrigens inklusive der Schrankensteuerung an den Zuwegen zu dem Krankenhaus, wegen des Angriffs abgeschaltet werden mussten. Ich glaube, das zeigt ganz deutlich, wie wichtig es ist, die Kommunen in der IT-Sicherheit stärker mit in die Pflicht zu nehmen, aber auch entsprechend zu unterstützen. Da hätte ich mir vom Freistaat Bayern mehr Drive gewünscht.

Die anderen Bundesländer haben gesagt, sie halten die Kommunen da auch raus. Sonst sagt Bayern eigentlich auch immer: Es ist uns doch egal, was die anderen Bundesländer sagen. Wir gehen voran. Wir machen mehr. Wir gehen weiter. – Das würde

ich mir in dem Fall auch wünschen. Vielleicht kommt da noch ein Änderungsvorschlag, vielleicht von den FREIEN WÄHLERN, die die Themen des modernen Staates und der Kommunen für sich so hoch proklamieren.

(Felix Locke (FREIE WÄHLER): Von euch kommt da wohl nichts, oder?)

– Vielleicht kommt da von euch noch etwas. Darüber würde ich mich freuen.

(Beifall bei den GRÜNEN)

Erster Vizepräsident Tobias Reiß: Nächster Redner ist der Kollege Tobias Beck.

Tobias Beck (FREIE WÄHLER): Sehr geehrter Herr Präsident, werte Kolleginnen und Kollegen, liebe Besucherinnen und Besucher! Täglich erreichen uns Berichte über Cyberangriffe in verschiedenen Sektoren, sei es in der Wirtschaft, den Finanzen, den Immobilien oder im Gesundheitswesen. All dies sind Angriffe auf unseren täglichen Alltag und den unserer Bürgerinnen und Bürger. Zudem müssen bei den täglich wachsenden Angriffsmöglichkeiten auch Gesetze der Situation entsprechend angepasst und erweitert werden, um auch weiterhin die Cybersicherheit im privaten, wirtschaftlichen und staatlichen Sektor zu erhalten.

Hier sei gesagt: Hundertprozentige Sicherheit gibt es nicht; aber der Staat hat die Aufgabe, die Rahmenbedingungen so zu setzen, dass das Risiko minimiert und eine Rekapitulation der Ereignisse möglich ist. Deshalb gibt es für die Neufassung der NIS-2-Richtlinie, welche von den Mitgliedstaaten bis Oktober dieses Jahres umzusetzen ist, Ansätze, um Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Europäischen Union in nationales Recht umzusetzen.

Die Bayerische Staatsregierung hat mit der Errichtung des Landesamts für Sicherheit in der Informationstechnik und der gesetzlichen Verpflichtung der Behörden zu angemessener Informationssicherheit mit dem Bayerischen Digitalgesetz sowie der Einführung von Managementsystemen für Informationssicherheit in den staatlichen Behörden bereits Maßnahmen zur IT-Sicherheit für Verwaltungsbehörden in Bayern

ergriffen, die den Zielsetzungen der Richtlinie sehr nahekommen. Insbesondere besteht gemäß der Richtlinie das Cybersecurity Incidence Response Team bereits als Bayern-CERT im LSI. Zudem verfügt das LSI in seiner Funktion als Behörde zur Gefahrenabwehr bereits über Befugnisse, unter anderem zur Untersuchung der Sicherheit in der Informationstechnik staatlicher und an das Behördennetz angeschlossener Stellen. Gleichwohl bedürfen die sehr detaillierten Vorgaben der EU-Richtlinie der Umsetzung ergänzender Regelungen im Landesrecht. Dies betrifft etwa das dreistufige Verfahren für Einrichtungen im Anwendungsbereich der Richtlinie zur Meldung erheblicher Sicherheitsvorfälle an das LSI.

Aufgrund der sich erst noch abzeichnenden bundesrechtlichen Regelungen sind die nationalen Rahmenbedingungen zwar weiterhin offen; gleichwohl ist zur Wahrung der Umsetzungsfrist das Bayerische Digitalgesetz bereits jetzt anzupassen. Vor allem die Entwicklung der Bedrohungslage macht die Notwendigkeit einer engeren Zusammenarbeit zwischen BSI und LSI deutlich.

Wie die Cybervorfälle gerade in jüngster Vergangenheit gezeigt haben, geht besondere Gefahr von hochspezialisierten Cyberangriffen aus, sogenannten Advanced Persistent Threats oder APTs. Angreifer versuchen dabei, vorsichtig und verdeckt vorzugehen, sodass zwischen dem erfolgreichen Hack der Kommunikationstechnik und der Aufdeckung des Angriffes in der Regel große Zeiträume liegen. Hier wird in aller Regel nur mitgehört und protokolliert, was im System passiert. Aufgrund dieser Infiltrierung können weitere Angriffe sehr detailliert geplant und teils erfolgreich umgesetzt werden.

Um das Ganze etwas einfacher und verständlicher zu machen: Wenn heute jemand ein Auto stehlen will, wird dies dadurch einfacher, wenn man weiß, um welchen Autotyp es sich handelt, welches Baujahr das Auto hat und welcher Serie es zugehört. Genau so erfolgen die Angriffe auf die IT-Systeme. Mit APTs wird versucht, die Gerätehersteller und Firmwarestände herauszufinden, um so einen höheren Grad an erfolgreichen Attacken zu erreichen.

An diesem Punkt setzt die NIS-2-Richtlinie an: Die Protokollspeicherdauer wird auf 18 Monate erhöht. Das verbessert die Möglichkeit der Reaktion auf Angriffe und gewährleistet unserer Ansicht nach zugleich einen angemessenen Schutz von personenbezogenen Daten.

Der letzte Punkt ist die Änderung des Gesetzes über die Bayerische Landesstiftung. Dazu ist schon einiges gesagt worden. Es geht hauptsächlich darum, dass die Landesstiftung auch digital tagen kann und dass Umlaufverfahren auch elektronisch durchgeführt werden können. Das ist unserer Meinung nach eine sehr gute und wichtige Änderung.

Zum Schluss möchte ich noch einmal darauf hinweisen: Die Sicherheit der Informationstechnik staatlicher und sonstiger an das Behördennetz angeschlossener Stellen muss auch in Zukunft im Fokus des Bayerischen Digitalgesetzes bleiben. Deshalb bitte ich um Ihre Zustimmung.

(Beifall bei der CSU)

Erster Vizepräsident Tobias Reiß: Vielen Dank. – Nächster Redner ist der Fraktionsvorsitzende der SPD, Florian von Brunn.

Florian von Brunn (SPD): Sehr geehrter Herr Vizepräsident, sehr geehrte Damen und Herren! Gut, dass sich die Europäische Union um die Themen Cyberkriminalität und Schutz vor Hackerangriffen kümmert. Die Richtlinie muss jetzt umgesetzt werden. Der Freistaat Bayern macht das jetzt, der Bund ist intensiv bei der Umsetzung. Es gibt dort schon Referentenentwürfe. Insofern sollte man hier nicht mit irgendwelchen falschen Behauptungen den Eindruck erzeugen, auf Bundesebene geschehe nichts. Zumal wir dort mit dem Bundesamt für Sicherheit in der Informationstechnik eine sehr gut aufgestellte Behörde haben.

Das Gleiche gilt natürlich auch für das Landesamt für Sicherheit in der Informationstechnik hier in Bayern. Es ist notwendig, dass wir diese Behörde haben. Ich halte es

auch für dringend notwendig, dass wir jetzt die mit der europäischen Richtlinie kommenden Veränderungen umsetzen. Es ist auf jeden Fall richtig und wichtig, dass wir zum Beispiel auch den Zeitraum für die Protokollierung verändern, damit man auf einer Firewall und einem Serversystem nachschauen kann, wann der Angriff erfolgt ist, welche Techniken dabei genutzt worden sind usw. Es geht dabei um Angriffe aus China, es geht um Angriffe aus Russland. Dabei wundert es mich nicht, dass die AfD-Fraktion Probleme damit hat, dass wir hier gegen Cyberkriminalität klare Kante zeigen, da es um ihre Freunde aus Russland und China geht.

Es geht auch um global agierende Kriminelle. Allein an dem, was der Bitkom in seiner Studie im letzten Jahr festgestellt hat, sieht man, um welche Dimensionen es geht: Nur in einem Jahr 206 Milliarden Euro Schäden für Unternehmen durch IT-Diebstahl, durch Spionage und Sabotage. Nicht mitgezählt wurden dabei die Angriffe auf Krankenhäuser, auf Schulen und Kommunen usw.

Es wäre gut, im Zusammenhang mit der Beratung dieses Gesetzes auch darüber zu reden, wie wir unsere Kommunen in Bayern noch besser unterstützen können, wie wir Krankenhausverbünde noch besser unterstützen können, wie wir andere öffentliche Einrichtungen oder Wohlfahrtsverbände beim Thema IT-Sicherheit noch besser unterstützen können.

Herr Kollege Adjei hat schon das Krankenhaus Agathariedangesprochen: Es gab in den letzten zwei Jahren eine ganze Reihe von Vorfällen, zum Beispiel der Angriff auf das Medienzentrum München im Oktober 2022. Davon waren 55 Schulen im Landkreis München betroffen sowie 20 Grund- und Hauptschulen im Landkreis Berchtesgaden. Wahrscheinlich sind die Daten nicht in fremde Hände gelangt.

Im November 2023 wurden im Landkreis Neu-Ulm mehrere Kommunen von Hackern lahmgelegt. Davon waren Bürgerbüros betroffen, sodass Passanträge nicht bearbeitet werden konnten. Die Friedhofsverwaltungen hatten plötzlich keinen Zugriff mehr auf Programme, weil durch Ransomware die Daten verschlüsselt waren. In diesem Januar

– und nun reden wir über gravierende Vorfälle – flossen bei der Bezirksklinik Mittelfranken Personaldaten, Patientendaten, unternehmensinterne Dokumente plötzlich ab. Die Kliniken im Verbund waren aufgrund dieses Angriffes nur noch telefonisch erreichbar. Im Klinikum am Europakanal in Erlangen konnte gar nicht mehr telefoniert werden. Im Mai 2024 sind bei der IT-Infrastruktur der Katholischen Jugendfürsorge Augsburg offenbar massenhaft sensible Daten in die Hände von Kriminellen oder ausländischen Diensten gelangt: Patientendaten, Personaldaten, Finanzdaten.

Das dürfen wir nicht länger zulassen, und deswegen ist es wichtig und richtig, dass wir alles unternehmen, um die IT-Sicherheit in Bayern zu gewährleisten und um Cyberkriminellen das Handwerk zu legen. Wir werden uns deshalb als SPD auch intensiv an den Beratungen beteiligen. – Vielen Dank für Ihre Aufmerksamkeit.

(Beifall bei der SPD)

Erster Vizepräsident Tobias Reiß: Herr von Brunn, bleiben Sie bitte am Rednerpult. Es liegt eine Meldung zu einer Zwischenbemerkung des Herrn Kollegen Andreas Jurca vor.

Andreas Jurca (AfD): Werter Kollege von Brunn!

Florian von Brunn (SPD): Ich bin nicht Ihr Kollege. Ich bitte darum, den Begriff zu vermeiden.

(Beifall bei der SPD – Widerspruch bei der AfD)

Andreas Jurca (AfD): Wir sitzen zusammen hier im Landtag, soweit ich weiß. – Sie werden hier nicht müde, uns wegen unserer Freundschaften zu China und Russland zu kritisieren. Wenn ich mich recht erinnere, war der Bundeskanzler Scholz von der SPD im April für zwei Tage in China. Haben Sie ihn auch schon kritisiert, oder wie stehen Sie dazu? Distanzieren Sie sich von Ihrem Bundeskanzler?

Florian von Brunn (SPD): Wissen Sie, was der Unterschied zwischen Sozialdemokraten, zwischen dem Bundeskanzler Olaf Scholz und Leuten wie Ihnen ist? – Von uns fährt niemand nach Russland, um dort zu bestätigen, dass Putin demokratische Wahlen durchgeführt hat.

(Widerspruch und Lachen bei der AfD)

Das zeigt doch schon, in welchem geistigen Zustand Sie sich befinden. Mehr muss man dazu nicht mehr sagen.

(Beifall bei der SPD)

Erster Vizepräsident Tobias Reiß: Vielen Dank. – Damit ist die Aussprache geschlossen, und ich schlage vor, den Gesetzentwurf dem Ausschuss für Wirtschaft, Landesentwicklung, Energie, Medien und Digitalisierung als federführendem Ausschuss zu überweisen. Erhebt sich Widerspruch? – Das ist nicht der Fall. Dann ist das so beschlossen.