Landtag von Baden-Württemberg **Drucksache 16 / 9145**

16. Wahlperiode **28. 10. 2020**

Antrag

der Abg. Doris Senger u. a. AfD

und

Stellungnahme

des Ministeriums für Wissenschaft, Forschung und Kunst

Cybersicherheit an Hochschulen, Universitätsklinika und außeruniversitären Forschungseinrichtungen in Baden-Württemberg

Antrag

Der Landtag wolle beschließen,

die Landesregierung zu ersuchen

zu berichten,

1. ob es in Anbetracht des digitalen Fortschritts eine Cybersicherheitsstrategie für alle Hochschulen, Universitätsklinika und außeruniversitären Forschungen in Baden-Württemberg gibt;

2. wie die aktuelle IT-Sicherheit an Hochschulen, Universitätsklinika und außeruniversitären Einrichtungen beurteilt wird, insbesondere hinsichtlich der aktuell vorhandenen Angriffsflächen/Risikofaktoren;

3. welche Maßnahmen zur Behebung der identifizierten Risikofaktoren ergriffen wurden;

4. ob jede Hochschule, jedes Universitätsklinikum und jede außeruniversitäre Forschungsanstalt eine IT-Abteilung für ihre Cybersicherheit hat und wie diese personell und materiell (Geräte) ausgestattet sind;

5. wie viele Cyberangriffe es in den letzten fünf Jahren auf die Hochschulen, Universitätsklinika und außeruniversitären Forschungseinrichtungen gab und wie hoch der zugefügte Schaden ist;

6. welche Maßnahmen nach den Cyberangriffen ergriffen wurden;

7. welche finanziellen Mittel den Hochschulen, Universitätsklinika und außeruniversitären Einrichtungen explizit für die Cybersicherheit aktuell zur Verfügung gestellt werden (das Budget für Sicherheit nach Universität, Hochschule und Uniklinika aufgeschlüsselt);

Eingegangen: 28. 10. 2020 / Ausgegeben: 30. 11. 2020

8. ob es Pläne gibt, allen Hochschulen, Universitätsklinika und außeruniversitären Forschungseinrichtungen ein Budget zur Verfügung zu stellen, welches explizit für die IT-Sicherheit da ist;

9. ob der Landesregierung bekannt ist, dass aufgrund der aktuellen Rahmenbedingungen die Hochschulen enorme Problem haben, gute IT-Spezialisten einzustellen, weil sie in der Wirtschaft ungleich bessere Konditionen vorfinden, und wie gedenkt sie hier – explizit in diesem Bereich die Hochschulen – konkurrenzfähiger zu machen;

10. wie die Effektivität des 2018 ausgerichteten Arbeitskreises Informationssicherheit, die Ergebnisse der Analyse und Schlussfolgerungen beurteilt werden;

11. welche Hochschulen, Universitätsklinika und außeruniversitäre Forschungseinrichtungen im Falle eines Cyberangriffs ein Notfallmanagement (kurze Planbeschreibung) haben.

28. 10. 2020

Senger, Stauch, Wolle,
Dr. Grimmer, Baron AfD

Begründung

Die Digitalisierung hat unser Leben komfortabler gemacht. Vieles ist per Mausklick möglich. Wir haben aber auch gelernt, dass neue Technologien auch Nachteile mit sich bringen. Die digitale Transformation macht auch vor Hochschulen nicht Halt. Die registrierten Cyberangriffe auf Hochschulen und Forschungseinrichtungen haben stark zugenommen. Insofern kommt der IT und deren Sicherheit eine steigende Bedeutung zu.

Es ist unbestritten, dass Informationssicherheit an Hochschulen kein Projekt ist, das in drei oder vier Jahren zu Ende ist. Informationssicherheit ist in der digitalisierten Gesellschaft eine Daueraufgabe, die die Hochschulen stets optimal erfüllen müssen. Insofern soll mit diesem Antrag beleuchtet werden, wie die aktuelle Situation der Hochschulen in punkto Cybersicherheit ist und ob und welche Pläne es gibt, diesen Bereich in Zukunft zu organisieren.

Stellungnahme

Mit Schreiben vom 19. November 2020 Nr. 34-0275.6/72/1 nimmt das Ministerium für Wissenschaft, Forschung und Kunst in Abstimmung mit dem Ministerium für Finanzen, dem Ministerium für Inneres, Digitalisierung und Migration sowie dem Ministerium für Wirtschaft, Arbeit und Wohnungsbau zu dem Antrag wie folgt Stellung:

Der Landtag wolle beschließen,

die Landesregierung zu ersuchen

zu berichten,

1. ob es in Anbetracht des digitalen Fortschritts eine Cybersicherheitsstrategie für alle Hochschulen, Universitätsklinika und außeruniversitären Forschungen in Baden-Württemberg gibt;

Die Absicherung des Cyberraums und der Schutz vor Cyber-Angriffen ist eines der zentralen Themen für die Zukunft Baden-Württembergs. Die Landesregierung

hat auf diese Herausforderung zum einen mit der Entwicklung von Eckpunkten für eine landesweite Cybersicherheitsstrategie reagiert[1], die die staatliche Handlungsfähigkeit in Fällen von Cyberangriffen gewährleisten und die Cybersicherheit ganzheitlich in allen gesellschaftlichen Sektoren stärken soll. Zum anderen befindet sich das Gesetz zur Verbesserung der Cybersicherheit und Änderung anderer Vorschriften (CSVG) aktuell in Vorbereitung zur Einbringung in den Landtag. Als zentraler Baustein ist darin die Einrichtung einer Cybersicherheitsagentur (CSBW) vorgesehen. Der Hochschulbereich wird sich an der Entwicklung einer umfassenden Cybersicherheitsstrategie aktiv beteiligen und die kooperative Zusammenarbeit mit der CSBW suchen.

Komplementär zu der landesweiten Cybersicherheitsstrategie haben sich die Universitäten und Hochschulen in Baden-Württemberg in einem Rahmenkonzept Informationssicherheit darauf verständigt, gemeinsam ein dauerhaftes hochschulübergreifendes Informationssicherheitsnetzwerk zu etablieren. Es soll im Zusammenspiel von lokalen und übergreifenden Stellen Synergien beim Ressourceneinsatz, beim Informationsaustausch und der Konzeption und Umsetzung von Schutzmaßnahmen heben. Diese Strategie des breiten Wissens- und Informationsaustausches und des dafür etablierten Netzwerkes bietet eine ideale Ansprechpartnerstruktur für die Zusammenarbeit mit der CSBW.

Die vier Universitätsklinika Baden-Württembergs betreiben Informationssicherheitsmanagementsysteme, welche auch Strategien für Maßnahmen im Bereich Cybersicherheit beinhalten. Die Gesamtstrategie wird im Rahmen einer Zusammenarbeit der Universitätsklinika des Landes im Bereich Informationssicherheit abgestimmt und weiterentwickelt.

Die außeruniversitären Forschungseinrichtungen (AUF) sind ebenfalls sensibilisiert für die Gefahren der Cyberkriminalität, haben sich sehr intensiv mit ihnen auseinandergesetzt und verfügen über IT-Sicherheitskonzepte. Teilweise sind sie in national organisierte Cybersicherheitsstrukturen eingebunden, so z. B. innerhalb der Fraunhofer-Gesellschaft (FhG) und des Deutschen Zentrums für Luft- und Raumfahrt (DLR).

2. wie die aktuelle IT-Sicherheit an Hochschulen, Universitätsklinika und außeruniversitären Einrichtungen beurteilt wird, insbesondere hinsichtlich der aktuell vorhandenen Angriffsflächen/Risikofaktoren;

3. welche Maßnahmen zur Behebung der identifizierten Risikofaktoren ergriffen wurden;

Die Ziffern 2 und 3 werden zusammen beantwortet.

Wie in der Drucksache 16/8662 vom Innenministerium ausgeführt wurde, konnte eine spezifische Zunahme von Angriffen auf Telearbeitsplätze in heimischen Büros von den Ermittlungs- und Verfassungsschutz-Behörden sowie dem zentralen IT-Dienstleister der Landesverwaltung BITBW bisher nicht festgestellt werden. Gleichwohl kann angenommen werden, dass der allgemeine Trend einer zunehmenden Bedrohung durch Cyberangriffe im Zuge der fortschreitenden Digitalisierung unabhängig von der Entwicklung der COVID-19-Pandemie weiter anhält. Zudem wird eine Zunahme von Angriffen auf Kommunikationsplattformen registriert, die den Versuch des Mitschnitts von Unternehmenskommunikation über Remote-Zugänge erkennbar werden lässt.

Aufgrund der gewachsenen Sensibilität sowie der verstärkten Vernetzung der Hochschulen sind sie gegenüber dieser Bedrohungslage gut gerüstet. Ziel ist es, durch einen kontinuierlich zu verbessernden Informationsfluss und Wissensaustausch unter ihnen, gemeinsame präventive und reaktive Maßnahmen zu entwickeln und so das allgemeine Schutzniveau aller Hochschulen weiter zu erhöhen.

[1] Siehe dazu *https://im.baden-wuerttemberg.de/de/service/presse-und-oeffentlichkeitsarbeit/pressemitteilung/pid/einrichtung-einer-cybersicherheitsagentur/*

Bei den Universitätsklinika haben sich bestehende Maßnahmen zur Absicherung bis heute als effektiv erwiesen. Weitere technische und personelle Maßnahmen sind kontinuierlich notwendig. Sie werden auf der Grundlage entsprechender Risikobetrachtungen jeweils individuell und an das jeweilige Risiko angepasst durchgeführt.

Auch bei den wirtschaftsnahen Forschungseinrichtungen in Baden-Württemberg ist die Gewährleistung der IT-Sicherheit eine wichtige Verwaltungsaufgabe und liegt in deren Verantwortung. Die Einrichtungen reagieren mit Maßnahmen, die dem jeweiligen Risikoszenario angepasst sind. Hierzu zählen neben technischen und organisatorischen Schutzmaßnahmen insbesondere Sensibilisierungs- und Schulungsmaßnahmen für die Mitarbeiterinnen und Mitarbeiter. Bei verschiedenen AUF wurde die Möglichkeit von Remote-Logins in das genutzte Wissenschaftsnetz für Wissenschaftler von außen deaktiviert, um Gefahrenpotenzial zu verringern.

4. ob jede Hochschule, jedes Universitätsklinikum und jede außeruniversitäre Forschungsanstalt eine IT-Abteilung für ihre Cybersicherheit hat und wie diese personell und materiell (Geräte) ausgestattet sind;

Die Hochschulen und Universitätsklinika verfügen jeweils über Organisationseinheiten, die für die IT und/oder IT-Sicherheit zuständig sind. Eine detaillierte Erhebung der aktuellen Ausstattungen war im Rahmen dieser Landtagsanfrage nicht möglich. Ergänzend wird auf Ziffer 7 verwiesen.

Bei den AUF obliegt die Ausstattung und Umsetzung von Maßnahmen zur Cybersicherheit der Verantwortung der jeweiligen Forschungseinrichtungen bzw. Institute. Die Fraunhofer-Gesellschaft hat hierzu Informationssicherheitsbeauftragte in allen Instituten eingesetzt und ein eigenes Fraunhofer Security Operations Center etabliert, das die Fraunhofer-Gesellschaft und ihre Institute bei der Erkennung und Bearbeitung von Cyberangriffen unterstützt. Auch an allen Instituten der Innovationsallianz Baden-Württemberg sind Mitarbeiterinnen und Mitarbeiter für die IT-Sicherheit beschäftigt. Das DLR hat seine IT-Infrastruktur und damit auch Aufgaben im Bereich IT-Sicherheit größtenteils an externe Dienstleister ausgelagert. Diesen Dienstleistern obliegt es, die Zahl der im Bereich IT-Sicherheit eingesetzten Mitarbeiterinnen und Mitarbeiter angemessen zu steuern.

5. wie viele Cyberangriffe es in den letzten fünf Jahren auf die Hochschulen, Universitätsklinika und außeruniversitären Forschungseinrichtungen gab und wie hoch der zugefügte Schaden ist;

Eine systematische Erfassung von Cyberangriffen auf Hochschulen, die fünf Jahre zurückreicht, liegt nicht vor. Cyberangriffe im weitesten Sinne, wie Portscans, Spam-Mails oder Phishing-Angriffe, erfolgen täglich tausendfach auf die Hochschulen. Seit Sommer 2018 wurden dem Wissenschaftsministerium rund 20 Cyberangriffe auf Hochschulen bzw. Hochschuleinrichtungen angezeigt, die über die zahlreichen täglichen von den Hochschulen routinemäßig abgewehrten Angriffe hinausgingen. Insgesamt ist davon auszugehen, dass sich schwerwiegende Angriffe auf Netzwerke oder in Form von Verschlüsselungstrojanern in den letzten fünf Jahren im einstelligen Bereich hielten. Keiner der Angriffe verursachte, soweit bekannt, einen Schaden in monetärer Hinsicht oder in Bezug auf den Abfluss brisanter Daten oder Informationen. Dies gilt auch für die Hackerangriffe im Mai 2020, bei denen im Zuge einer weltweiten Angriffswelle auf Hoch- und Höchstleistungsrechenzentren auch baden-württembergische Universitätsstandorte, an denen High Performance Computing (HPC) betrieben wird, betroffen waren. Mehrere Hundert Forschungsprojekte, die zur Berechnung, Modellierung oder Simulation auf unterschiedlichen Forschungsgebieten besonders hohe Rechenkapazitäten erfordern, konnten die HPC-Rechner für einen Zeitraum von rund vier Wochen nicht nutzen.

Auch die Universitätsklinika sind täglich unzähligen Cyberangriffen in Form von Phishing- oder Spam-Mails ausgesetzt. Ein Universitätsklinikum beziffert diese Zahl für den Zeitraum von Januar 2019 bis August 2020 mit durchschnittlich ca. 16.000 Angriffe pro Tag. Der zugefügte Schaden liegt bisher maßgeblich im kurzfristigen Ausfall einzelner Rechner und insbesondere in der Bindung zusätzlicher Personal-Ressourcen.

Bei den AUF waren in den letzten fünf Jahren trotz einer gewissen Zunahme von Angriffen ebenfalls keine gravierenden Hackerangriffe zu verzeichnen. Oftmals handelt es sich nicht um gezielte Angriffe auf die spezifische Einrichtung, sondern um großangelegte Angriffswellen u. a. von Malware und Phishing. Die Gesamtzahl dieser ungerichteten Angriffe wird nicht erfasst. Die Landesregierung wurde jedoch über fünf gezielte Cyberangriffe auf Institute der Innovationsallianz BW sowie zwei Cyberangriffe auf Fraunhofer-Institute in Baden-Württemberg in den vergangenen fünf Jahren informiert. Der Landesregierung ist kein hierdurch entstandener Schaden bekannt. Beim DLR liegt der Fokus von Cyberangriffen auf der zentralen IT-Infrastruktur, welche nicht in Baden-Württemberg angesiedelt ist. Ein spezifischer Bezug von Angriffen auf die IT-Infrastruktur in Baden-Württemberg ist nicht zu erkennen.

6. welche Maßnahmen nach den Cyberangriffen ergriffen wurden;

Die Reaktion der betroffenen Einrichtungen auf Cyberangriffe richtet sich nach der Vorgehensweise der Angriffe. Neben Investitionen in leistungsfähige Firewalls und redundante Datenhaltung werden betroffene Server passgenau nach Art und Umfang des Angriffs gesperrt, forensisch gesichert, mit Back-Ups versehen oder neukonfiguriert.

Im Hochschulbereich ist durch die Etablierung einer Meldekette sichergestellt, dass alle notwendigen Instanzen frühzeitig über Cyberangriffe informiert werden. Dies betrifft neben der unverzüglichen Benachrichtigung des Wissenschaftsministeriums und des Landes-CISO die Information des CERT BWL durch die Hochschulen. Sofern die Gefahr einer Datenpanne besteht, wird der Landesbeauftragte für Datenschutz und Informationsfreiheit informiert. Sofern Hinweise auf nachrichtendienstliche Aktivitäten vorliegen, wird das Landesamt für Verfassungsschutz beteiligt. Kriminelle Handlungen werden zur Anzeige gebracht.

Die Universitätsklinika melden nach den gesetzlichen Vorgaben an das Bundesamt für Sicherheit in der Informationstechnik (BSI). Ebenso werden Sicherheitsvorfälle einem Review unterzogen und gezielte Maßnahmen zur Risikominimierung angestrebt. Ggf. werden polizeiliche Ermittlungen und teilweise Neuinstallationen der Client-Hardware durchgeführt. Die meisten Cyberangriffe werden über implementierte Standard-Maßnahmen bewältigt. Bei erheblichen Cyberangriffen erfolgt soweit möglich und umsetzbar eine der Situation angepasste individuelle Behandlung durch Maßnahmen.

Nach den fünf gezielten Cyberangriffen auf Institute der Innovationsallianz BW sowie zwei Cyberangriffen auf Fraunhofer-Institute in Baden-Württemberg wurden sowohl technische Maßnahmen zum Schutz vor zukünftigen Cyberangriffen ergriffen als auch zusätzliche Sensibilisierungs- und Schulungsmaßnahmen für Mitarbeiterinnen und Mitarbeiter durchgeführt.

7. welche finanziellen Mittel den Hochschulen, Universitätsklinika und außeruniversitären Einrichtungen explizit für die Cybersicherheit aktuell zur Verfügung gestellt werden (das Budget für Sicherheit nach Universität, Hochschule und Uniklinika aufgeschlüsselt);

8. ob es Pläne gibt, allen Hochschulen, Universitätsklinika und außeruniversitären Forschungseinrichtungen ein Budget zur Verfügung zu stellen, welches explizit für die IT-Sicherheit da ist;

Die Ziffern 7 und 8 werden zusammen beantwortet.

Zusätzlich zur Grundfinanzierung wurden in den Doppelhaushalten 2018/19 und 2020/21 den Hochschulen insgesamt 58 Neustellen nebst Ausstattung und den Medizinischen Fakultäten ab 2020 jeweils jährlich 70 Tsd. Euro für den Bereich Informationssicherheit zur Verfügung gestellt, um den Ausbau des Informationssicherheitsmanagementsystems zu ermöglichen und die bis dahin in unterschiedlichem Umfang an den Einrichtungen eingesetzten finanziellen und personellen Ressourcen aufzustocken. Diese Bereitstellung eines Gesamtbudgets von rund 6,06 Mio. Euro konkret für Zwecke der Informationssicherheit und IT-Sicherheit im Bereich der Hochschulen und Universitätsklinika ist eine große und wichtige Investition in die Zukunft. Gemäß der Hochschulfinanzierungsvereinbarung 2021 bis 2025 wird eine Überführung der Stellen in die Hochschulkapitel angestrebt.

Die Gewährleistung der IT-Sicherheit ist eine wichtige Verwaltungsaufgabe der wirtschaftsnahen Forschungseinrichtungen und liegt in deren Verantwortung. Das Land beteiligt sich an den hieran anfallenden Aufwänden im Rahmen der Grundfinanzierung. Darüber hinaus werden keine zusätzlichen finanziellen Mittel explizit für die Informationssicherheit zur Verfügung gestellt.

9. ob der Landesregierung bekannt ist, dass aufgrund der aktuellen Rahmenbedingungen die Hochschulen enorme Problem haben, gute IT-Spezialisten einzustellen, weil sie in der Wirtschaft ungleich bessere Konditionen vorfinden, und wie gedenkt sie hier – explizit in diesem Bereich die Hochschulen – konkurrenzfähiger zu machen;

Die Personalsuche im Bereich von IT-Spezialisten ist generell anspruchsvoll. Dennoch konnten aktuell (Stand: 10. November 2020) zwei Drittel der Hochschulstandorte die bereitgestellten Personalstellen besetzen. Das zeigt, dass die Vorzüge einer Dauerbeschäftigung im öffentlichen Dienst weiterhin attraktiv sind und angesichts der pandemiebedingten Unsicherheit des Arbeitsmarktes eventuell an Attraktivität gewinnen.

10. wie die Effektivität des 2018 ausgerichteten Arbeitskreises Informationssicherheit, die Ergebnisse der Analyse und Schlussfolgerungen beurteilt werden;

Es wird angenommen, dass der sog. Steuerkreis Informationssicherheit gemeint ist. Dieser setzt sich aus Vertretern aller Hochschularten zusammen und trifft sich seit Anfang 2019 regelmäßig mit dem Ziel, die Zusammenarbeit der Universitäten und Hochschulen zum Thema Informationssicherheit zu festigen und zu verstärken. Die bisherige Arbeit des Steuerkreises war geprägt von aktuellen Herausforderungen der Hochschulen wie der rechtssicheren Gestaltung von online-Studienangeboten sowie dem Aufbau zentraler Arbeitsstrukturen. Im Zusammenhang mit den Hackerangriffen auf mehrere Universitätsstandorte haben sich die positiven Effekte der Netzwerkbildung auf einen schnellen und koordinierten Informationsaustausch und einen effektiven Reaktionsplan gezeigt.

11. welche Hochschulen, Universitätsklinika und außeruniversitäre Forschungseinrichtungen im Falle eines Cyberangriffs ein Notfallmanagement (kurze Planbeschreibung) haben.

Nach der Verwaltungsvorschrift des Innenministeriums zur Informationssicherheit vom Mai 2017 ist bei allen Dienststellen und Einrichtungen des Landes ein Notfallmanagement nach dem Standard des Bundesamts für Sicherheit in der Informationstechnik einzuführen. Entsprechend dieser Vorschrift sind die Hochschulen des Landes derzeit dabei, in einem systematischen und strukturierten

Prozess die Vorgaben des BSI-Grundschutzes inklusive des Notfallmanagements auf ihre bestehenden Prozesse und Verfahren anzuwenden.

Die Universitätsklinika besitzen im Rahmen des Notfallmanagements entsprechende Notfallpläne. Ebenso werden Workshops durchgeführt mit dem Ziel, weitere Maßnahmen zu identifizieren.

Auch bei den AUF wurden Notfallbereiche identifiziert und Notfallpläne entwickelt. So gibt es z. B. bei der Fraunhofer-Gesellschaft Regelungen und Vorkehrungen zu Sicherheits- und Datenschutzvorfällen, die Cyberangriffe umfassen und ein etabliertes Krisenmanagement-System. Sie betreffen Meldewege, Beurteilungen, Analysen durch das zentrale Security Operation Center, Beteiligungen des Gesamtbetriebsrates, Information der Öffentlichkeit und andere Reaktionen. Bei der Erkennung und Analyse einzelner Sicherheitsvorfälle waren Sicherheitsbehörden behilflich.

Bauer

Ministerin für Wissenschaft
Forschung und Kunst