Landtag von Baden-Württemberg **Drucksache 17 / 4022**

17. Wahlperiode **25.1.2023**

Antrag

der Abg. Dennis Birnstock und Daniel Karrais u. a. FDP/DVP

und

Stellungnahme

des Ministeriums für Wissenschaft, Forschung und Kunst

Cybersicherheit an den Hochschulen in Baden-Württemberg

Antrag

Der Landtag wolle beschließen,

die Landesregierung zu ersuchen

zu berichten,

1. was die Landesregierung infolge des erfolgreichen Hackerangriffs mit der Schadsoftware Emotet im Dezember 2019 auf die Universität Gießen unternommen hat, um die Hochschulen in Baden-Württemberg bei der Cybersicherheit zu unterstützen;

2. welche Fälle cyberkrimineller Angriffe auf Hochschulen im Land ihr aus den letzten zehn Jahren bekannt sind;

3. welche Gefahren für die Datensicherheit an den hiesigen Hochschulen durch Ransomware-Angriffe sie erkennt;

4. welche Schlüsse sie aus den aktuellen Vorfällen, etwa dem Angriff auf die Hochschule Heilbronn im November 2022, für die Notwendigkeit gezielter landesseitiger Unterstützungsmaßnahmen für die Hochschulen zieht;

5. welche Schutzmaßnahmen für die Forschungsdaten an den Hochschulen sie für angezeigt hält;

6. welche Schutzmaßnahmen gegen digitale Spionageangriffe auf die Daten der Auftragsforschung an den Hochschulen sie für angezeigt hält, soweit bei diesen auch unternehmerische Interessen und mögliche Wettbewerbsnachteile zu beachten sind;

7. inwieweit sie Risiken erkennt, dass sensible Daten von Studierenden oder Hochschulpersonal in den Fokus gezielter Hackerangriffe geraten könnten;

Eingegangen: 25.1.2023 / Ausgegeben: 8.3.2023

8. welche Handlungsoptionen sie erkennt, soweit bspw. in der hochschulischen Forschung manche Großgeräte mit veralteten Computern betrieben werden, für welche keine Sicherheitsupdates mehr zur Verfügung gestellt werden, die aber in ihrer originären Funktion erhaltenswert sind (etwa teure Elektronenmikroskope in der Medizin);

9. inwieweit die Hochschulen am operationalisierten Austausch der Cybersicherheitsagentur BW und den regelmäßig stattfindenden Fachaustauschen, insbesondere hinsichtlich des Austauschs über mögliche Gefahrenlagen, notwendige Prävention und stetige Detektion, teilhaben;

10. ob eine Anbindung der Hochschulen und deren Rechenzentren an die bestehenden Kooperationsformen zum Thema Cybersicherheit in Baden-Württemberg sichergestellt ist;

11. inwieweit geplant ist, die landesseitigen Unterstützungsmaßnahmen für die Cybersicherheit der Hochschulen gezielt zu verstärken.

25.1.2023

Birnstock, Karrais, Dr. Timm Kern, Brauer, Dr. Rülke,
Haußmann, Weinmann, Bonath, Fischer, Haag, Hoher,
Dr. Jung, Reith, Dr. Schweickert, Trauschel FDP/DVP

Begründung

In jüngster Zeit geraten Hochschulen immer mehr in den Fokus von Hackerangriffen, wie etwa die Hochschule Heilbronn im November 2022. Das Rechenzentrum der Hochschule hatte „unübliche Aktivitäten“ im Netzwerk festgestellt und die Institution vorübergehend vollständig vom Netz genommen. Da die Hochschulen im Land zahlreiche sensible Daten, seien es Forschungsinhalte oder Personendaten von Studierenden oder Hochschulpersonal, zu verwalten haben, stellt sich die Frage nach möglicherweise notwendigen Maßnahmen an den Hochschulen, die einer Unterstützung durch das Land bedürfen. Inwieweit bestehende Strukturen der Cybersicherheitsarchitektur im Land ausreichen oder neue Kooperationen etabliert werden müssten, soll dieser Antrag ebenfalls klären.

Stellungnahme

Mit Schreiben vom 20. Februar 2023 Nr. MWK42-0141.5-33/1/3 nimmt das Ministerium für Wissenschaft, Forschung und Kunst im Einvernehmen mit dem Ministerium des Inneren, für Digitalisierung und Kommunen und dem Ministerium für Finanzen zu dem Antrag wie folgt Stellung:

Der Landtag wolle beschließen,

die Landesregierung zu ersuchen

zu berichten,

1. was die Landesregierung infolge des erfolgreichen Hackerangriffs mit der Schadsoftware Emotet im Dezember 2019 auf die Universität Gießen unternommen hat, um die Hochschulen in Baden-Württemberg bei der Cybersicherheit zu unterstützen;

Im Sommer 2019 wurde das Hochschulnetzwerk bwInfoSec aufgebaut, um gemeinsam die Informationssicherheit an den Hochschulen sowie den Kunst- und Kultureinrichtungen des Landes Baden-Württemberg zu verbessern. Dazu werden Informationen geteilt, zentrale Dienste etabliert, gemeinsame Projekte bearbeitet und Hilfestellungen bei Problemen geleistet. Der Kooperationsverbund bwInfoSec ist eine bundesweit einzigartige Struktur, die sich den Fragestellungen der Informationssicherheit für eine abgestimmte Strategie der Hochschulen im Land widmet.

2. welche Fälle cyberkrimineller Angriffe auf Hochschulen im Land ihr aus den letzten zehn Jahren bekannt sind;

Wie zur Drucksache 16/9145 aus dem Jahr 2020 – Cybersicherheit an Hochschulen, Universitätsklinika und außeruniversitären Forschungseinrichtungen in Baden-Württemberg, Frage 2 – mitgeteilt, liegt eine systematische Erfassung von Cyberangriffen auf Hochschulen, die zehn Jahre zurückreicht, nicht vor. Cyberangriffe wie Portscans, Spam-Mails oder Phishing-Angriffe erfolgen täglich tausendfach auf die Hochschulen. Seit Sommer 2018 wurden dem Ministerium für Wissenschaft, Forschung und Kunst rd. 107 Cyberangriffe auf Hochschulen bzw. Hochschuleinrichtungen mitgeteilt, die über die zahlreichen täglichen, von den Hochschulen routinemäßig abgewehrten Angriffe hinausgingen. Schwerwiegende Angriffe auf Netzwerke oder von Verschlüsselungstrojanern bewegen sich dabei im einstelligen Bereich. Bis zum Jahr 2020 verursachte keiner der Angriffe, soweit bekannt, einen unmittelbaren Schaden in monetärer Hinsicht. 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. Bei den jüngsten Angriffen aus den Jahren 2021 und 2022 auf die Pädagogischen Hochschulen Weingarten-Ravensburg und Freiburg sowie die Hochschule Heilbronn konnten allerdings Datenabflüsse nicht ausgeschlossen werden. Auch mussten erhebliche Beträge für die Wiederinbetriebnahme von Systemen mit Hilfe von Dienstleistern investiert werden.

Die Cyberabwehr des LfV beobachtete zudem in den letzten Jahren immer wieder Cyberangriffe auf akademische Einrichtungen, die mutmaßlich von fremden Nachrichtendiensten initiiert wurden. Besonders zu nennen ist dabei die Cyberangriffskampagne „Mabna Institute“. Diese, vom iranischen Nachrichtendienst gesteuerten Angriffe sind bereits seit vielen Jahren aktiv und richten sich hauptsächlich gegen Bibliotheks- und Forschungsplattformen von Hochschulen. Mit diesen Angriffen sollen persönliche Zugangsdaten von Studierenden oder Mitarbeitenden erlangt werden, um anschließend illegal Zugriff auf interne Datenbanken, Wissenssammlungen oder Forschungsergebnisse, z. B. aus unveröffentlichten Dissertationen, zu erlangen.

3. welche Gefahren für die Datensicherheit an den hiesigen Hochschulen durch Ransomware-Angriffe sie erkennt;

Ransomware-Angriffe stellen derzeit eine der häufigsten Angriffsformen gegen Hochschulen dar. Sie können dabei sowohl die Daten von Studierenden und Mitarbeiterinnen und Mitarbeitern als auch Forschungsdaten betreffen. Für die Datensicherheit bestehen dabei die zwei grundlegenden Gefahren des Datenverlustes (durch die Verschlüsselung der Daten sind diese nach einem erfolgreichen Angriff nicht mehr nutzbar) und der Veröffentlichung von Daten.

4. welche Schlüsse sie aus den aktuellen Vorfällen, etwa dem Angriff auf die Hochschule Heilbronn im November 2022, für die Notwendigkeit gezielter landesseitiger Unterstützungsmaßnahmen für die Hochschulen zieht;

Die Landesregierung sieht sich in den in Ziffer 1 genannten frühzeitig eingeleiteten Aktivitäten zur Steigerung der Informationssicherheit an den staatlichen Hochschulen im Land bestärkt. So wurde beispielsweise beim Vorfall an der Hochschule Heilbronn sowohl die bestehende Kooperation mit der Cybersicherheitsagentur Baden-Württemberg (CSBW) als auch der Informationsaustausch innerhalb von bwInfoSec gewinnbringend genutzt.

5. welche Schutzmaßnahmen für die Forschungsdaten an den Hochschulen sie für angezeigt hält;

Zum Schutz von Forschungsdaten sind folgende Maßnahmen angezeigt:

- Gesichertes Backup und eine entsprechende Langzeitarchivierung, um im Falle einer Störung oder eines Angriffs Daten wiederherstellen zu können.
- Updates, um Systeme auf dem aktuellsten Stand zu halten.
- Accountsicherheit, z. B. durch sichere Passwörter.
- Sensibilisierung von Mitarbeiterinnen und Mitarbeitern für die digitalen Gefahren mit Hilfe von Schulungen und Informationen.
- Verschlüsselung, um die Vertraulichkeit und die Integrität von Daten zu gewährleisten.

6. welche Schutzmaßnahmen gegen digitale Spionageangriffe auf die Daten der Auftragsforschung an den Hochschulen sie für angezeigt hält, soweit bei diesen auch unternehmerische Interessen und mögliche Wettbewerbsnachteile zu beachten sind;

Es wird auf die Antwort zu Ziffer 4 und 5 verwiesen.

7. inwieweit sie Risiken erkennt, dass sensible Daten von Studierenden oder Hochschulpersonal in den Fokus gezielter Hackerangriffe geraten könnten;

Personenbezogene Informationen sind für Angreifer finanziell attraktive Ziele, da gestohlene Datensätze verkauft werden können. Oftmals werden Institutionen im Zuge von Ransomware-Angriffen mit der Preisgabe derartiger Daten erpresst. Die Verwendung gestohlener personenbezogener Daten eröffnet Kriminellen zudem Angriffsmöglichkeiten durch Phishing oder, da Nutzerinnen und Nutzer Mailadressen und Passwörter häufig für verschiedene Dienste verwenden, durch die illegitime Anmeldung bei anderen Diensten (Credential Stuffing).

Wissenschaftliche Einrichtungen stehen zudem seit langem im Fokus ausländischer Nachrichtendienste. Deren Ziel besteht im Rahmen der Cyberspionage im gezielten Know-how-Abfluss. Das Interesse gilt hier insbesondere unveröffentlichten Forschungsergebnissen. Jedoch könnte auch das Ziel verfolgt werden, weitere Hinweise auf potenzielle Opfer zu generieren oder die IT-Systeme der wissenschaftlichen Einrichtungen als Angriffsinfrastruktur zu missbrauchen. Frem-

de Staaten setzen für ihre Angriffe im Cyberraum verschiedene Cybergruppierungen ein. Diese werden generell als APT-Gruppe (Advanced Persistent Threat; übersetzt: fortgeschrittene, andauernde Bedrohung) bezeichnet und sollen die wahre Identität von Angriffen verschleiern. APT-Angriffe zeichnen sich durch einen sehr hohen personellen wie finanziellen Ressourceneinsatz sowie erhebliche technisch-methodische Fähigkeiten aus und sind nur sehr schwer zu entdecken. Mit diesen Angriffen gehen zu Beginn einer Attacke oftmals ausgefeilte manipulative Methoden (Social Engineering) einher, um Menschen zu einem bestimmten, sicherheitskritischen Verhalten zu verleiten. Außerdem verwenden APT vielfach sog. Spear-Phishing-E-Mails, die passgenau auf die Interessenlagen weniger Empfänger oder Einzelpersonen zugeschnitten sind, um z. B. mittels versteckt integrierter oder angehängter Schadsoftware IT-Systeme zu kompromittieren, und so letztlich unbemerkt Datenabflüsse zu generieren.

Insgesamt ist von einer anhaltend hohen abstrakten Gefährdungslage für akademische Einrichtungen und deren Personal auszugehen.

8. welche Handlungsoptionen sie erkennt, soweit bspw. in der hochschulischen Forschung manche Großgeräte mit veralteten Computern betrieben werden, für welche keine Sicherheitsupdates mehr zur Verfügung gestellt werden, die aber in ihrer originären Funktion erhaltenswert sind (etwa teure Elektronenmikroskope in der Medizin);

Wichtig ist zunächst eine Netzwerk-Isolierung solcher Großgeräte, um den Zugriff aus anderen Bereichen (z. B. dem öffentlichen Internet) zu vermeiden. Netzwerkseitig können Geräte in einem getrennten Subnetzwerk mit restriktiven Regeln genutzt werden, welche die ein- und ausgehende Kommunikation auf das benötigte Minimum reduzieren. Softwareseitig ist es empfehlenswert, isoliert virtuelle Umgebungen für den Betrieb zu verwenden (Sandbox). Auch hier ist zu beachten, dass ein- und ausgehende Verbindungen auf ein absolutes Minimum reduziert werden müssen.

9. inwieweit die Hochschulen am operationalisierten Austausch der Cybersicherheitsagentur BW und den regelmäßig stattfindenden Fachaustauschen, insbesondere hinsichtlich des Austauschs über mögliche Gefahrenlagen, notwendige Prävention und stetige Detektion, teilhaben;

Die Hochschulen sind an den Warn- und Informationsdienst des Computer Emergency Response Team des Landes (CERT BWL) in der CSBW angebunden und werden regelmäßig über aktuelle Gefahrenlagen und mögliche Hilfestellungen informiert. Hierzu zählen auch Mitteilungen zu Präventionsmaßnahmen und zur Detektion verdächtiger Aktivitäten. Das CERT BWL der CSBW ist in Krisenfällen eine der ersten Anlaufstellen für Hochschulen. Somit kooperieren Hochschulen und CSBW sowohl im reaktiven als auch im präventiven Bereich. Die Unterstützung des CERT BWL wurde im letzten Jahr u. a. von der Hochschule Mannheim, der Pädagogischen Hochschule Freiburg sowie der Hochschule Ulm bei der Vorfallsbehandlung in Anspruch genommen. So konnte beispielsweise im Falle der Hochschule Heilbronn durch die Zusammenarbeit mit dem CERT BWL weiterer, weitaus schwerwiegenderer Schaden abgewendet werden.

Das CERT BWL hat ein „Eckpunktepapier für den sicheren Betrieb der Netzwerkinfrastruktur“ erstellt und dem Hochschulsektor zur individuellen Überprüfung der Sicherheitsarchitektur zur Verfügung gestellt. Um die Kooperation zwischen den Hochschulen des Landes weiter zu intensivieren und zu verstetigen, wurde eine Arbeitsgruppe aus der Föderation bwInfoSec und der CSBW etabliert.

10. ob eine Anbindung der Hochschulen und deren Rechenzentren an die bestehenden Kooperationsformen zum Thema Cybersicherheit in Baden-Württemberg sichergestellt ist;

Die Hochschulen sind durch bwInfoSec regelmäßig mit verschiedenen Akteuren der Cybersicherheit im engen Austausch und in Kooperationen eingebunden. Der Informationssicherheitssteuerkreis nimmt hierbei eine Schlüsselrolle ein. In diesem Kontext bestehen Kooperationen in bilateralen Formaten (bspw. mit der CSBW oder dem Wissenschaftsnetzwerk BelWü) sowie mit multilateralen Kooperationsprojekten (bspw. bwCampusNetz – hier arbeiten mehrere Universitäten unter Leitung des Karlsruher Instituts für Technologie (KIT) zusammen, um die Campusnetze der Universitäten näher zu beleuchten). Ferner vernetzt bwInfoSec die beteiligten Institutionen hochschulartübergreifend in verschiedenen Arbeitsgruppen (zur Multifaktorauthentifizierung, zum Aufbau eines ISMS, zu Formulierung einer Informationssicherheitsleitlinie und zur Sensibilisierung von Mitarbeiterinnen und Mitarbeiter). Auch hierbei ist bwInfosec eng an die Aktivitäten der Landesregierung angebunden. So findet regelmäßig ein Austausch mit anderen Verantwortlichen für den Aufbau eines ISMS im Verantwortungsbereich des Ministeriums des Inneren, für Digitalisierung und Kommunen statt.

Seitens des Landeskriminalamts Baden-Württemberg werden im Rahmen von Kooperationen und Projekten mit Hochschulen, sowohl in Baden-Württemberg als auch im Bundesgebiet, verschiedene Maßnahmen zur Erhöhung der Informationssicherheit umgesetzt. In den Kooperationen mit der Hochschule Albstadt-Sigmaringen, der Hochschule Aalen, der Dualen Hochschule Heilbronn sowie der Hochschule Mittweida werden sowohl Aspekte der Personalqualifizierung, als auch der Entwicklungen innovativer technischer Lösungen aufgegriffen.

Das LfV sensibilisiert bereits seit vielen Jahren anlassbezogen wie anlassunabhängig Hochschulen und Forschungseinrichtungen hinsichtlich der Bedrohungen durch nachrichtendienstlich gesteuerte Spionage und Sabotage und berät diese im Hinblick auf geeignete personelle, technische und organisatorische Schutzmaßnahmen.

11. inwieweit geplant ist, die landesseitigen Unterstützungsmaßnahmen für die Cybersicherheit der Hochschulen gezielt zu verstärken.

Seit dem Jahr 2020 hat Ministerium für Wissenschaft, Forschung und Kunst zur Etablierung von Beauftragten für Informationssicherheit an den Hochschulen 58 Stellen mit Sachmittelausstattung bereitgestellt. Darin enthalten ist ein zwölf-köpfiges Kernteam, das den Erfahrungsaustausch zwischen den Hochschulen voranbringen und die Abwehr von Cyberangriffen durch Beratungs- und Sensibilisierungsleistungen, Hilfestellungen bei der Vorfallsbewältigung und dem zentralen Betrieb von Sicherheitstools stärken soll. Insgesamt werden für diese Maßnahmen im Hochschulbereich seit dem Jahr 2020 jährlich rund 6,25 Mio. Euro und ab dem Jahr 2023 jährlich rund 6,5 Mio. Euro zur Verfügung gestellt.

Darüber hinaus soll zwischen dem Hochschulbereich und der CSBW eine gesonderte Vereinbarung i. S. d. § 2 Absatz 2 Satz 2 des Cybersicherheitsgesetzes Baden-Württemberg geschlossen werden, um die Zusammenarbeit auf operativer, strategischer und taktischer Ebene auszugestalten.

Außerdem beteiligt sich die Zentrale Ansprechstelle Cybercrime (ZAC) beim Landeskriminalamt Baden-Württemberg regelmäßig an einer Vielzahl von Präventionsveranstaltungen, in denen zielgerichtet aktuelle Angriffsvektoren und Modi Operandi, das für die jeweilige Zielgruppe hieraus resultierende Bedrohungspotenzial sowie passgenaue Abwehr- und Gegenmaßnahmen dargestellt werden. Im Zusammenhang mit Hochschulen war die ZAC im November 2021 in die Durchführung einer Veranstaltung für die Leiter der IT-Abteilungen der baden-württembergischen Universitäten eingebunden. Für das Jahr 2023 ist u. a. eine Beteiligung der ZAC an der IT-Fachtagung des Deutschen Studentenwerks e. V. in Konstanz vorgesehen.

Olschowski

Ministerin für Wissenschaft,
Forschung und Kunst