Landtag von Baden-Württemberg **Drucksache 17 / 4075**

17. Wahlperiode **31.1.2023**

Antrag

der Abg. Alexander Salomon und Michael Joukov GRÜNE

und

Stellungnahme

des Ministeriums für Wissenschaft, Forschung und Kunst

IT-Sicherheit an Hochschulen in Baden-Württemberg

Antrag

Der Landtag wolle beschließen,

die Landesregierung zu ersuchen

zu berichten,

1. wie viele und welche IT-Sicherheitsvorfälle ihr in den letzten fünf Jahren von den Hochschulen des Landes gemeldet wurden;

2. ab welcher Schwere der Sicherheitsvorfälle sie durch die Hochschulen informiert wird;

3. welche Einschränkungen der IT-Dienste der Hochschulen des Landes in den letzten fünf Jahren aufgrund von Cyberangriffen zu verzeichnen waren und sind;

4. welche Präventions- und Aufklärungsmaßnahmen zu Informationssicherheit im Hochschulbereich durchgeführt werden;

5. wie der Umsetzungsstand der Maßnahmen zur Stärkung der Informationssicherheit an Hochschulen ist, die in der Hochschulfinanzierungsvereinbarung II festgeschrieben wurden;

6. wie sich die Zusammenarbeit der Hochschulen mit den weiteren Stellen und Einrichtungen zur IT-Sicherheit gestaltet, insbesondere mit der Cybersicherheitsagentur und dem Bundesamt für Sicherheit in der Informationstechnik;

7. welche Bereiche der IT-Sicherheit der Hochschulen von dem Informationssicherheitsnetzwerk abgedeckt und bearbeitet werden, das 2018 gegründet wurde;

Eingegangen: 31.1.2023 / Ausgegeben: 7.3.2023

8. welche Ergebnisse die Evaluation des Gesamtkonzepts des Informationssicherheitsnetzwerks hatte;

9. wie sie die Bedrohungslage für die IT-Sicherheit der Hochschulen aktuell bewertet und welche Konsequenzen sie daraus für das Gesamtkonzept Informationssicherheit an Hochschulen zieht.

31.1.2023

Salomon, Joukov, Aschhoff, Erikli, Knopf,
Köhler, Saint-Cast, Seemann GRÜNE

Begründung

Der Antrag soll einen Überblick über IT-Sicherheitsvorfälle an baden-württembergischen Hochschulen geben sowie den aktuellen Stand der speziell im Hochschulbereich ergriffenen Maßnahmen zur Stärkung der IT-Sicherheit und deren Wirksamkeit beleuchten.

Stellungnahme*)

Mit Schreiben vom 24. Februar 2023 Nr. MWK42-0141.5-33/2/3 nimmt das Ministerium für Wissenschaft, Forschung und Kunst im Einvernehmen mit dem Ministerium des Inneren, für Digitalisierung und Kommunen zu dem Antrag wie folgt Stellung:

Der Landtag wolle beschließen,

die Landesregierung zu ersuchen

zu berichten,

1. wie viele und welche IT-Sicherheitsvorfälle ihr in den letzten fünf Jahren von den Hochschulen des Landes gemeldet wurden;

Die Hochschulen waren in den vergangenen Jahren von folgenden Angriffsformen betroffen: Ransomware-Angriffe, Kryptomining über Trojaner, Phishing-E-Mails. Außerdem stellten folgende große Sicherheitslücken die Hochschulen vor Herausforderungen: log4j, Spring4Shell, Follina-Microsoft-Lücke.

Eine vollständige Auskunft über die Anzahl aller IT-Sicherheitsvorfälle ist – unabhängig des Schweregrades – nur bedingt möglich. 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 gemeldet, die über die zahlreichen täglichen, von den Hochschulen routinemäßig abgewehrten Angriffe hinausgingen.

*) Nach Ablauf der Drei-Wochen-Frist eingegangen.

Der Cybersicherheitsagentur Baden-Württemberg (CSBW) wurden seit ihrer Gründung eine im einstelligen Bereich liegende Zahl an Vorfällen im Hochschulbereich gemeldet. In drei Fällen war die CSBW unterstützend mit forensischer Analyse oder zur Vorbereitung der Wiederherstellung der Systeme tätig.

Die Cyberabwehr des Landesamts für Verfassungsschutz (LfV) registrierte in den letzten Jahren immer wieder Cyberangriffe auf wissenschaftliche Einrichtungen, die einen mutmaßlich nachrichtendienstlichen Hintergrund aufgewiesen haben. 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 und Universitäten. Mit diesen Angriffen sollen persönliche Zugangsdaten von Studierenden oder Mitarbeiterinnen und Mitarbeitern erlangt werden, um anschließend illegal Zugriff auf interne Datenbanken, Wissenssammlungen oder Forschungsergebnisse, z. B. aus unveröffentlichten Dissertationen, zu erlangen. Nach sorgfältiger Abwägung zwischen dem verfassungsrechtlich zu gewährleistenden Informationsinteresse des Landtags und dem öffentlichen Interesse an der Geheimhaltung der genauen Fallzahlen und deren Hintergründe können weitergehende Einzelheiten im Rahmen dieser Beantwortung nicht dargestellt werden. Aus ihrem Bekanntwerden könnten fremde Nachrichtendienste Rückschlüsse auf die Analysefähigkeiten des LfV ziehen und ihre Vorgehensweise hieran gezielt anpassen. Dadurch könnte die Funktionsfähigkeit des LfV beeinträchtigt werden, was sich wiederum schädlich auf die Interessen des Landes Baden-Württemberg auswirken kann.

2. ab welcher Schwere der Sicherheitsvorfälle sie durch die Hochschulen informiert wird;

Wie im Rahmen der Hochschulfinanzierungsvereinbarung II festgelegt, erfolgen Meldungen an das Ministerium für Wissenschaft, Forschung und Kunst bei schwerwiegenden Sicherheitsvorfällen. Die Meldung erfolgt dementsprechend anlassbezogen nach Einschätzung der Hochschulleitung. In der Praxis zählen hierzu signifikante Beeinträchtigungen zentraler Prozesse und kritischer Dienste der Hochschulen. Generell sind die Auswirkungen von IT-Sicherheitsvorfällen sehr unterschiedlich, sodass sich ein genauer Schwellenwert für eine Meldepflicht kaum festlegen lässt.

Unabhängig von einem eventuell festgestellten Schweregrad eines (IT-)Sicherheitsvorfalls haben öffentliche Stellen gemäß § 9 Abs. 1 LVSG die ihnen bekannt gewordenen personenbezogenen Daten und sonstigen Informationen von sich aus, ohne vorheriges Ersuchen, dem LfV zu übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, dass diese Informationen zur Wahrnehmung von Aufgaben nach § 3 Abs. 2 LVSG erforderlich sind. Soweit bei einer Hochschule also der Verdacht besteht, dass ein mutmaßlich nachrichtendienstlich gesteuerter Cyberangriff vorliegen könnte, muss die Cyberabwehr des LfV durch die jeweilige Hochschule, unabhängig vom Schweregerad des Angriffs, informiert werden. Hierdurch wird sichergestellt, dass Vorgehensweisen ausländischer Nachrichtendienste möglichst frühzeitig und umfassend erkannt und bearbeitet werden. Zudem können durch das LfV ebenso potenziell weitere Betroffene frühzeitig informiert und sensibilisiert werden.

3. welche Einschränkungen der IT-Dienste der Hochschulen des Landes in den letzten fünf Jahren aufgrund von Cyberangriffen zu verzeichnen waren und sind;

In den letzten Jahren waren aufgrund von Cyberangriffen Informationen, Daten, Dokumente, Netzwerke, Rechnerressourcen, Kommunikationssysteme und personenbezogene Daten betroffen.

Prinzipiell können Cyberangriffe Hochschulen unterschiedlich stark beeinträchtigen. Wenn ein zentrales System erfolgreich angegriffen wird (z. B. das Identitätsmanagement), können schlimmstenfalls alle IT-Dienste der Institution ausfallen. Wird ein spezifischer Dienst angegriffen (z. B. E-Mail, Campusmanagement), ste-

hen die mit diesem Dienst zusammenhängenden Funktionen nicht mehr zur Verfügung. Angriffe können außerdem auch nur dezentrale Einheiten betreffen, nicht die gesamte Institution. In diesem Fall kommt es zu begrenzten Ausfällen in den jeweils betroffenen Instituten.

4. welche Präventions- und Aufklärungsmaßnahmen zu Informationssicherheit im Hochschulbereich durchgeführt werden;

Die Föderation bwInfoSec bietet den Hochschulen Unterstützung in verschiedenen Schwerpunktbereichen der Informationssicherheit:

– Konkret unterstützt das zentral etablierte Kernteam die Hochschulen beim Aufbau eines Informationssicherheitsmanagementsystems (ISMS) durch das Hosting einer ISMS-Software sowie durch Beratungen. Das ISMS ist ein Grundbaustein für die Verbesserung der Informationssicherheit. Es erfasst strukturiert die IT-Infrastruktur und legt die organisatorischen Prozesse zur Verwaltung, Steuerung und kontinuierlichen Verbesserung der Informationssicherheit fest. Der Austausch zwischen den beteiligten Institutionen erfolgt über regelmäßige Treffen in einer Arbeitsgruppe.
– Auf technischer Ebene unterstützt bwInfoSec die Hochschulen bei der gezielten Prüfung kritischer Systeme und Dienste durch Penetrationstests (Pentests). Hierbei werden aus Angreiferperspektive Schwachstellen gesucht und ausgenutzt, um auf dieser Informationsgrundlage anschließend Angriffsvektoren zu schließen. Die Pentests haben sich an Hochschulen in der Praxis bereits als sehr hilfreich erwiesen.
– Zudem bietet das Kernteam ab dem Jahr 2023 die automatische Durchführung von Schwachstellenscans an. Schwachstellenscans untersuchen, aus Außen- oder Innenperspektive, automatisiert die IT-Infrastruktur von Institutionen auf Sicherheitslücken und Fehlkonfigurationen. Da diese Prüfung automatisiert erfolgt, können, im Gegensatz zu Pentests, große Infrastrukturen umfassend untersucht werden. Ein strukturiertes Schwachstellenmanagement dient dazu, Angriffsflächen systematisch und zeitnah zu verkleinern. Dies leistet einen substanziellen Beitrag zur Prävention von Angriffen.
– Das Kernteam bündelt ferner die Expertisen der beteiligten Institutionen in Arbeitsgruppen. Aktuell wird im Rahmen einer Arbeitsgruppe die Verbreitung von Multifaktorauthentifizierungsverfahren geplant und umgesetzt. Denn besonders häufig sind schlecht gesicherte Accounts Einfallstore für Angreiferinnen und Angreifer. Die Absicherung von Zugängen durch einen weiteren Faktor (bspw. einen Fingerabdruck oder einen Code auf dem Smartphone), der Nutzernamen und Passwort ergänzt, erschwert Angriffe deutlich. Weitere Arbeitsgruppen befassen sich mit dem Erstellen einer Informationssicherheitsleitlinie sowie der Sensibilisierung von Mitarbeiterinnen und Mitarbeiter.
– Um Mitarbeiterinnen und Mitarbeiter über die Gefahren des digitalen Raums aufzuklären, besteht vonseiten bwInfoSec das Angebot an die Hochschulen, praxisorientierte Awareness-Schulungen durchzuführen. Hierdurch werden Mitarbeiterinnen und Mitarbeiter zu Themen wie Social Engineering (Phishing) sensibilisiert, um langfristig diese Angriffsformen sicher identifizieren zu können. Da viele Cyberangriffe menschliche Schwachstellen ausnutzen, kann so ein signifikanter Beitrag zur Informationssicherheit an Hochschulen geleistet werden.

  Diese laufenden Anstrengungen werden stetig ausgebaut.

Im Zusammenhang mit Hochschulen war zudem die Zentrale Ansprechstelle Cybercrime (ZAC) beim Landeskriminalamt Baden-Württemberg 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.

Im Übrigen wird hinsichtlich weiterer Maßnahmen der Landesverwaltung auf die Stellungnahme zu den Ziffern 9 bis 11 der Kleinen Anfrage der Abg. Dennis Birnstock und Daniel Karrais u. a. FDP/DVP (Drucksache 17/4022) verwiesen.

5. wie der Umsetzungsstand der Maßnahmen zur Stärkung der Informationssicherheit an Hochschulen ist, die in der Hochschulfinanzierungsvereinbarung II festgeschrieben wurden;

Um den wachsenden Herausforderungen im Bereich der Informationssicherheit zu begegnen, wurde im engen Austausch zwischen Hochschulen und dem Ministerium für Wissenschaft, Forschung und Kunst bereits im Jahr 2018 das Rahmenkonzept Informationssicherheit bwInfoSec erarbeitet. Zur Stärkung der Hochschulen wurden durch die Landesregierung in den Doppelhaushalten 2018/2019 und 2020/2021 58 neue Informationssicherheitsstellen geschaffen. Hierdurch wurden die einzelnen Institutionen personell erheblich gestärkt. Durch die im Rahmenkonzept festgelegten Maßnahmen wird die Informationssicherheit substanziell und nachhaltig verbessert. Es ist gleichzeitig das Gründungsdokument der bundesweit einzigartigen Föderation bwInfoSec zur hochschulübergreifenden Synergiebildung im Bereich Informationssicherheit. In ihrem Rahmen tauschen sich Vertreterinnen und Vertreter der Hochschulen regelmäßig mit anderen Akteuren aus der Politik (bspw. dem Ministerium für Wissenschaft, Forschung und Kunst sowie der CSBW) aus. Die strategische Ausrichtung der Föderation obliegt dem Steuerkreis bwInfoSec, in dem Hochschulen und das Ministerium für Wissenschaft, Forschung und Kunst repräsentiert sind. In den zweiwöchentlich stattfindenden Sitzungen des Steuerkreises Informationssicherheit werden aktuelle Sicherheitsvorfälle behandelt und die Umsetzung der laufenden Projekte zur Verbesserung der Informationssicherheit durch das Kernteam koordiniert.

Das Kernteam Informationssicherheit wurde im Jahr 2021 gegründet und bearbeitet seither gebündelt zentrale Aufgaben und Herausforderungen für die Hochschulen. Außerdem werden Dienste zur Verbesserung der Informationssicherheit zur Verfügung stellt und Beratungen hierzu durchgeführt (siehe Antwort auf Ziffer 4). Das Kernteam besteht aus insgesamt 12 Mitarbeiterinnen und Mitarbeitern (jeweils sechs an der Universität Heidelberg und am Hochschulservicezentrum Baden-Württemberg in Reutlingen [HSZ]).

6. wie sich die Zusammenarbeit der Hochschulen mit den weiteren Stellen und Einrichtungen zur IT-Sicherheit gestaltet, insbesondere mit der Cybersicherheitsagentur und dem Bundesamt für Sicherheit in der Informationstechnik;

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. Vertreten durch die Sprecherinnen und Sprecher stellt er Kontakt zu den unterschiedlichen Akteuren her und lotet Kooperationspotenziale aus. In diesem Kontext bestehen Kooperationen in bilateralen Formaten – insbesondere mit der CSBW und dem Wissenschaftsnetzwerk BelWü – sowie mit multilateralen Kooperationsprojekten (bspw. bwCampusNetz – in diesem arbeiten mehrere Universitäten unter Leitung des Karlsruher Instituts für Technologie [KIT] zusammen, um die Campusnetze der Universitäten näher zu beleuchten). Die Hochschulen werden durch die CSBW regelmäßig über aktuelle Gefahrenlagen informiert. Hierzu zählen auch Mitteilungen zu Präventionsmaßnahmen und zur Detektion verdächtiger Aktivitäten. Nach der Übernahme des Computer Emergency Response Team des Landes (CERT BWL) ist die CSBW zudem in Krisenfällen einer der ersten Ansprechpartner für Hochschulen. Um die Kooperation mit Hochschulen zu intensivieren und zu verstetigen, besteht aktuell eine Arbeitsgruppe aus der Föderation bwInfoSec und Vertreterinnen und Vertretern der CSBW.

Um die Zusammenarbeit auf operativer, strategische und taktischer Ebene weiter auszugestalten, soll dazu zwischen dem Hochschulbereich und der CSBW eine Vereinbarung i. S. d. § 2 Absatz 2 Satz 2 des Cybersicherheitsgesetzes Baden-Württemberg geschlossen werden.

Ferner vernetzt bwInfoSec die beteiligten Institutionen hochschulartübergreifend in verschiedenen Arbeitsgruppen, beispielsweise zur Multifaktorauthentifizierung, zum Aufbau eines ISMS, zu Formulierung einer Informationssicherheitsleitlinie und zur Sensibilisierung von Mitarbeiterinnen und Mitarbeitern. 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. Die Hochschulen sind demnach über Institutionen hinweg mit den relevanten Akteuren auf Landesebene vernetzt.

Zudem bestehen institutionsübergreifende Kooperationen zwischen den Informationssicherheitsbeauftragten der Hochschulen. Auch der Arbeitskreis der Leiterinnen und Leiter der wissenschaftlichen Rechenzentren (ALWR) steht im engen Austausch mit der Föderation bwInfoSec und widmet sich regelmäßig Themen der Informationssicherheit.

Die CSBW steht als zentrale Koordinierungsstelle in Belangen der Cybersicherheit und zur Lageerfassung stets in engem Kontakt mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI), den CERTs des Bundes und der Länder und weiteren Institutionen wie dem Nationalen Cyber-Abwehrzentrum. Darüber hinaus steht die CSBW mit allen Behörden und den Rechenzenten der Landesverwaltung in einem regelmäßigen und konstruktiven Austausch. Hierzu zählen u. a. das Landeskriminalamt Baden-Württemberg (LKA), das LfV, die Landesoberbehörde IT Baden-Württemberg (BITBW), das Sicherheitszentrum IT in der Finanzverwaltung (SITiF BW), die Komm.ONE AöR sowie weitere Dienstleister der Behörden im IT-Sektor.

Durch ein permanentes Monitoring einschlägiger öffentlicher Quellen, aber auch von Quellen im Darknet erfasst die CSBW zudem relevante Informationen über Schwachstellen und Sicherheitsvorfälle. Die sodann erfassten Informationen werden von den Sicherheitsexpertinnen und -experten der CSBW analysiert und bewertet und in Form von Warnmeldungen, teils ergänzt um Handlungsempfehlungen u. a. den Sicherheitsverantwortlichen der Hochschulen im Land zur Verfügung gestellt.

Nach einem Cyberangriff steht den Hochschulen die CSBW mit dem CERT BWL als Anlaufstelle zur Verfügung. Mehrere Hochschulen wurden im letzten Jahr bei der Bewältigung von IT-Sicherheitsvorfällen und sicherheitskritischen Ereignissen durch die CSBW unterstützt. Die Unterstützung umfasst dabei u. a. den Bereich der Koordination der Fallbehandlung, die technische Bearbeitung, die Krisenkommunikation sowie die Unterstützung bei der Wiederherstellung zur sicheren Wiederinbetriebnahme der Systeme. Nach einer ersten Fern-Analyse wird bei entsprechender Indikation das Mobile Incident Response Team (MIRT) der CSBW entsandt. Dieses bearbeitet den Vorfall, bis die kritische Phase überwunden und beispielsweise ein Abfluss von Daten oder einer Ausweitung des Schadens ausgeschlossen werden kann. Dabei wird u. a. analysiert, wie weit der Angreifer sich im Netzwerk ausbreiten konnte. Dabei arbeiten die Vorfalls-Experten der CSBW eng mit den IT-Verantwortlichen der Hochschulen zusammen, um die notwendigen Informationen zu den jeweils vorliegenden komplexen IT-Infrastrukturen zu berücksichtigen und auch um die zu ergreifenden Schritte im Hinblick auf einen potentiellen Wiederaufbau optimal abstimmen zu können.

Weiter ist die CSBW dualer Partner der DHBW Heilbronn und stellt im Jahr 2023 zwei Studienplätze der Fachrichtung Wirtschaftsinformatik mit dem Schwerpunkt Software Engineering zur Verfügung. Die Ausbildungskooperation besteht gemeinsam mit dem LKA und der EnBW AG. Teil dieser Kooperation ist ein Austauschprogramm, in dessen Rahmen die dualen Studierenden zwei Praxisphasen bei einem der Kooperationspartner verbringen.

Im Übrigen wird auf die Stellungnahme zu den Ziffern 9 bis 11 der Kleinen Anfrage der Abg. Dennis Birnstock und Daniel Karrais u. a. FDP/DVP (Drucksache 17/4022) verwiesen.

7. welche Bereiche der IT-Sicherheit der Hochschulen von dem Informationssicherheitsnetzwerk abgedeckt und bearbeitet werden, das 2018 gegründet wurde;

Die durch bwInfoSec abgedeckten Bereiche umfassen sowohl organisatorisch-institutionelle Themen als auch technische Aspekte. Im Fokus stehen dabei immer die Hochschulen als Gesamtinstitutionen, nicht nur einzelne dezentrale Organisationseinheiten.

Folgende organisatorisch-institutionellen Themen werden durch bwInfoSec abgedeckt:

– Die Föderation bwInfoSec unterstützt die Hochschulen beim Aufbau eines Informationssicherheitsmanagementsystems (ISMS) durch das Hosting einer ISMS-Software sowie durch Beratungen. Das ISMS ist ein Grundbaustein für die Verbesserung der Informationssicherheit. Es erfasst strukturiert die IT-Infrastruktur und legt die organisatorischen Prozesse zur Verwaltung, Steuerung und kontinuierlichen Verbesserung der Informationssicherheit fest.
– Mehrere Arbeitsgruppen befassen sich mit dem Aufbau eines ISMS, dem Erstellen einer Informationssicherheitsleitlinie sowie der Sensibilisierung von Mitarbeiterinnen und Mitarbeitern. Zudem organisiert das Kernteam regelmäßig Schulungen zum Grundschutz des BSI, konkret zum BSI IT-Grundschutz Praktiker sowie zum BSI IT-Grundschutz Berater, die allen Hochschulen vergünstigt angeboten werden.

Folgende technische Bereiche werden durch bwInfoSec abgedeckt:

– bwInfoSec unterstützt die Hochschulen bei der gezielten Prüfung kritischer Systeme und Dienste durch Pentests (s. Ziffer 4).
– Zudem bietet das Kernteam die Durchführung von Schwachstellenscans an (s. Ziffer 4).
– Eine Arbeitsgruppe beschäftigt sich mit der Etablierung von Multifaktorauthentifizierungsverfahren an Hochschulen. Denn besonders häufig sind schlecht gesicherte Accounts Einfallstore für Angreiferinnen und Angreifern. Die Absicherung von Zugängen durch einen weiteren Faktor (bspw. einen Fingerabdruck oder einen Code auf dem Smartphone), der Nutzernamen und Passwort ergänzt, erschwert Angriffe deutlich.

8. welche Ergebnisse die Evaluation des Gesamtkonzepts des Informationssicherheitsnetzwerks hatte;

Die Evaluation des Gesamtkonzeptes des Informationssicherheitsnetzwerks wird bis Ende des Jahres 2023 erfolgen.

9. wie sie die Bedrohungslage für die IT-Sicherheit der Hochschulen aktuell bewertet und welche Konsequenzen sie daraus für das Gesamtkonzept Informationssicherheit an Hochschulen zieht.

Immer wieder verdeutlichen derzeit erfolgreiche Cyberangriffe die hohe Bedrohungslage im Bereich der IT-Sicherheit. Auch Hochschulen sind mit dieser Herausforderung täglich konfrontiert. Im Gegensatz zu Unternehmen oder anderen öffentlichen Einrichtungen mit klaren hierarchischen Strukturen stehen Hochschulen hier vor weiteren, besonderen Aufgaben. Auch aufgrund der heterogenen und über Jahrzehnte gewachsenen Informationsinfrastrukturen sind Hochschulen durchaus Ziele für Angreiferinnen und Angreifer. Das Spannungsverhältnis einer offenen akademischen Gemeinschaft mit zahlreichen Diensten für Studierende und Mitarbeiterinnen und Mitarbeiter bietet Angreifern teilweise Möglichkeiten zur Durchführung von Angriffen. Dies erfordert oft ein Abwägen zwischen Sicherheit und offener, freier Forschung und Lehre. Hochschulen stehen in diesem Kontext daher vor besonderen Herausforderungen, um neben der Sicherheit auch die freie Forschung und Lehre zu gewährleisten. Die Aktivitäten im Rahmen der Föderation bwInfoSec werden daher ausgebaut und intensiviert.

Die CSBW schätzt die Bedrohungslage nach wie vor als hoch ein. Die geplante Intensivierung und Verstetigung der Zusammenarbeit der Hochschulen und der CSBW ist daher geboten. Auch die Cyberabwehr des LfV registriert bereits seit Jahren eine hohe, abstrakte Gefährdungssituation in Bezug auf mögliche Cyberangriffe mit nachrichtendienstlichem Hintergrund. Durch den völkerrechtswidrigen Angriffskrieg der Russischen Föderation auf die Ukraine im Februar 2022 hat sich diese Gefährdungslage weiter erhöht.

Wie bereits unter Ziffer 1 dargestellt, stehen wissenschaftliche Einrichtungen dabei ebenfalls im Fokus fremdstaatlich gelenkter oder nachrichtendienstlich gesteuerter Angriffsgruppierungen. Besonders relevant für diese Gruppierungen sind dabei noch unveröffentlichte Forschungsergebnisse, Dissertationen oder sonstige wissenschaftliche Informationen aus dem Bereich der Hochtechnologie, welche beispielsweise aufgrund von staatlichen Sanktionen oder Embargobestimmungen nicht auf legalem Wege beschafft werden können.

Die Cyberabwehr des LfV empfiehlt wissenschaftlichen Einrichtungen präventiv die Umsetzung zahlreicher Schutzmaßnahmen zur Stärkung der Resilienz ihrer IT-Systeme. Hierzu gehören u. a. regelmäßige Sensibilisierungen der Beschäftigten und Studierenden zur Verwendung sicherer Zugangsdaten und zur Erkennung eventueller Phishing-Angriffe. Die bedarfsgerechte Übermittlung von Steckbriefen zu verschiedenen Angriffsgruppierungen oder Warnmeldungen zu aktuellen Angriffskampagnen gewährleisten, dass mögliche Angriffsversuche möglichst frühzeitig erkannt werden können. Schließlich können durch die Cyberabwehr auch Beratungsleistungen bei der Optimierung der internen Vorgaben zur Verbesserung der Informationssicherheit der jeweiligen wissenschaftlichen Einrichtung erfolgen.

Olschowski

Ministerin für Wissenschaft,
Forschung und Kunst