Landtag von Baden-Württemberg **Drucksache 16 / 5298**

16. Wahlperiode **03. 12. 2018**

Antrag

der Abg. Nese Erikli u. a. GRÜNE

und

Stellungnahme

des Ministeriums für Wissenschaft, Forschung und Kunst

Informationssicherheit baden-württembergischer Hochschulen und außeruniversitärer Forschungseinrichtungen

Antrag

Der Landtag wolle beschließen,

die Landesregierung zu ersuchen

zu berichten,

1. welche Informationen der Landesregierung über die Anzahl der Cyberangriffe auf Hochschulen und außeruniversitäre Forschungseinrichtungen in Baden-Württemberg innerhalb der letzten fünf Jahre vorliegen;

2. über welche Erkenntnisse die Landesregierung hinsichtlich der Frage verfügt, ob bei den ihr bekannten Angriffen bestimmte Forschungsfelder stärker von Cyberattacken betroffen sind als andere;

3. welche Erkenntnisse der Landesregierung über die Urheber dieser Angriffe vorliegen;

4. wie sich die finanziellen Mittel, die das Land den Hochschulen und außeruniversitären Forschungseinrichtungen explizit für die Informationssicherheit zur Verfügung stellt, in den letzten fünf Jahren entwickelt haben;

5. wie viele Vollzeitstellen aktuell in der IT-Sicherheit an baden-württembergischen Hochschulen und außeruniversitären Forschungseinrichtungen besetzt sind (bitte nach Hochschule und Forschungseinrichtung getrennt auflisten);

6. inwieweit die Rechenzentren der Hochschulen und Universitäten im Land eigene CERTs (Computer Emergency Response Team) eingerichtet haben, wie diese zusammenarbeiten und welche Auswirkungen sich daraus auf den Ressourcenbedarf ergeben;

Eingegangen: 03. 12. 2018 / Ausgegeben: 25. 01. 2019

7. welche Maßnahmen zur Verbesserung eines zentralen Monitorings von Cyberattacken auf Hochschulen und außeruniversitäre Forschungseinrichtungen von der Landesregierung ergriffen wurden und welche für die Zukunft geplant sind;

8. welche Maßnahmen darüber hinaus vonseiten der Landesregierung geplant sind, um die IT-Sicherheit an baden-württembergischen Hochschulen und außeruniversitären Forschungseinrichtungen zu erhöhen;

9. ob mittlerweile eine Entscheidung getroffen wurde in der Frage, in welchem Umfang die Verwaltungsvorschrift Informationssicherheit des Innenministeriums an den Hochschulen umzusetzen ist.

03. 12. 2018

Erikli, Salomon, Filius, Manfred Kern,
Lösch, Marwein, Seemann GRÜNE

Begründung

Baden-Württemberg ist in hohem Maße auf seine Innovationskraft angewiesen. Kaum eine Region in Europa verfügt über eine so große Zahl an Forschungseinrichtungen. Diese legen den Grundstein für den Wohlstand unseres Landes und sollten daher unter besonderen Schutz, auch im Bereich der IT-Sicherheit, gestellt werden.

Einige Maßnahmen zur Verbesserung der IT-Sicherheit und zur Abwehr von Cyberangriffen werden in Drucksache 16/2793 (Antrag der Abg. Klaus Hoher u. a. FDP/DVP) aus dem Herbst 2017 dargestellt. Den Antragstellern geht es mit dem vorliegenden Antrag auch um ein Update hinsichtlich der in diesem Antrag erst angedeuteten Planungen.

Stellungnahme

Mit Schreiben vom 2. Januar 2019 Nr. 34-0275.6/31/1 nimmt das Ministerium für Wissenschaft, Forschung und Kunst in Abstimmung mit 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. welche Informationen der Landesregierung über die Anzahl der Cyberangriffe auf Hochschulen und außeruniversitäre Forschungseinrichtungen in Baden-Württemberg innerhalb der letzten fünf Jahre vorliegen;

Hochschulen[1] sind ihrem Auftrag und Selbstverständnis nach „offene“ Systeme, die der Kommunikation mit der Öffentlichkeit und mit internationalen (Forschungs-) Communities verpflichtet sind. Dies führt dazu, dass es dort neben besonders geschützten Bereichen (Studierenden-/Verwaltung, zentrale IT-Serverdienste, Bibliotheksdienste) auch eine breite und diversifizierte dezentrale IT-Struktur gibt.

[1] Der Begriff Hochschule umfasst im Folgenden auch das Karlsruhe Institute of Technology.

Für Angreifer ist diese IT-Landschaft attraktiv, insbesondere um IT-Ressourcen zum Versenden von Spam- und Phishing-Mails zu nutzen oder die schnellen Internetverbindungen für illegales File Sharing zu missbrauchen.

Auf die Hochschulen erfolgen dementsprechend täglich tausendfach Cyberangriffe im weitesten Sinne, wie Portscans, SPAM-Mails oder Phishing-Angriffe. Dabei wird von den Hochschulen eine Zunahme der Häufigkeit und Intensität dieser Angriffe beobachtet, ohne dass dazu ein detailliertes Monitoring unternommen wird bzw. mangels personeller und finanzieller Kapazitäten unternommen werden kann.

Schwerwiegende Angriffe auf Netzwerke oder in Form von Verschlüsselungstrojanern hielten sich in den letzten fünf Jahren im einstelligen Bereich. So wurde an einer Hochschule für angewandte Wissenschaften im Jahr 2018 erstmalig ein Account durch eine Phishing-Attacke übernommen.

Die außeruniversitären Forschungseinrichtungen sind wie Unternehmen auch täglich einer Vielzahl von Angriffsversuchen ausgesetzt, die aber von Sicherheitssoftware zumeist schnell erkannt und automatisch abgewiesen werden. Im Folgenden wird daher lediglich auf gezielte bzw. gravierende Cyberangriffe eingegangen.

Die Institute der Innovationsallianz Baden-Württemberg berichteten der Landesregierung von insgesamt fünf gezielten Cyberangriffen in den vergangenen fünf Jahren. In einem Fall zielten die Angreifer darauf ab, Passwörter durch vielfaches, automatisiertes Ausprobieren zu erraten (sog. Brute-Force-Angriff). In zwei Fällen richteten sich die Angriffe gegen die Telefonanlage. In zwei weiteren Fällen versuchten Angreifer mittels gefälschter E-Mails und Telefonanrufe, Verwaltungsmitarbeiter dazu zu bewegen, Geld auf unbekannte Konten zu überweisen (sog. CEO-Fraud). In keinem Fall erlangten die Angreifer Zugriff auf Forschungsergebnisse oder andere sensible Informationen.

Das Deutsche Zentrum für Luft- und Raumfahrt (DLR) veröffentlicht keine Angaben zu konkreten Vorfällen und zur Anzahl der Cyberangriffe auf seine Standorte und Institute in Baden-Württemberg. Laut Auskunft der zentralen IT-Sicherheit des DLR liegt der Fokus von Cyberangriffen auf der zentralen IT-Infrastruktur des DLR, welche nicht in Baden-Württemberg angesiedelt ist. Ein spezifischer Bezug von Angriffen auf die IT-Infrastruktur in Baden-Württemberg ist nicht zu erkennen.

In den vergangenen fünf Jahren wurden etwa 50 gravierendere Angriffe auf die baden-württembergische Fraunhofer-Institute gemeldet und analysiert. In Einzelfällen gab es Hinweise oder Verdachtsmomente auf nachrichtendienstlichen Hintergrund. Ob diese Angriffe auf Wissenschaftsspionage zielten oder andere Ziele wie die vorbereitende Infiltration von Kommunikationsnetzen hatten, konnte nicht eindeutig nachvollzogen werden. Diesbezüglich verfügt Fraunhofer über keine eigenen Erkenntnisse, die über die des Verfassungsschutzes hinausgehen.

Beim Landesamt für Verfassungsschutz (LfV) sind in den vergangenen Jahren zahlreiche Hinweise zu mutmaßlich nachrichtendienstlich gesteuerten Cyber-Spionageangriffen gegen Hochschulen und Forschungseinrichtungen eingegangen. In den vergangenen fünf Jahren konnten acht akademische Einrichtungen im Land identifiziert werden, die mit hoher Wahrscheinlichkeit Opfer solcher Attacken geworden sind. Die eindeutige Nachweisführung im Einzelfall war insbesondere mangels fehlender Netzwerkprotokolldaten der betroffenen Systeme zum Teil nicht mehr möglich, ein Datenabfluss nicht oder nicht mehr feststellbar. Von einer hohen Dunkelziffer ist auszugehen.

Das LfV ist bestrebt, unmittelbar nach Kenntniserlangung über neue Cyberangriffswellen eine zeitnahe Informationsweitergabe zu gewährleisten, um so eine Sensibilisierung aller potenziell Betroffenensicherzustellen. Diese erfolgt in der Regel in Form von elektronischen Warnmeldungen. Bei Hinweisen auf eine mögliche Betroffenheit von Hochschulen und Universitäten wurden mittlerweile direkte Meldewege mit dem Ministerium für Wissenschaft, Forschung und Kunst vereinbart und festgelegt.

Der Polizeilichen Kriminalstatistik (PKS) lassen sich keine belastbaren Zahlen zu aktuellen und vergangenen Cyberangriffen auf Hochschulen und außeruniversitäre Forschungseinrichtungen entnehmen, da systembedingt nicht nach der Art der Geschädigten recherchiert werden kann.

2. über welche Erkenntnisse die Landesregierung hinsichtlich der Frage verfügt, ob bei den ihr bekannten Angriffen bestimmte Forschungsfelder stärker von Cyberangriffen bedroht sind als andere;

Auch mangels eines detaillierten Monitorings konnten Angriffsmuster auf bestimmte Forschungsfelder überwiegend nicht registriert werden. Eine Universität hat gezielte Angriffe auf ingenieurwissenschaftliche Forschungsbereiche verzeichnet.

Nach Erkenntnissen des LfV stehen Forschungsfelder, die Hochtechnologiebereiche umfassen, grundsätzlich im Fokus fremder Nachrichtendienste. In der Vergangenheit konnte eine Zunahme von Cyber-Spionageangriffen gegen Einrichtungen beobachtet werden, die im Bereich der Energietechnik forschen bzw. tätig sind. Zum einen geht es um Know-how-Abfluss, zum anderen könnten fremde Nachrichtendienste mit Angriffen gegen solche Forschungseinrichtungen aber auch das Ziel verfolgen, weitere Hinweise auf potenzielle Opfer zu generieren oder deren IT-Netze als Angriffsinfrastruktur zu missbrauchen.

In der Vergangenheit konnte etwa ein besonderes Interesse an naturwissenschaftlichen Fakultäten festgestellt werden, die Forschung in Hochtechnologiebereichen oder der Energietechnik betreiben. Zudem standen unveröffentlichte Dissertationen und Forschungsergebnisse im Fokus fremder Nachrichtendienste. Als Hintergrund dieser Angriffe wird u. a. der Diebstahl geistigen Eigentums zur Umgehung bestehender Sanktionen vermutet.

3. welche Erkenntnisse der Landesregierung über die Urheber dieser Angriffe vorliegen;

Mangels Ressourcen erfolgt in der Regel keine systematische forensische Analyse. Sie wäre sehr aufwendig, da die Angreifer ihre Herkunft zumeist aktiv verschleiern. Einzelne schwerwiegende Angriffe wurden zur Anzeige gebracht. Die Fahndungserkenntnisse liegen den Strafverfolgungsbehörden vor.

Eine exakte Attribution von Cyberangriffen zu einem fremden Nachrichtendienst ist laut LfV überaus schwierig. Im Bereich staatlich gesteuerter Cyberangriffe ist mit Blick auf die Angriffsmittel und Angriffsmethoden von einem hochprofessionellen, konspirativen und gezielten Vorgehen der Angreifer auszugehen. Hinzu kommt, dass in Bezug auf das Aufklärungsinteresse fremder Staaten oftmals Interessenüberschneidungen zu erkennen sind.

Im Jahr 2017 erlangte das LfV Hinweise zu einer groß angelegten Spear-Phishing-Kampagne gegen Hochschulen und Forschungseinrichtungen westlicher Staaten, darunter auch Erkenntnisse zu mehreren mutmaßlich betroffenen Einrichtungen mit Sitz in Baden-Württemberg. Von einem staatlich gesteuerten Cyberangriff ist auszugehen. In diesem Zusammenhang wurde durch das US-Departement of Justice inzwischen Anklage gegen neun iranische Staatsbürger sowie gegen die iranische Organisation „Mabna Institute“ erhoben, die in Zusammenhang mit diesem Angriff stehen sollen. Die Verfassungsschutzbehörden beobachten seit längerem einen maßgeblichen Ausbau der iranischen Cyberfähigkeiten mit verschiedenen Zielrichtungen.

Bei anderen Angriffen, insbesondere bei solchen, die sich gegen Forschungseinrichtungen mit Verbindungen zum Energiesektor richteten, deuten Anhaltspunkte darauf hin, dass es sich hierbei um mutmaßlich staatlich gesteuerte Cyberspionagegruppen mit russischem Hintergrund handelt. Insbesondere die russischen staatlichen Stellen zuzuordnende Cyberangriffskampagne „APT 29“ wie auch die, vermutlich vom russischen Nachrichtendienst FSB gelenkte, Cyberangriffskampagne „Snake“ (alias „Uroburos“, alias „Turla“) zielen vorwiegend auch auf die Bereiche Energie und Energietechnik ab.

4. wie sich die finanziellen Mittel, die das Land den Hochschulen und außeruniversitären Forschungseinrichtungen explizit für die IT-Sicherheit zur Verfügung stellt, in den letzten fünf Jahren entwickelt haben;

In den Globalhaushalten der Hochschulen sind keine expliziten Mittel für das Thema IT- oder allgemein für die Informationssicherheit ausgewiesen. Dies gilt

gleichermaßen für die außeruniversitären Forschungseinrichtungen im Geschäftsbereich des Wissenschaftsministeriums. Vielmehr liegt es in der Zuständigkeit und Verantwortlichkeit der Hochschulleitungen, die notwendigen Ressourcen für dieses zunehmend wichtige Thema bereitzustellen. Die Hochschulen verweisen diesbezüglich allerdings auf Zielkonflikte, da mangels frei verfügbarer Reserven Gelder für Wissenschaft und Forschung umgewidmet werden müssen.

Um die Grundlagenarbeit zu unterstützen, hat das Wissenschaftsministerium in den Jahren 2015 bis 2017 den Universitäten des Landes insgesamt 1,5 Mio. Euro für die Konzeption einer kooperativen IT-Sicherheitsstruktur zur Verfügung gestellt. Zudem werden in den Haushalten 2018 und 2019 insgesamt zwölf Stellen bereitgestellt, um ein Informationssicherheitsmanagement an den Hochschulen sowie den Kunst- und Kultureinrichtungen voranzubringen.

Die Gewährleistung der IT-Sicherheit ist eine wichtige Verwaltungsaufgabe der außeruniversitären Einrichtungen 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.

5. wie viele Vollzeitstellen aktuell in der IT-Sicherheit an baden-württembergischen Hochschulen und außeruniversitären Forschungseinrichtungen besetzt sind (bitte nach Hochschule und Forschungseinrichtung getrennt auflisten);

An sieben von neun Universitäten werden Personalkapazitäten im Umfang von einem Vollzeitäquivalent (VZÄ) oder mehr für den Bereich IT-Sicherheit bzw. den umfassenderen Bereich Informationssicherheit bereitgestellt. An zwei Universität sind es 1 VZÄ, an drei Universitäten sind es 1,5 VZÄ, 1,75 VZÄ bzw. 2 VZÄ und an zwei weiteren Universitäten, die zugleich ein CERT betreiben, sind es 3 VZÄ bzw. 6 VZÄ.

An den Pädagogischen Hochschulen, der Duale Hochschule und den nichtuniversitären Hochschulen erreichen die eingesetzten Stellenanteile jeweils nicht den Umfang eines Vollzeitäquivalents mit Ausnahme von zwei Hochschulen für Angewandte Forschung.

Am Deutschen Krebsforschungszentrum sind zwei Vollzeitstellen besetzt, eine weitere ist ausgeschrieben.

Beim FZI Forschungszentrum Informatik Karlsruhe sind aktuell acht Mitarbeiterinnen und Mitarbeiter im Bereich der unternehmensinternen IT eingesetzt, die allesamt über weitgehende sicherheitstechnische Kenntnisse verfügen. Weiterhin sind am FZI 16 Mitarbeiterinnen und Mitarbeiter für externe Forschungsprojekte zur IT-Sicherheit beschäftigt. Bei den anderen Forschungsinstituten der Innovationsallianz Baden-Württemberg sind ebenfalls Mitarbeiter für die IT-Sicherheit beschäftigt, deren Grad der Inanspruchnahme – ja nach Größe des Instituts – von 0,5 bis 1 Vollzeitstelle reicht.

Zur personalpolitischen Situation im Bereich IT-Sicherheit veröffentlicht das DLR keine Angaben. Eine solche Angabe wäre ohnehin nicht aussagekräftig, da das DLR seine IT-Infrastruktur und damit auch Aufgaben im Bereich IT-Sicherheit größtenteils an externe Dienstleister ausgelagert hat und es diesen Dienstleistern obliegt, die Zahl der im Bereich IT-Sicherheit (vollzeit-)beschäftigten Mitarbeiter selbst angemessen zu steuern.

Alle Fraunhofer-Institute haben Informationssicherheits-Beauftragte. Diese sind je nach Institutsgröße und Schwerpunkt mit ca. 30 bis 100 % ihrer Arbeitszeit für IT-Sicherheit im IT-Betrieb des jeweiligen Instituts tätig, im Schnitt etwa 0,5 Stellen pro Institut. Dazu kommen anteilig Stellen, die für alle nationalen Standorte verantwortlich sind; umgerechnet auf Baden-Württemberg ergeben sich etwa 1,5 Stellen. Auf diese Weise kann für die in Baden-Württemberg ansässigen Fraunhofer Institute rechnerisch ein Äquivalent zu rd. neun Vollzeitstellen ermittelt werden.

6. wieweit die Rechenzentren der Hochschulen und Universitäten im Land eigene CERTs (Computer Emergency Response Team) eingerichtet haben, wie diese zusammenarbeiten und welche Auswirkungen sich daraus auf den Ressourcenbedarf ergeben;

Zum jetzigen Zeitpunkt verfügen drei Universitäten über Einrichtungen mit der expliziten Benennung und dem expliziten Auftrag eines CERTs. Sie kooperieren miteinander sowie in nationalen und internationalen Verbundstrukturen für das IT- bzw. Informationssicherheitsmanagement. Durch die Mitwirkung im Arbeitskreis Informationssicherheit der deutschen Forschungseinrichtungen (AKIF) findet eine fachliche Vernetzung sowie die Abstimmung von Gefahren- und Risikobewertungen und Handlungsmaßnahmen statt. Der lokale Aufwand zur Aufrechterhaltung der operativen IT-Sicherheit bleibt jedoch trotz Vernetzungen und Zusammenarbeit erhalten und entfällt nicht gänzlich.

An den Pädagogischen Hochschulen, der Dualen Hochschule und den nichtuniversitären Hochschulen sind mangels Personalkapazität bislang keine CERTs eingerichtet, obwohl dies für sinnvoll und notwendig erachtet wird. Bis auf Weiteres werten die Hochschulen die Meldungen u. a. der CERTs des Deutschen Forschungsnetzes (DFN) und des CERT BWL aus.

7. welche Maßnahmen zur Verbesserung eines zentralen Monitorings von Cyberattacken auf Hochschulen und außeruniversitäre Forschungseinrichtungen von der Landesregierung ergriffen wurden und welche für die Zukunft geplant sind;

Mit der Besetzung der dem Wissenschaftsministerium für das Thema Informationssicherheit zugewiesenen Stellen ist mit dem Aufbau eines zentralen Monitorings von Cyberattacken auf Hochschulen begonnen worden. Eine Ansprechpartnerin für Informationssicherheit im Hochschulbereich agiert in enger Abstimmung mit den Hochschulen. In einem ersten Schritt wurden Meldewege von und zu den Hochschulen aufgebaut, nachdem diese nach Aufforderung des Wissenschaftsministeriums jeweils einen Informationssicherheitsbeauftragten bzw. eine Informationssicherheitsbeauftragte benannt haben.

Darüber hinaus ist geplant, die zwölf dem Wissenschaftsministerium für 2018 und 2019 zugewiesenen Stellen zur Stärkung der Informationssicherheit an den Hochschulen und Kunst- und Kultureinrichtungen (vgl. Frage 4) zu bündeln und zwei miteinander vernetzte Kompetenzteams zu etablieren, die einerseits die Universitäten, andererseits die vom Hochschulservicezentrum in Reutlingen (HSZ) betreuten Hochschulen und Einrichtungen unterstützen.

8. welche Maßnahmen darüber hinaus vonseiten der Landesregierung geplant sind, um die IT-Sicherheit an baden-württembergischen Hochschulen und außeruniversitären Forschungseinrichtungen zu erhöhen;

Aufgabe der in der Antwort zu Frage 7 genannten Kompetenzteams wird es sein, Anforderungen der Informationssicherheit, die übergreifend oder zentral erfüllt werden können, zu identifizieren und für die Gesamtheit der Hochschulen und Einrichtungen zu bearbeiten. Das beginnt mit der Verankerung der Informationssicherheit als Aspekt der Prozessqualität in den Hochschulen, der nicht nur rechtlich gefordert ist, sondern auch eine Gestaltungsaufgabe im Rahmen der Governance-Struktur und der institutionellen Awareness darstellt. Entsprechende Sensibilisierungsaktivitäten sollen von den Kompetenzteams genauso wie Schulungsmaßnahmen oder Kommunikationskonzepte für Störfälle konzipiert werden. Des Weiteren ist geplant, neben dem technischen Erfahrungsaustausch und der Erprobung neuer Sicherheitstechnologien insbesondere das Notfallmanagement mit der Identifizierung und Kommunikation von Schwachstellen und Vorfallsursachen im Sinne eines gemeinsamen CERT der Hochschulen so auszubauen, dass lokale Notfallteams wirksam unterstützt werden können. Auch kann in dem Verbund über Peer-Audits nachgedacht werden, mit denen die Hochschulen gegenseitig ihren Stand der Informationssicherheit bewerten. Auch wenn eine allgemeine Zertifizierungspflicht für Hochschulen derzeit nicht besteht, kann dieser Schritt für Kooperationen u. a. mit der Wirtschaft hilfreich sein.

Von Bedeutung ist dabei auch, dass derzeit seitens des Innenministeriums das CERT BWL als zentrale, ressort- und rechenzentrumsübergreifend agierende Operationseinheit sowohl für reaktive als auch für präventive Maßnahmen für die Einrichtungen der Landesverwaltung neu konzipiert und sowohl technisch als auch organisatorisch anforderungsgerecht aufgestellt wird. Neben der Behandlung von Sicherheitsvorfällen in Form einer „Task-Force“ sollen auch weitgehend automatisierte technische Maßnahmen zur automatisierten Angriffserkennung („zentrales Monitoring“) umgesetzt werden. Damit wird das CERT BWL ein wichtiger Kooperationspartner für die Hochschulen werden.

9. ob mittlerweile eine Entscheidung getroffen wurde in der Frage, in welchem Umfang die Verwaltungsvorschrift Informationssicherheit des Innenministeriums an den Hochschulen umzusetzen ist.

Die Verwaltungsvorschrift Informationssicherheit (VwV Informationssicherheit) verpflichtet alle Dienststellen und Einrichtungen des Landes zum Aufbau eines Informationsmanagementsystems (ISMS). Die Hochschulen unterfallen dieser Verpflichtung grundsätzlich auch. Allerdings kann dort der Aufbau eines ISMS nicht für den vom Grundrecht der Wissenschaftsfreiheit geschützten Lehr- und Forschungsbereich verbindlich gemacht, sondern nur empfohlen werden.

Die mangelnde Durchsetzbarkeit der VwV im Forschungs- und Lehrbereich entlässt die Hochschulen jedoch nicht aus ihrer Verantwortung, sondern verstärkt diese eher. Insbesondere mit Blick auf den Schutzgegenstand der sensiblen Forschungsdaten, die in puncto Vertraulichkeit, Verfügbarkeit und Integrität einen hohen Standard an Informationssicherheit benötigen, wollen die Hochschulen daher der Empfehlung folgen und ein einheitliches ISMS auf Basis der VwV Informationssicherheit aufbauen, das sowohl den Personal- und Haushaltsbereich als auch den Forschungs- und Lehrbereich umfasst.

Der Aufbau eines ISMS mit funktionierenden Strukturen für Planung, Umsetzung, Überprüfung und Verbesserung der Informationssicherheit erfordert neben der Bearbeitung übergreifender Aufgaben durch die in der Antwort zu Frage 7 genannten Kompetenzteams bei jeder Hochschule auch Ressourcen vor Ort. Zur Höhe dieses Bedarfes liegen erste Hochrechnungen der Hochschulen vor. Danach müssten – unter Berücksichtigung von Synergien durch institutionenübergreifende Kooperation – für die lokale Informationssicherheit rd. 80 weitere Stellen eingesetzt werden, die an den Hochschulen jedoch derzeit nicht vorhanden sind.

In Vertretung

Steinbach

Ministerialdirektor