Deutscher Bundestag **Drucksache 19/18830**

19. Wahlperiode 22.04.2020

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Dr. Jens Brandenburg (Rhein-Neckar), Katja Suding, Mario Brandenburg (Südpfalz), weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 19/17888 –

Cyberangriffe auf deutsche Hochschulen und Wissenschaftsorganisationen

Die Zahl der Angriffe auf IT-Systeme in Deutschland nimmt zu. Im Jahr 2018 erfasste das Bundeskriminalamt insgesamt 87.000 Cyberattacken auf Privatpersonen, Unternehmen und staatliche Organisationen (vgl. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2018.pdf?__blob=publicationFile&v=3). Die Zahl nicht erfasster Angriffe auf IT-Systeme dürfte jedoch deutlich höher liegen (vgl. https://t3n.de/news/hackerattacken-deutsche-firmen-1175330/). Auch Hochschulen und außeruniversitäre Forschungseinrichtungen sind aufgrund ihres Zugangs zu vertraulichen Forschungsergebnissen einem erhöhten Risiko von Cyberangriffen ausgesetzt (vgl. https://www.deutschlandfunk.de/datenschutz-hochschulen-wollen-sich-gegen-cyberattacken.680.de.html?dram:article_id=448238). Um kritische Infrastrukturen wie Stromnetze, Verkehrswege, Krankenhäuser und Verwaltung zu schützen, fördert das Bundesministerium für Bildung und Forschung drei Kompetenzzentren zur IT-Sicherheitsforschung (https://www.bmbf.de/de/it-sicherheitsforschung-fuer-die-digitale-zukunft-6601.html). Ende 2019 musste die Universität Gießen aufgrund eines Hackerangriffs das gesamte IT-Netzwerk für mehrere Tage offline nehmen – vom WLAN in den Studentenwohnheimen über das Ausleihsystem der Bibliothek bis hin zur Lehrplattform „Stud.IP“. Die Hintergründe des Angriffs blieben unklar (vgl. https://www.faz.net/aktuell/rhein-main/region-und-hessen/uni-giessen-faehrt-nach-cyberangriff-computer-wieder-hoch-16567874.html). Universitätspräsident Prof. Dr. Joybrato Mukherjee sprach in diesem Zusammenhang von einem „digitalen Notstand“ (vgl. https://www.tagesspiegel.de/wissen/nach-cyberangriff-komplett-offline-die-uni-giessen-liegt-lahm/25352288.html).

Vorbemerkung der Bundesregierung

Die Hochschulen liegen gemäß der föderalen Kompetenzverteilung in der Zuständigkeit der Länder (Artikel 30 GG). Dies umfasst – unbeschadet der insbesondere in den Antworten zu den Fragen 14 und 15 genannten Maßnahmen der Bundesregierung – auch die Gewährleistung der IT-Sicherheit. Die meisten Landesverfassungen gestehen den Hochschulen zudem das Recht der Selbstver-

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums für Bildung und Forschung vom 17. April 2020 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

waltung im Rahmen der Gesetze zu. Vor diesem Hintergrund erfasst die Bundesregierung keine Daten über den Zustand der an Hochschulen der Länder genutzten IT-Systeme und kann insofern auch keine Aussagen über den Zustand der Sicherheit der IT-Systeme deutscher Hochschulen insgesamt treffen. Dies gilt nicht für die Hochschulen im Zuständigkeitsbereich des Bundes. Dies sind die Hochschule des Bundes für öffentliche Verwaltung (HS-Bund) sowie die Universitäten der Bundeswehr in Hamburg und München.

Der Begriff „Außeruniversitäre Forschungseinrichtungen und der übrigen durch den Bund finanzierten Wissenschaftsorganisationen“ wird im Rahmen dieser Anfrage so verstanden, dass die vom Bund finanzierten Mitglieder der Allianz der Wissenschaftsorganisationen (Helmholtz-Gemeinschaft, Leibniz-Gemeinschaft, Max-Planck-Gesellschaft, Fraunhofer-Gesellschaft, Deutsche Forschungsgemeinschaft, Wissenschaftsrat, Leopoldina, Alexander von Humboldt-Stiftung, Deutscher Akademischer Austauschdienst) umfasst sind. Diese sind fast durchweg rechtlich selbstständige Organisationen und sind somit nicht zur Meldung von Cyberangriffen an die Bundesbehörden verpflichtet.

Entsprechend erhalten die Bundesbehörden keine regelmäßigen Meldungen zu Cyberangriffen auf die vorgenannten Forschungs- und Bildungseinrichtungen und führen dazu auch keine Statistiken.

Die Einrichtungen der Wissenschaft und Forschung in Deutschland registrieren fortlaufend eine Vielzahl von Angriffsversuchen auf ihre IT-Infrastruktur, wie etwa durch Viren, Trojaner und Phishing-Mails. Diese werden in der Regel durch die laufenden Präventionsmaßnahmen der IT-Sicherheitsarchitektur zuverlässig abgewehrt. Gezielte Cyberangriffe auf eine für spezifische Branchen oder Institutionen wichtige Server-Infrastruktur von außen, die auf das Ausspähen vertraulicher Daten und/oder auf die Sabotage der Serverinfrastruktur gerichtet sind, kommen in Bezug auf die Einrichtungen der Wissenschaft wesentlich seltener vor.

Die Beantwortung der Fragen 21 und 22 kann aus Gründen des Staatswohls nicht vollständig offen erfolgen. Arbeitsmethoden und Vorgehensweisen der Nachrichtendienste des Bundes sowie Einzelheiten zur nachrichtendienstlichen Erkenntnislage sind im Hinblick auf die künftige Erfüllung des gesetzlichen Auftrags der Nachrichtendienste des Bundes besonders schutzwürdig. Eine Veröffentlichung von Einzelheiten betreffend solcher Erkenntnisse würde zu einer Schwächung der zur Verfügung stehenden Möglichkeiten zur Informationsgewinnung führen und ließe Rückschlüsse auf Aufklärungsschwerpunkte zu. Insofern könnte die Offenlegung entsprechender Informationen für die Sicherheit und die Interessen der Bundesrepublik Deutschland nachteilig sein. Deshalb sind die entsprechenden Informationen als Verschlusssache gemäß der Allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung – VSA) mit dem VS-Grad „VS-Nur für den Dienstgebrauch“ eingestuft und werden dem Deutschen Bundestag gesondert übermittelt.*

* Das Bundesministerium für Bildung und Forschung hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

1. Wie bewertet die Bundesregierung den Zustand der Sicherheit der IT-Systeme deutscher Hochschulen, außeruniversitärer Forschungseinrichtungen und der übrigen durch den Bund finanzierten Wissenschaftsorganisationen?

2. Wie bewertet die Bundesregierung das Risiko von Angriffen auf die IT-Systeme dieser Einrichtungen?

   Für wie wahrscheinlich hält die Bundesregierung Angriffe auf die IT-Systeme dieser Einrichtungen, und mit welchen Folgen solcher Angriffe rechnet die Bundesregierung?

Die Fragen 1 und 2 werden im Zusammenhang beantwortet.

Deutsche Hochschulen und Forschungseinrichtungen sind Orte international führender Forschung und Entwicklung. Sie stellen damit in vielen Fällen ein attraktives Ziel für das Ausspähen vertraulicher Daten und/oder für die Sabotage der Serverinfrastruktur dar, insbesondere, wenn an international kompetitiven Forschungsgegenständen gearbeitet wird. Der Schutz der dortigen IT-Systeme sollte sich daher auf einem hohen Niveau befinden, um negative Folgen wie den Abfluss von Forschungsergebnissen oder in Ausnahmefällen die Verfügbarkeitsbeeinträchtigung von Forschungsinfrastrukturen zu verhindern.

An außeruniversitären Forschungseinrichtungen und bundesfinanzierten Forschungsorganisationen sind die Rahmenbedingungen für die Sicherheit der IT-Systeme grundsätzlich als sehr gut zu bewerten. Die vorhandenen Strukturen wurden in den vergangenen Jahren auch wegen der wahrgenommenen Bedrohungslage stetig verbessert und ermöglichen es den Organisationen Konzepte anzuwenden, wie sie vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlen und auch in der Wirtschaft oder auch in Behörden zum Einsatz kommen.

Die Hochschulen in Zuständigkeit des Bundes haben die Empfehlungen des BSI, insbesondere zum IT-Grundschutz, beachtet, sodass die Bundesregierung für diese Einrichtungen von einem soliden Zustand der IT-Sicherheit der dortigen Systeme ausgeht. Die HS-Bund fällt zudem unter den Geltungsbereich des „Umsetzungsplans für die Gewährleistung der IT-Sicherheit in der Bundesverwaltung“ (Umsetzungsplan Bund – UP Bund). Eine 2019 durchgeführte Sachstandserhebung ergab für die HS-Bund eine Umsetzung des UP Bund auf einem hohen Niveau. Bezüglich des Zustands der IT-Sicherheit der weiteren Hochschulen wird auf die Vorbemerkung der Bundesregierung verwiesen.

Durch eine Mischung aus zentralen und dezentralen Maßnahmen sowie durch die Heterogenität der verwendeten IT-Systeme in der deutschen Wissenschaftslandschaft ist zudem sichergestellt, dass sich als Folge erfolgreicher Angriffe keine sog. Domino-Effekte ergeben.

3. Wie begründet die Bundesregierung ihre Auffassung, dass mit Blick auf potenzielle Angriffe auf die IT-Systeme von Hochschulen und Wissenschaftseinrichtungen keine „Bedrohungslage von bundesweiter Bedeutung für die deutsche Wissenschafts- und Hochschullandschaft“ vorliege (vgl. die Antwort der Bundesregierung auf die Schriftliche Frage 93 des Abgeordneten Kai Gehring auf Bundestagsdrucksache 19/16761)?

Die diesbezügliche Antwort der Bundesregierung bezog sich entsprechend der Fragestellung auf einen konkreten Cyberangriff auf eine einzelne Universität im Dezember 2019.

Angriffe auf die IT-Systeme von Hochschulen und Wissenschaftseinrichtungen müssen immer im jeweiligen Einzelfall betrachtet werden. Wann ein solcher

Angriff zu einer Bedrohungslage von bundesweiter Bedeutung für die deutsche Wissenschafts- und Hochschullandschaft werden kann, kann daher nicht pauschal beantwortet werden. Da die IT-Systeme der Hochschulen und Wissenschaftseinrichtungen zudem sehr heterogen sind, hat sich mit einem erfolgreichen Angriff auf eine Hochschule die allgemeine Bedrohungslage für Hochschulen und andere Wissenschaftseinrichtungen nicht notwendigerweise verändert.

4. Wie viele und welche Angriffe auf die IT-Systeme deutscher Hochschulen, außeruniversitärer Forschungseinrichtungen und übriger aus Mitteln des Bundes finanzierter Wissenschaftsorganisationen gab es nach Kenntnis der Bundesregierung jeweils in den Jahren von 2010 bis 2019 (bitte nach Jahren, Ländern sowie Hochschulen, Forschungseinrichtungen und übrigen Wissenschaftsorganisationen aufteilen)?

5. Bei wie vielen und welchen dieser Angriffe wurden nach Kenntnis der Bundesregierung Daten der Hochschulen bzw. Forschungseinrichtungen durch die Angreifer entwendet (bitte nach Jahren – 2010 bis 2019 –, Ländern sowie Hochschulen, Forschungseinrichtungen und übrigen Wissenschaftsorganisationen aufteilen)?

6. In welchem Umfang wurden bei diesen Angriffen nach Kenntnis der Bundesregierung Daten welches Vertraulichkeitsniveaus jeweils entwendet (bitte nach Jahren – 2010 bis 2019 –, Ländern, und verschiedenen Vertraulichkeitsniveaus – öffentlich, vertraulich, streng vertraulich – aufteilen und in Gigabyte ausweisen)?

7. In welchem Umfang wurden bei diesen Angriffen nach Kenntnis der Bundesregierung vertrauliche Daten entwendet, insbesondere

   a) persönliche Daten, wie Namen und Adressen von Hochschulangehörigen;

   b) Noten und Ergebnisse von Prüfungsleistungen von Studierenden und Doktoranden;

   c) Prüfungsleistungen von Studierenden;

   d) bisher unveröffentlichte und vertrauliche Forschungsdaten bzw. Forschungsergebnisse (bitte jeweils nach Jahren – 2010 bis 2019 – und Ländern aufteilen)?

Die Fragen 4 bis 7 werden im Zusammenhang beantwortet.

Die Bundesregierung hat zur Beantwortung Angaben der außeruniversitären Forschungseinrichtungen und der übrigen vom Bund finanzierten Wissenschaftsorganisationen zur Anzahl der gezielten Cyberangriffe erbeten, die in der nachfolgenden Tabelle dargestellt sind. Dabei ist zu beachten, dass die Abgrenzung gezielter Angriffe nicht immer trennscharf vorzunehmen ist, sodass die Zählweise zwischen den einzelnen Einrichtungen Abweichungen unterliegt (siehe hierzu auch die Vorbemerkung der Bundesregierung). Ebenfalls ist zu beachten, dass die Erfassung von Cyberangriffen je nach Einrichtung unterschiedlich weit zurückreicht, sodass sich auch deshalb mit zunehmender zeitlicher Nähe höhere Fallzahlen ergeben. Eine Aufschlüsselung der Cyberangriffe nach Ländern ist nicht möglich.

Angriffe nach Jahren:

Jahr	Anzahl Angriffe
2010	2
2011	2
2012	3
2013	5
2014	12
2015	12
2016	26
2017	25
2018	24
2019	63

Angriffe nach Einrichtungen:

Einrichtungen	Anzahl Angriffe
Außeruniversitäre Forschungseinrichtungen	172
Weitere Wissenschaftseinrichtungen	2

Nach sorgfältiger Abwägung ist die Bundesregierung zu der Auffassung gelangt, dass über diese Zahlen hinaus keine konkretere Beantwortung der Frage erfolgen kann. Die erbetenen Auskünfte sind geheimhaltungsbedürftig, weil sie Informationen enthalten, die im Zusammenhang mit der Arbeitsweise und Methodik des Bundesamtes für Verfassungsschutz (BfV) stehen. Im Detail betrifft die Frage den Kenntnisstand der Cyberabwehr des BfV. Grundsätzlich gilt, dass die Cyberabwehr tatsächlichen Anhaltspunkten für verdeckte nachrichtendienstliche Aktivitäten ausländischer Staaten in der Bundesrepublik Deutschland im Rahmen ihrer gesetzlichen Zuständigkeit der Cyberabwehr des BfV (§ 3 Absatz 1 Nummer 2 des Bundesverfassungsschutzgesetzes) nachgeht. Die Erkenntnisse, die dabei gewonnen werden, unterliegen der Vertraulichkeit und sind besonders schutzbedürftig. Eine (zur Veröffentlichung bestimmte) Antwort der Bundesregierung auf diese Fragen würde spezifische Informationen zur Tätigkeit der Sicherheitsbehörden einem nicht eingrenzbaren Personenkreis nicht nur im Inland, sondern auch im Ausland zugänglich machen. Dabei würde die Gefahr entstehen, dass die Methodik und der Kenntnisstand der Cyberabwehr des BfV aufgedeckt und damit auch der zukünftige Erkenntnisgewinn und Einsatzerfolg gefährdet würde. Dies könnte einen Nachteil für die wirksame Aufgabenerfüllung der Sicherheitsbehörden und damit für die Interessen der Bundesrepublik Deutschland bedeuten. Die Fragestellung berührt derart schutzbedürftige Geheimhaltungsinteressen, dass auch ein geringfügiges Risiko des Bekanntwerdens, wie es auch bei einer Übermittlung an die Geheimschutzstelle des Deutschen Bundestages nicht ausgeschlossen werden kann, aus Staatswohlgründen vermieden werden muss. In diesem Fall überwiegt daher das Staatswohlinteresse gegenüber dem parlamentarischen Informationsrecht.

8. Wie hoch schätzt die Bundesregierung den durch Cyberangriffe entstandenen Schaden bei Hochschulen sowie insbesondere bei außeruniversitären Forschungseinrichtungen und übrigen aus Mitteln des Bundes finanzierten Wissenschaftsorganisationen (bitte nach Jahren – 2010 bis 2019 –,Ländern sowie Hochschulen, Forschungseinrichtungen und übrigen Wissenschaftsorganisationen aufteilen)?

   Wie kommt die Bundesregierung zu dieser Schätzung?

Wie in der Vorbemerkung der Bundesregierung ausgeführt, führt der Bund keine Statistiken über Cyberangriffe auf die in der Frage genannten Forschungs- und Bildungseinrichtungen. Eine geeignete Datengrundlage für eine Schätzung liegt mithin nicht vor.

9. In wie vielen und welchen Fällen waren potenzielle Angriffe auf die IT-Systeme deutscher Hochschulen, außeruniversitärer Forschungseinrichtungen und übriger aus Mitteln des Bundes finanzierten Wissenschaftsorganisationen nach Kenntnis der Bundesregierung zuvor dem Bundesnachrichtendienst, dem Bundesamt für Verfassungsschutz, dem Bundesamt für Sicherheit in der Informationstechnik (BSI) oder nachgelagerten Behörde des Bundesregierung bekannt?

   Wie viele potenzielle Angriffe konnten aufgrund von Aktivitäten dieser Behörden bereits vor Realisierung abgewehrt werden (bitte nach Jahren – 2010 bis 2019 – und Ländern aufteilen)?

Es wird auf die Antwort zu den Fragen 4 bis 7 verwiesen.

10. In wie vielen und welchen Fällen erfolgreicher bzw. abgewehrter Angriffe auf die IT-Systeme deutscher Hochschulen, außeruniversitärer Forschungseinrichtungen und übriger aus Mitteln des Bundes finanzierten Wissenschaftsorganisationen nahmen nach Kenntnis der Bundesregierung die Ermittlungsbehörden (insb. der Generalbundesanwalt und das Bundeskriminalamt) Ermittlungen auf (bitte nach Jahren – 2010 bis 2019 – und Ländern aufteilen)?

    In wie vielen und welchen Fällen konnten die Angreifenden identifiziert werden?

Der Generalbundesanwalt beim Bundesgerichtshof hat mit Bezug auf Angriffe der in der Fragestellung bezeichneten Art von 2010 bis 2019 insgesamt fünf strafrechtliche Ermittlungsverfahren wegen des in seine originäre Verfolgungszuständigkeit (§ 142a Absatz 1 Satz 1, § 120 Absatz 1 Nummer 3 des Gerichtsverfassungsgesetzes) fallenden Delikts der geheimdienstlichen Agententätigkeit gemäß § 99 des Strafgesetzbuchs eingeleitet.

Weitere Auskünfte zu Jahren, Verfahrensgegenstand und identifizierten Personen können nicht erteilt werden, da diese Informationen Rückschlüsse auf zum Teil noch verdeckt geführte Ermittlungsverfahren zuließen und damit Ermittlungen beeinträchtigen könnten. Das verfassungsrechtlich verbürgte Frage- und Informationsrecht des Deutschen Bundestages gegenüber der Bundesregierung wird insoweit durch das gleichfalls Verfassungsrang genießende schutzwürdige Interesse der Gewährleistung einer funktionsgerechten und organadäquaten Aufgabenwahrnehmung begrenzt. Das Frage- und Informationsrecht des Parlaments muss in diesem konkreten Fall nach Abwägung der widerstreitenden Interessen zurückstehen. Im Übrigen wird auf die Vorbemerkung der Bundesregierung verwiesen.

11. In wie vielen und welchen Fällen unterstützte das Bundesamt für Sicherheit in der Informationstechnik nach Kenntnis der Bundesregierung gemäß § 5a Absatz 7 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) von Angriffen auf die IT-Systeme betroffene Hochschulen bzw. Wissenschaftseinrichtungen bei der Wiederherstellung ihrer IT-Systeme (bitte nach Jahren – 2010 bis 2019 –, Ländern sowie Hochschulen, Forschungseinrichtungen und übrigen Wissenschaftsorganisationen aufteilen)?

Das BSI hat keine Hochschulen und Wissenschaftseinrichtungen im angefragten Zeitraum bei der Wiederherstellung der IT-Systeme im Rahmen von § 5a Absatz 7 des BSI-Gesetzes unterstützt.

12. In wie vielen Fällen handelte es sich, sofern die Identität der Angreifenden geklärt werden konnte, dabei nach Kenntnis der Bundesregierung um

    a) inländische Unternehmen;

    b) inländische Privatpersonen;

    c) inländische Gruppen privater Personen;

    d) ausländische staatliche Organisationen (insbesondere Geheimdienste);

    e) ausländische Unternehmen;

    f) ausländische Privatpersonen;

    g) ausländische Gruppen privater Personen (bitte jeweils nach Jahren – 2010 bis 2019 – und Ländern aufteilen)?

Es wird auf die Antworten zu den Fragen 4 bis 7 und 10 verwiesen.

13. Welche Erkenntnisse hat die Bundesregierung jeweils über die Absichten der Angriffe auf die IT-Systeme deutscher Hochschuleinrichtungen, Forschungseinrichtungen und Wissenschaftseinrichtungen?

Es wird auf die Antworten zu den Fragen 4 bis 7, 8 und 10 verwiesen.

14. Inwiefern betrachtet es die Bundesregierung als ihre (Teil-)Zuständigkeit, die Angriffe auf die IT-Systeme deutscher Hochschuleinrichtungen, Forschungseinrichtungen und Wissenschaftseinrichtungen zu erkennen, zu verhindern und so die IT-Sicherheit zu gewährleisten bzw. die Einrichtungen dabei zu unterstützen?

Die Einrichtungen der Wissenschaft sind rechtlich selbständige Organisationen, die auch für ihre eigene IT-Sicherheit verantwortlich sind. Mit der Grundfinanzierung der Einrichtungen garantieren Bund und Länder hierfür gute Rahmenbedingungen. Durch das Bundesamt für Sicherheit in der Informationstechnik werden darüber hinaus Empfehlungen zur IT-Sicherheit ausgesprochen, die für die Bundeshochschulen verbindlich gelten und für die Wissenschaftseinrichtungen als Orientierung dienen.

15. Wie, und über welche nachgelagerten Behörden unterstützt die Bundesregierung

    a) die Länder und die Hochschulen,

    b) die außeruniversitären Forschungseinrichtungen,

    c) übrige aus Mitteln des Bundes finanzierte Wissenschaftsorganisationen bei der Sicherung ihrer IT-Systeme und sensibler Daten vor Angriffen durch Hacker?

Für Fragen zur IT-Sicherheit in der Informationsgesellschaft wurde am 1. Januar 1991 das BSI gegründet. Dieses Bundesamt nimmt u. a. die Aufgabe der Abwehr von Gefahren für die Sicherheit in der Informationstechnik des Bundes wahr. Zu den Aufgaben des BSI gehört auch die Beratung der zuständigen Stellen des Bundes sowie, auf Ersuchen der zuständigen Stellen der Länder, auch deren Unterstützung. Im Übrigen leisten sich alle Behörden des Bundes und der Länder gegenseitig Rechts- und Amtshilfe (Artikel 35 Absatz 1 GG).

16. In welchem Umfang stellt die Bundesregierung Personal für diese Unterstützungsleistungen zur Verfügung?

Das BSI hält Personal für gesetzlich zugewiesene Unterstützungsaufgaben bereit. Für Einrichtungen der Länder erfolgt eine unmittelbare personelle Unterstützung allenfalls im Rahmen der Amtshilfe. Der personelle Umfang ergibt sich aus der durch den Einzelfall erforderlichen Priorisierung.

17. Hat die Bundesregierung gemeinsam mit allen außeruniversitären Forschungseinrichtungen und allen übrigen aus Mitteln des Bundes finanzierten Wissenschaftsorganisationen Notfallpläne ausgestaltet, um Angriffe auf die IT-Systeme der genannten Einrichtungen frühzeitig zu erkennen und Schäden zu minimieren?

    Wenn ja, wann wurden diese Pläne erarbeitet und abgeschlossen?

    Welche Maßnahmen sind in diesen Plänen vorgesehen?

    Wenn nein, für wie viele Organisationen fehlen solche Pläne bisher, und aus welchen Gründen?

Die Forschungseinrichtungen und Wissenschaftsorganisationen sind selbständige Organisationen, deren IT-Sicherheitskonzepte eigenverantwortlich erstellt und umgesetzt werden. Im Übrigen wird auf die Antworten zu den Fragen 1 und 2, 14, 16 und 18 verwiesen.

18. In welchem Umfang stand die Bundesregierung den Hochschulen und Ländern bei der Entwicklung solcher Pläne beratend zur Verfügung?

Zu Fragen der IT-Sicherheit arbeitet das BSI mit den Ländern in verschiedenen Bund-Länder-Arbeitsgremien zusammen. So wurde durch die AG InfoSic eine Leitlinie mit Umsetzungsplanung erarbeitet, welche kürzlich durch den IT-Planungsrat beschlossen wurde. Das BSI hat bei der Erstellung der Umsetzungsmaßnahmen für das Handlungsfeld zum IT-Notfallmanagement mitgewirkt. Im Übrigen wird auf die Vorbemerkung der Bundesregierung verwiesen.

19. In welcher Form unterstützte die Bundesregierung, beispielsweise über das Bundesamt für Sicherheit in der Informationstechnik, die Universität Gießen beim Erkennen, Reagieren und Entfernen der Schadsoftware auf den Hochschulservern?

Das BSI hat das zuständige Landes-CERT Hessen bei der Unterstützung der Universität Gießen zum Erkennen, Reagieren und Entfernen der Schadsoftware auf den Systemen der Hochschule beraten.

20. Welche Konsequenzen hat die Bundesregierung aus den Angriffen auf die IT-Systeme der Universität Gießen im Dezember 2019 gezogen, und welche Maßnahmen hat sie seitdem ergriffen?

Die Bundesregierung zielt darauf ab, u. a. durch Empfehlungen des BSI (z. B. zum IT-Grundschutz) und durch Rechtsetzung in ihrer Zuständigkeit, wie dem IT-Sicherheitsgesetz, insgesamt ein hohes Niveau von Cybersicherheit in Deutschland zu schaffen. Das BSI verfolgt die Veröffentlichungen auf dem Gebiet der IT-Sicherheit und Meldungen zu IT-Sicherheitsvorfällen und passt die eigenen Maßnahmen und Empfehlungen erforderlichenfalls an. Das BSI informiert nicht nur Stellen des Bundes, sondern auch Bürger und Unternehmen über die Gefahren und Auswirkungen von Schadprogrammen. Darüber hinaus hat das BSI ein Dokument für IT-Sicherheitsbeauftragte und Systemadministratoren von KMU und kleineren Behörden veröffentlicht mit Hinweisen zur Ersten Hilfe bei einem schweren IT-Sicherheitsvorfall.

21. Ist der Bundesregierung der Fall des Verdachts auf (Forschungs-)Spionage durch den ehemaligen chinesischen Leiter des Konfuzius-Instituts Brüssel bekannt (vgl. https://www.zeit.de/news/2019-10/30/leiter-von-chinesischem-kulturinstitut-aus-schengen-raum-verbannt)?

Wenn ja, wie bewertet die Bundesregierung diesen Fall mit Blick auf die Aktivitäten der chinesischen Konfuzius-Institute an deutschen Hochschulen?

Welche Konsequenzen zieht sie aus dieser Einschätzung?

Der genannte Fall ist der Bundesregierung bekannt, ebenso die zwischenzeitlich von der mit dem betroffenen Konfuzius-Institut kooperierenden Freien Universität Brüssel getroffene Entscheidung, die Zusammenarbeit nach Ablauf der Vertragslaufzeit im Juni 2020 nicht zu verlängern. Die Bundesregierung nimmt den Vorgang sehr ernst. Ergänzend wird auf die Vorbemerkung der Bundesregierung zur gesonderten Übermittlung von Informationen mit dem VS-Grad „VS-Nur für den Dienstgebrauch“ verwiesen.*

22. Wie bewertet die Bundesregierung das Risiko potenzieller Forschungsspionage über die Zugänge zu den IT-Systemen deutscher Hochschulen durch chinesische Konfuzius-Institute?

Liegen der Bundesregierung Erkenntnisse vor, ob das von der chinesischen Regierung ins Ausland entsandte Lehrpersonal der Konfuzius-Institute neben einer „stärkeren ideologischen Vorbereitung“ (vgl. Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der FDP auf Bundestagsdrucksache 19/15560) auch Vorbildung auf dem Gebiet der Informationstechnologie aufweist und/oder über berufliche Erfahrun-

* Das Bundesministerium für Bildung und Forschung hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

gen bzw. Ausbildung auf dem Gebiet geheimdienstlicher bzw. militärischer Aktivitäten besitzt?

Mit welchen Ländern und Hochschulen hat die Bundesregierung diese Risiken und mögliche vorbeugende Maßnahmen erörtert?

Der Bundesregierung liegen hierzu keine eigenen Erkenntnisse vor. Sie steht weiter in engem Kontakt und Austausch mit der Allianz der deutschen Wissenschaftsorganisationen. In diesem Rahmen werden auch Themen der Kooperation und die Vermeidung unerwünschter Einflussnahmen ausländischer Institutionen auf Wissenschaftsorganisationen erörtert. Anlassbezogen tritt die Bundesregierung mit den Ländern, betroffenen Hochschulen und Forschungsorganisationen beratend in Kontakt.

Ergänzend wird auf die Vorbemerkung der Bundesregierung zur gesonderten Übermittlung von Informationen mit dem VS-Grad „VS-Nur für den Dienstgebrauch“ verwiesen.*

* Das Bundesministerium für Bildung und Forschung hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333