Deutscher Bundestag **Drucksache 20/12259**

20. Wahlperiode 10.07.2024

Antwort

der Bundesregierung

auf die Kleine Anfrage der Fraktion der CDU/CSU
– Drucksache 20/11830 –

Cyberangriffe auf Wissenschaft und Forschung in Deutschland

Vorbemerkung der Fragesteller

Deutschland sieht sich mit einer wachsenden Bedrohung durch Cyberangriffe konfrontiert, die u. a. Privatpersonen, Unternehmen, Wissenschaftseinrichtungen und politische Parteien betreffen. Laut Bundeskriminalamt (BKA) stiegen die aus dem Ausland begangenen Cyberstraftaten 2023 um 28 Prozent an, was zu einem Schaden von knapp 148 Mrd. Euro führte (www.bka.de/DE/Aktuelle Informationen/StatistikenLagebilder/Lagebilder/Cybercrime/2023/CC_2023.html).

Hochschulen und außeruniversitäre Forschungseinrichtungen sind in den vergangenen Jahren vermehrt in das Fadenkreuz von Kriminellen geraten und Ziel bzw. Opfer von Cyberangriffen geworden. Cyberangriffe wie auf die Berliner Hochschule für Technik (www.tagesspiegel.de/wissen/sicherheitsvorfall-berliner-hochschule-fur-technik-von-cyberangriff-betroffen-11243161.html), die Hessische Hochschule für öffentliches Management und Sicherheit (www.faz.net/aktuell/rhein-main/cyberangriff-sensible-daten-von-hessischer-polizeihochschule-gestohlen-19724405.html) und die Hochschule Hannover (www.spiegel.de/netzwelt/web/ransomware-hackerangriff-beeintraechtigt-teile-der-hochschule-hannover-a-e6247f8b-7adb-4bdd-986c-7a85068b38a3) sind nur eine unvollständige kleine Auswahl von Fällen, die jüngst bundeweit Schlagzeilen gemacht haben.

Auch außeruniversitäre Forschungseinrichtungen stehen in diesem Hinblick vor enormen Herausforderungen. Die Präsidentin der Leibniz Gemeinschaft, Dr. Martina Brockmeier, hob im Mai 2024 für ihre Forschungseinrichtung hervor:

„Ich habe, was unsere Finanzierung als Forschungsgemeinschaft angeht, große Sorgen, wobei noch zwei Kostenfaktoren hinzukommen, die Sie nicht genannt haben. Einerseits der Präventivschutz vor und die Kosten von akuten Cyberattacken, von denen wir zuletzt mehrere hatten, andererseits die notwendigen Investitionen in Klimaneutralität und Nachhaltigkeit. Das sind Aufgaben, für die wir keinerlei Rücklagen haben“ (www.jmwiarda.de/https-www.jmwiarda.de-2024-05-13-wir-spueren-doch-alle-das-spannungsfeld/).

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern und für Heimat vom 10. Juli 2024 übermittelt.

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

Vorbemerkung der Bundesregierung

Die Bundesregierung hat ihren Antworten folgende Definition zugrunde gelegt:

„Ein Cyberangriff ist eine Einwirkung auf ein oder mehrere andere informationstechnische Systeme im oder durch den Cyberraum, die zum Ziel hat, deren IT-Sicherheit durch informationstechnische Mittel ganz oder teilweise zu beeinträchtigen."

Cybersicherheitsstrategie für Deutschland 2021, vgl. S. 133 (Glossar)

Allgemeine Ausführungen zu der föderalen Kompetenzverteilung bzgl. Hochschulen, zum Recht der Selbstverwaltung von Hochschulen sowie zu außeruniversitären Forschungseinrichtungen:

Die Hochschulen liegen gemäß der föderalen Kompetenzverteilung in der Zuständigkeit der Länder. Dies umfasst auch die Sicherheit der IT-Infrastrukturen. Die meisten Landesverfassungen gestehen den Hochschulen zudem das Recht der Selbstverwaltung im Rahmen der Gesetze zu. Die Hochschulen sind nicht zur Meldung von Cyberangriffen an Bundesbehörden verpflichtet. Vor diesem Hintergrund erfasst die Bundesregierung nicht systematisch Daten über Cyberangriffe auf IT-Systeme an Hochschulen und kann daher zu den Fragen zu den Hochschulen in Länderzuständigkeit keine umfassenden Auskünfte geben.

Der Begriff der „Wissenschaftseinrichtungen" wird im Rahmen dieser Anfrage so verstanden, dass damit die Helmholtz-Gemeinschaft (HGF), Leibniz-Gemeinschaft (WGL), Max-Planck-Gesellschaft (MPG), Fraunhofer-Gesellschaft (FHG) sowie die Deutsche Forschungsgemeinschaft (DFG) gemeint sind. Diese Einrichtungen sind rechtlich selbständig. Sie unterliegen nicht der Fachaufsicht des Bundesministeriums für Bildung und Forschung (BMBF) und sind grundsätzlich eigenständig für ihre IT-Sicherheit verantwortlich. Eine Verpflichtung zur Meldung von Cyberangriffen an Bundesbehörden besteht nicht.

Allgemeine Ausführungen zu den Rechtsgrundlagen der Universitäten der Bundeswehr:

Die beiden Universitäten der Bundeswehr Hamburg und München wurden auf der Grundlage von Verwaltungsabkommen zwischen der Bundesregierung und den Sitzländern errichtet. Sie sind nichtrechtsfähige Körperschaften des öffentlichen Rechts. Hinsichtlich der akademischen Angelegenheiten unterstehen sie der Rechtsaufsicht ihrer Sitzländer und der des Bundesministeriums der Verteidigung. In den übrigen Angelegenheiten sind sie Dienststellen der Bundeswehrverwaltung.

Allgemeine Ausführungen zur Erfassung und Aufbereitung der Daten:

Die Bundesregierung hat zur Beantwortung der Fragen Angaben oben aufgeführten Wissenschaftseinrichtungen entsprechend der o. g. Definition von Cyberangriffen erbeten.

Bei den Angaben der Wissenschaftseinrichtungen ist zu berücksichtigen, dass die Erfassung in den unterschiedlichen Einrichtungen nicht einheitlich stattfindet und daher die Zählung zwischen den einzelnen Einrichtungen abweichen kann (siehe dazu auch die jeweiligen Anmerkungen der einzelnen Wissenschaftsorganisationen).

Die großen Differenzen in den ausgewiesenen Zahlen beruhen insbesondere darauf, dass die Wissenschaftseinrichtungen die o. g. Definition des Begriffs „Cyberangriff" unterschiedlich ausgelegt haben. So bezieht sich die Antwort der Leibniz-Gemeinschaft auf Cyberangriffe mit Schäden, die der Deutschen Forschungsgemeinschaft auf erfolgreiche Cyberangriffe. Demgegenüber hat die Helmholtz-Gemeinschaft alle Vorfälle aufgeführt, in deren Folge es theoretisch

zu einem Schadensereignis kommen konnte (daher die sehr hohen Fallzahlen in den Antworten zu den Fragen 1, 7 und 22).

1. Wie viele Cyberangriffe auf Wissenschaftseinrichtungen wurden in den Jahren 2022, 2023 und 2024 festgestellt?

Dem Bundeskriminalamt sind in den Jahren 2022 bis 2024 mit Stand 19. Juni 2024 42 Cyberangriffe auf Hochschulen und Wissenschaftseinrichtungen bekannt geworden.

Entsprechend der Abfrage wurden durch die Wissenschaftseinrichtungen folgende Daten gemeldet:

Fraunhofer-Gesellschaft

Die Definition wird so verstanden, dass speziell Ransomwareangriffe, Hacking, Cyberspionage usw. gemeint sind, bei denen Netzwerke unterminiert, Server übernommen, Daten verschlüsselt oder abgezogen wurden.

Jahr	Anzahl der Cyberangriffe
2022	3
2023	0
2024	0

Max-Planck-Gesellschaft

Jahr	Anzahl der Cyberangriffe
2022	6
2023	2
2024	0

Helmholtz-Gemeinschaft

Die Helmholtz-Gemeinschaft versteht die Definition so, dass alle Angriffe gemeint sind, in deren Folge es zu einem Schadensereignis kommen kann. Dies schließt etwa Phishing-Emails und verbotene Login-Versuche in Helmholtz-Accounts ein.

Jahr	Anzahl der Cyberangriffe
2022	1 265
2023	1 290
2024	1 168

Leibniz-Gemeinschaft

Der Leibniz-Gemeinschaft liegen keine Übersichten darüber vor, wie viele Cyberangriffe pro Jahr auf ihre Einrichtungen verübt wurden. In den Jahren 2022 bis 2024 sind fünf Angriffe auf Leibniz-Einrichtungen bekannt geworden, die Schäden angerichtet haben.

Jahr	Anzahl der Cyberangriffe mit Schäden
2022	2
2023	3
2024	0

Deutsche Forschungsgemeinschaft

Jahr	Anzahl der erfolgreichen Cyberangriffe
2022	0
2023	1
2024	0

2. Wie hoch beziffert die Bundesregierung den seit 2022 jährlich entstandenen Schaden durch Cyberangriffe auf Wissenschaftseinrichtungen in Deutschland?

21. Wie hoch wird nach Kenntnis der Bundesregierung der seit 2022 jährlich entstandene Schaden durch Cyberangriffe auf Einrichtungen der FhG, MPG, HGF und WGL beziffert (bitte einzeln entlang der Jahre 2022, 2023 und 2024 aufführen)?

Die Fragen 2 und 21 werden gemeinsam beantwortet.

Der Bundesregierung liegen nach entsprechender Abfrage folgende Daten der Wissenschaftseinrichtungen vor.

Fraunhofer-Gesellschaft

Jahr	Höhe des Schadens in Euro
2022	ca. 15 Mio. gesamt (beinhaltet: Analyse, Bereinigung, Wiederherstellung usw. und abgeschätzte Folgeschäden)
2023	0
2024	0

Max-Planck-Gesellschaft

Jahr	Höhe des Schadens in Euro
2022	500 000
2023	700 000
2024	0

Anmerkung: Der Schaden für die Wissenschaft lässt sich schwer beziffern, deshalb wurden hier nur die externen Wiederherstellungskosten aufgeführt.

Helmholtz-Gemeinschaft

Jahr	Höhe des Schadens in Euro
2022	170 500
2023	12 336 280
2024	74 000

Deutsche Forschungsgemeinschaft

Jahr	Höhe des Schadens in Euro
2022	0
2023	0
2024	0

Der Bundesregierung liegen keine entsprechenden Zahlen zur Leibniz-Gemeinschaft vor.

3. Wie verhält sich nach Kenntnis der Bundesregierung seit 2022 die Anzahl von Cyberangriffen auf Wissenschaftseinrichtungen in Deutschland zu Cyberangriffen auf Wissenschaftseinrichtungen in Frankreich, den Niederlanden, Großbritannien, Polen, Tschechien, Italien und Spanien?

Der Bundesregierung liegen keine belastbaren Daten zu Cyberangriffen auf Wissenschaftseinrichtungen in Frankreich, den Niederlanden, Großbritannien, Polen, Tschechien, Italien und Spanien vor. Daher kann die Bundesregierung keinen Bezug zur Anzahl der Cyberangriffe auf Wissenschaftseinrichtungen in Deutschland herstellen.

4. Wie hoch ist nach Kenntnis der Bundesregierung der in den Mitgliedstaaten der Europäischen Union seit 2022 entstandene jährliche Schaden durch Cyberangriffe auf Wissenschaftseinrichtungen?

Der Bundesregierung liegen keine Daten aus den Mitgliedstaaten der Europäischen Union über den entstandenen Schaden durch Cyberangriffe auf Wissenschaftseinrichtungen vor.

5. In wie vielen Fällen wurden in Jahren 2022, 2023 und 2024 von Einrichtungen aus Wissenschaft und Forschung in Deutschland in Reaktion auf Cyberangriffe Lösegelder gezahlt (bitte entlang der Kategorien „Hochschule“ und „außeruniversitäre Forschungseinrichtungen“ aufschlüsseln), und in welcher durchschnittlichen Höhe wurden Lösegelder gezahlt?

Der Bundesregierung liegen keine Informationen im Sinne der Fragestellung vor.

6. In wie vielen Fällen wurden in den Jahren 2022, 2023 und 2024 die Ermittlungsbehörden des Bundes sowie nach Kenntnis der Bundesregierung jene der Länder bei der Bekämpfung von Cyberattacken involviert, und in wie vielen Fällen wurden dabei in welcher durchschnittlichen Höhe Lösegelder gezahlt?

In allen unter Frage 1 (Kenntnisse der Bundesregierung) aufgeführten Fällen waren bzw. sind Ermittlungsbehörden der Länder oder des Bundes involviert. Hinsichtlich der Teilfrage 2 zu Lösegeldzahlungen wird auf die Antwort zu Frage 5 verwiesen.

Die angefragten Wissenschaftseinrichtungen haben Folgendes gemeldet.

Fraunhofer-Gesellschaft

Jahr	Anzahl der Einbeziehung von Ermittlungsbehörden	Anzahl der Lösegeldzahlungen	Durchschnittliche Höhe der Lösegeldzahlungen
2022	2	0	0
2023	0	0	0
2024	0	0	0

Max-Planck-Gesellschaft

Jahr	Anzahl der Einbeziehung von Ermittlungsbehörden	Anzahl der Lösegeldzahlungen	Durchschnittliche Höhe der Lösegeldzahlungen
2022	5	0	0
2023	2	0	0
2024	0	0	0

Helmholtz-Gemeinschaft

Jahr	Anzahl der Einbeziehung von Ermittlungsbehörden	Anzahl der Lösegeldzahlungen	Durchschnittliche Höhe der Lösegeldzahlungen
2022	0	0	0
2023	4	0	0
2024	1	0	0

Leibniz-Gemeinschaft

Jahr	Anzahl der Einbeziehung von Ermittlungsbehörden	Anzahl der Lösegeldzahlungen	Durchschnittliche Höhe der Lösegeldzahlungen
2022	2	0	–
2023	3	0	–
2024	–	–	–

Der Bundesregierung sind keine derartigen Fälle bei der Deutschen Forschungsgemeinschaft bekannt.

7. In wie vielen Fällen wurden in den Jahren 2022, 2023 und 2024 die Ermittlungsbehörden des Bundes sowie nach Kenntnis der Bundesregierung jene der Länder der Bekämpfung von Cyberattacken nicht involviert, und in wie vielen Fällen wurden dabei in welcher durchschnittlichen Höhe Lösegelder gezahlt?

Es wird auf die Antwort zu Frage 6 verwiesen.

Die angefragten Wirtschaftseinrichtungen haben folgendes gemeldet.

Fraunhofer-Gesellschaft

Jahr	Anzahl der Nichteinbeziehung von Ermittlungsbehörden	Anzahl der Lösegeldzahlungen	Durchschnittliche Höhe der Lösegeldzahlungen
2022	1	0	0
2023	0	0	0
2024	0	0	0

Max-Planck-Gesellschaft

Jahr	Anzahl der Nichteinbeziehung von Ermittlungsbehörden	Anzahl der Lösegeldzahlungen	Durchschnittliche Höhe der Lösegeldzahlungen
2022	1	0	0
2023	0	0	0
2024	0	0	0

Helmholtz-Gemeinschaft

Jahr	Anzahl der Nichteinbeziehung von Ermittlungsbehörden	Anzahl der Lösegeldzahlungen	Durchschnittliche Höhe der Lösegeldzahlungen
2022	1 265	0	0
2023	1 286	0	0
2024	1 167	0	0

Der Bundesregierung sind bzgl. der Leibniz-Gemeinschaft und der Deutschen Forschungsgemeinschaft keine entsprechenden Fälle bekannt.

8. Wie hoch ist die Aufklärungsquote der Ermittlungsbehörden des Bundes sowie nach Kenntnis der Bundesregierung jene der Länder bei etwaigen Cyberangriffen auf Einrichtungen aus Wissenschaft und Forschung in den Jahren 2022, 2023 und 2024?

Der Bundesregierung liegen dazu keine Daten vor.

9. In wie vielen Fällen von Cyberangriffen auf staatliche und nichtstaatliche Einrichtungen wurde das Kommando Cyber- und Informationsraum (KdoCIR) der Bundeswehr um Amtshilfe gebeten?

Das Kommando Cyber- und Informationsraum wurde im Jahre 2023 in zwei Fällen um Amtshilfe ersucht.

10. In wie vielen Fällen hat das KdoCIR dem Amtshilfeersuchen entsprochen?

Das KdoCIR hat in keinem Fall dem Amtshilfeersuchen entsprochen.

11. In wie vielen Fällen konnte bzw. konnten nach Kenntnis der Bundesregierung der oder die Täter der Cyberangriffe ermittelt werden, und was weiß die Bundesregierung über diese Täter?

25. In wie vielen Fällen konnten nach Kenntnis der Bundesregierung Täter der Cyberangriffe ermittelt werden, und welche Kenntnisse hat die Bundesregierung über die Täter?

26. Welche sind nach Kenntnis der Bundesregierung die fünf Hauptursprungsländer von Cyberangriffen auf Einrichtungen der FHG, MPG, HGF und WGL in den Jahren 2022, 2023 und 2024?

Die Fragen 11, 25 und 26 werden gemeinsam beantwortet.

In einem Großteil der der Bundesregierung bekannten Fälle konnten die eingesetzten Schadsoftware-Varianten festgestellt sowie weitergehende Ermittlungsansätze generiert werden. Aufgrund noch laufender Ermittlungsverfahren können keine weitergehenden Ausführungen zu den Tätern gemacht werden. Trotz der grundsätzlichen verfassungsrechtlichen Pflicht der Bundesregierung, Informationsansprüche des Deutschen Bundestages zu erfüllen, tritt hier nach konkreter Abwägung der betroffenen Belange das Informationsinteresse des Parlaments hinter den berechtigten Geheimhaltungsinteressen zurück. Das Interesse der Allgemeinheit an der Gewährleistung einer funktionstüchtigen Strafrechtspflege leitet sich aus dem Rechtsstaatsprinzip ab und hat damit ebenfalls Verfassungsrang. Die gewünschte Auskunft würde weitergehende Ermittlungsmaßnahmen erschweren oder gar vereiteln, weshalb aus dem Prinzip der Rechtsstaatlichkeit folgt, dass vorliegend das betroffene Interesse der Allgemeinheit an der Gewährleistung einer funktionstüchtigen Strafrechtspflege und Strafverfolgung Vorrang vor dem Informationsinteresse hat.

12. Welche sind die fünf Hauptursprungsländer von Cyberangriffen auf deutsche Hochschulen in den Jahren 2022, 2023 und 2024?

Aufgrund noch laufender Ermittlungsverfahren können keine weitergehenden Ausführungen zu den Tätern gemacht werden. Zur Begründung wird auf die Antwort zu Frage 11 verwiesen.

Der Verfassungsschutzbericht 2023 nennt als Hauptakteure gegen Deutschland gerichteter Spionage einschließlich nachrichtendienstlich gesteuerter Cyberangriffe insbesondere die Russische Föderation, die Volksrepublik China und die Islamische Republik Iran.

13. Wie viele Hochschulen waren wie oft nach Kenntnis der Bundesregierung seit 2022 von Cyberangriffen betroffen (bitte entlang der Jahre 2022, 2023 und 2024 sowie nach Bundesländern auflisten)?

Nach Kenntnis der Bundesregierung waren 36 verschiedene Hochschulen und Einrichtungen aus Wissenschaft und Forschung durch Cyberangriffe betroffen. Von diesen 36 Hochschulen und Einrichtungen aus Wissenschaft und Forschung sind zwei mehrmals Ziel durch Cyberangriffe geworden. Im Jahr 2022 erfolgten 19 Angriffe, im Jahr 2023 18 Angriffe und bisher im Jahr 2024 fünf Angriffe.

14. Wie oft wurden seit 2022 die Bundeswehruniversitäten in Hamburg und in München Ziel eines Cyberangriffs?

Seit 2022 gab es zwei Vorfälle im Bereich der Universität der Bundeswehr München.

15. In wie vielen Fällen konnte der Angriff ohne Schaden abgewendet werden?

16. In wie vielen Fällen wurde der Angriff erst nach mehr als einem Monat erkannt?

18. In wie vielen Fällen wurde forschungsrelevantes Material und bzw. oder Daten entwendet oder beschädigt?

Die Fragen 15, 16 und 18 werden gemeinsam beantwortet.

Es wird auf die Vorbemerkung der Bundesregierung und die Antwort zu Frage 1 verwiesen.

17. In wie vielen Fällen wurden die Hochschulen durch den Angriff negativ beeinträchtigt, und um welche Schäden handelte es sich in diesen Fällen?

In 30 der 42 in der Antwort zu Frage 1 genannten der Bundesregierung bekannten Fälle von Cyberangriffen auf Hochschulen und Wissenschaftseinrichtungen wurden unterschiedliche Arten von Beeinträchtigungen festgestellt. Die festgestellten Schäden reichen von Ausfällen der Hochschul-Website über zeitweise Beeinträchtigungen von IT-gestützten Diensten und Hochschulangeboten, dem Ausleiten von Daten bis hin zu großflächigen Verschlüsselungen von IT-Servern und längerfristigen Ausfällen.

19. Wie haben sich nach Kenntnis der Bundesregierung und unter Einbindung der Hochschulrektorenkonferenz (HRK) die Ausgaben bzw. Haushaltsansätze zur Prävention und Bekämpfung von Cyberangriffen an Hochschulen in Deutschland seit 2022 entwickelt?

Ausgaben bzw. Haushaltsansätze zur Prävention und Bekämpfung von Cyberangriffen an Hochschulen werden bundesseitig nicht systematisch erfasst.

20. Wie viele Cyberangriffe wurden nach Kenntnis der Bundesregierung seit 2022 auf Einrichtungen der Fraunhofer-Gesellschaft (FhG), der Max-Planck-Gesellschaft (MPG), der Helmholtz-Gemeinschaft Deutscher Forschungszentren (HGF) und der Leibniz-Gemeinschaft (WGL) festgestellt?

Der Bundesregierung sind sieben Angriffe auf die benannten Einrichtungen bekannt.

Hinsichtlich der Meldungen der Wissenschaftseinrichtungen wird auf die Antwort zu Frage 1 verwiesen.

22. In wie vielen Fällen konnte nach Kenntnis der Bundesregierung der Angriff ohne Schaden abgewendet werden (bitte für die FhG, MPG, HGF und WGL einzeln aufführen)?

Fraunhofer-Gesellschaft

Jahr	Anzahl der Cyberangriffe
2022	1
2023	0
2024	0

Max-Planck-Gesellschaft

Jahr	Anzahl der Cyberangriffe
2022	4
2023	1
2024	0

Helmholtz-Gemeinschaft

Jahr	Anzahl der Cyberangriffe
2022	1 167
2023	1 169
2024	1 146

Leibniz-Gemeinschaft

Jahr	Anzahl der Cyberangriffe
2022	1
2023	1
2024	–

23. In wie vielen Fällen wurde nach Kenntnis der Bundesregierung der Angriff erst nach mehr als einem Monat erkannt (bitte für die FhG, MPG, HGF und WGL einzeln aufführen)?

Fraunhofer-Gesellschaft

Jahr	Anzahl der Cyberangriffe
2022	2
2023	0
2024	0

Helmholtz-Gemeinschaft

Jahr	Anzahl der Cyberangriffe
2022	0
2023	2
2024	0

Leibniz-Gemeinschaft

Jahr	Anzahl der Cyberangriffe
2022	1
2023	1
2024	–

Der Bundesregierung sind bzgl. der Max-Planck-Gesellschaft keine derartigen Fälle bekannt.

24. In wie vielen Fällen wurde nach Kenntnis der Bundesregierung forschungsrelevantes Material und bzw. oder Daten entwendet oder beschädigt?

Fraunhofer-Gesellschaft

Jahr	Anzahl der Cyberangriffe
2022	1
2023	0
2024	0

Max-Planck-Gesellschaft

Jahr	Anzahl der Cyberangriffe
2022	2
2023	0
2024	0

Helmholtz-Gemeinschaft

Jahr	Anzahl der Cyberangriffe
2022	0
2023	2
2024	0

Leibniz-Gemeinschaft

Jahr	Anzahl der Cyberangriffe
2022	1
2023	2
2024	–

Anmerkung: Hierzu liegen Informationen nur zu vier der fünf Einrichtungen vor. Eine dieser Einrichtungen konnte einen Datenabzug verhindern, die drei weiteren Fälle sind der vorstehenden Tabelle zu entnehmen.

27. Wie haben sich die Ausgaben bzw. Haushaltsansätze zur Prävention und Bekämpfung von Cyberangriffen in der FHG, MPG, HGF und WGL seit 2022 entwickelt (bitte je außeruniversitäre Forschungseinrichtung – AuF – einzeln für die Jahre entlang den Kategorien Prävention und Bekämpfung aufführen sowie in Relation zum Gesamtbudget der AuF setzen)?

Fraunhofer-Gesellschaft:

Der Vorstand der Fraunhofer Gesellschaft hat mit der Informationssicherheitskoordination und Sicherheitsinstituten als Reaktion auf Ransomwarevorfälle zusätzlich zu den bestehenden Sicherheitsmaßnahmen 2022 Sondermaßnahmen zur Erhöhung der Cybersicherheit beschlossen. Hierfür wurden 2022 und 2023 zunächst ca. 500 000 Euro für Sofortmaßnahmen ausgegeben, im Jahr 2024 absehbar ca. 2,5 Mio. Euro und den Folgejahren sind derzeit ca. 3 Mio. Euro für die Umsetzung strategischer Sondermaßnahmen vorgesehen. Zusätzlich ergreifen die Institute ihre lokalen IT-Maßnahmen.

Max-Planck-Gesellschaft:

Der Bundesregierung liegen keine Zahlen der Max-Planck-Gesellschaft vor.

Helmholtz-Gemeinschaft

Jahr	Ausgaben/HH-Ansätze zur Prävention in Euro	Prozentualer Anteil am Gesamtbudget	Ausgaben/HH-Ansätze zur Bekämpfung in Euro	Prozentualer Anteil am Gesamtbudget
2022	6 947 227	k. A.	94 500	k. A.
2023	13 819 794	k. A.	3 141 280	k. A.
2024	10 232 537	k. A.	1 046 000	k. A.

Die Zentren der Helmholtz-Gemeinschaft sind rechtlich unabhängig und agieren in eigener Verantwortung, das gilt auch für die Verausgabung von Mitteln zur Prävention und Bekämpfung von Cyberangriffen. Die Mittel, die die Zentren verausgabt haben, sind ausgewiesen. Aufgrund der unterschiedlichen Größen und individuellen Situationen der Zentren, wird die institutionelle Förderung des Bundes gemäß Einzelplan 30 Titel 3004 685 70 (Betrieb) angegeben: 2022: 2 341 454 000 Euro; 2023: 2 428 925 000 Euro; 2024: 2 486 267 000 Euro.

Leibniz-Gemeinschaft:

Hierzu liegen der Bundesregierung keine Informationen aus den einzelnen Einrichtungen vor. Im Jahr 2023 war an 90 der 97 Leibniz-Einrichtungen jeweils mindestens eine Person für IT-Sicherheit beschäftigt. Des Weiteren ist in der Geschäftsstelle der Leibniz-Gemeinschaft eine Referentin für Informationssicherheit zuständig.

Zum 1. Oktober 2023 haben 58 Einrichtungen der Leibniz-Gemeinschaft einen Rahmenvertrag für Incident Response Dienstleistungen abgeschlossen. In diesem Rahmen können die Einrichtungen professionelle Unterstützung durch einen international führenden IT-Sicherheitsdienstleister beziehen. Neben der Schadensminimierung im Falle eines Cyber-Angriffs umfasst das Angebot präventive Maßnahmen und Schulungen zu hervorragenden Konditionen.

28. Was hat die Bundesregierung in dieser Legislaturperiode unternommen, um die Resilienz von Wissenschaftseinrichtungen gegen Cyberangriffe zu erhöhen und bei der Abwehr von Cyberangriffen aktiv zu unterstützen, und welche internationalen Kooperationen hat die Bundesregierung mit dieser Zielstellung geschlossen?

Die Wissenschaftseinrichtungen sind rechtlich selbständig und für die Abwehrfähigkeit gegenüber Cyberangriffen grundsätzlich selbst verantwortlich. Der Bund und die Länder bieten mit ihrer verlässlichen Grundfinanzierung Rahmenbedingungen, um die Fähigkeiten an die jeweiligen Herausforderungen anzupassen.

Die Bundesregierung fördert seit November 2022 das Vorhaben „Reallabor für moderne Cybersicherheit in Forschungseinrichtungen“, das exemplarisch für zwei Wissenschaftseinrichtungen untersucht und aufzeigt, mit welchen Mitteln eine höhere Sicherheit vor Cyberangriffen an derartigen Einrichtungen geschaffen werden kann.

Mit Blick auf die Resilienz von Wissenschaftseinrichtungen gegen Cyberangriffe unterstützt die Bundesregierung u. a. mit speziell auf die Bedürfnisse von Wissenschaftseinrichtungen zugeschnittenen Angeboten, wie etwa das in 2022 veröffentlichte IT-Grundschutzprofil für Hochschulen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beobachtet kontinuierlich die Cybersicherheitslage und berichtet hierzu in Form von unterschiedlichen Lageprodukten (z. B. Tageslagebild, Monatslagebild, Cybersicherheitswarnungen), um Organisationen bei einer realistischen Lageeinschätzung zu unterstützen. Das BSI tauscht sich hierzu auch mit internationalen Partnern aus.

Das BSI bietet mit dem IT-Grundschutz einen Standard für alle Organisationen an, mit dem Cybersicherheit einfach und effektiv umgesetzt werden kann. Dieser wird kontinuierlich evaluiert und fortgeschrieben.

Der Bereich Wirtschafts- und Wissenschaftsschutz des Bundesamtes für Verfassungsschutz (BfV) führt eine langjährige vertrauensvolle Kooperation mit dem Arbeitskreis Sicherheit und Wissenschaft (AK SuWi, Teil des Arbeitskreis Informationssicherheit der deutschen Forschungseinrichtungen – AKIF). In diesem sind Vertreterinnen und Vertreter aus Universitäten und den deutschen Forschungsgemeinschaften versammelt. Hier finden regelmäßig Treffen statt, um sich über aktuelle Trends, Lagefeststellungen und zukünftige Entwicklungen von Bedrohungen auszutauschen.

Im Rahmen der Entwicklung einer nationalen Wirtschaftsschutzstrategie (die ausdrücklich auch Wissenschaftsschutz vorsieht) durch das Bundesministerium des Innern und für Heimat (BMI) wurde seitens des Bereichs Wirtschafts- und Wissenschaftsschutz die Einbindung des AK SuWi angeboten. Zusätzlich erfolgen proaktiv Sensibilisierungen von Forschungsgruppen, die aufgrund von internen Risikobewertungen einem erhöhtem Aufklärungsdruck unterliegen.

29. Steht die Bundesregierung zum Thema „Cyberangriffe auf deutsche Wissenschaftseinrichtungen“ im Austausch mit der Hochschulrektorenkonferenz (HRK), der Allianz der Wissenschaftsorganisationen und der Kultusministerkonferenz (KMK)?

30. Wenn ja, wie viele Gespräche gab es jeweils seit 2022 zwischen der Bundesregierung und der HRK, Allianz der Wissenschaftsorganisationen und der KMK zum Thema deutsche Wissenschaftseinrichtungen als Ziel von Cyberkriminalität?

31. Welche Schlüsse wurden aus diesen Gesprächen seitens der Bundesregierung gezogen?

Die Fragen 29 bis 31 werden gemeinsam beantwortet.

Das BMBF steht über regelmäßige Austauschformate mit den Leitungsebenen der Allianz in konstantem Austausch.

Dieser beinhaltet jeweils aktuelle, von beiden Seiten zu benennende Themen und in diesem Sinne anlassbezogen auch Bedrohungen durch Cyberkriminalität. Da dieser Austausch aber nicht unter einer bestimmten thematischen Überschrift erfolgt, sondern eben multithematisch aufgebaut ist, lässt sich die Anzahl der Gespräche zu eben diesem Thema nicht rekonstruieren.

Das BMBF hat das Thema Cyberangriffe auf Wissenschaftseinrichtungen in den Sitzungen der Kultusministerkonferenz (KMK) bzw. den Amtschefkonferenzsitzungen (AK) in dieser Legislaturperiode nicht thematisiert.

Auf Steuerungsebene wie auch auf Arbeitsebene ist ein Austausch im Rahmen der Bund-Länder-offenen Arbeitsgruppe Hybride Bedrohungen (BLoAG Hybrid, Federführung BMI) in der Struktur der Innenministerkonferenz (IMK) etabliert. Im Rahmen der BLoAG Hybrid wurden für die Bereiche: „Wirtschaft“, „Politik und Verwaltung“ und „Wissenschaft“ Unterarbeitsgruppen gebildet, die einen gemeinsamen Bericht zum Thema „Hybride Bedrohungen/illegitime Einflussnahme fremder Staaten – Notwendigkeit einer verstärkten Zusammenarbeit von Bund und Ländern einschließlich Kommunen“ verfasst haben. Das BMI hat den Bericht der IMK zu deren Frühjahrsitzung 2024 zur Kenntnis vorgelegt. Zur Abstimmung des Berichts fand ein Austausch auf Arbeitsebene zwischen dem BMBF und der KMK statt.

32. Wie oft hat sich die Bundesministerin für Bildung und Forschung, Bettina Stark-Watzinger, seit 2022 mit der Bundesministerin des Innern und für Heimat, Nancy Faeser, zum Thema „deutsche Wissenschaftseinrichtungen als Ziel von Cyberattacken“ ausgetauscht, und welche Ergebnisse wurden erzielt bzw. welche gemeinsamen Initiativen ergriffen?

Bundesministerin Bettina Stark-Watzinger und Bundesministerin Nancy Faeser tauschen sich regelmäßig zu relevanten politischen Themen aus. Die Leitungsgespräche werden nicht protokolliert, so dass im Nachgang eine genaue Rekonstruktion der behandelten Inhalte nicht möglich ist.

33. Welche Unterstützungsmöglichkeiten gibt es vonseiten der Bundesregierung im Falle eines Cyberangriffs auf eine deutsche Wissenschaftseinrichtung?

Das BSI verfügt über eine breite Palette von Unterstützungsmöglichkeiten, bei denen je nach Einzelfall seitens des BSI mehr oder weniger Ressourcen gebunden werden. Welche davon eingesetzt werden, muss und wird im Einzelfall und in Rücksprache mit den Betroffenen entschieden.

Der Bereich Wirtschafts- und Wissenschaftsschutz des BfV bietet Unterstützung bei Cyberangriffen an, die auf staatliche (gesteuerte) Akteure zurückgehen. Sensibilisierungen, Empfehlungen und eine operative Bearbeitung sind dabei möglich.

Weiterhin wird auf die Antwort zu Frage 28 verwiesen.

34. Welche präventiven Unterstützungsmöglichkeiten gibt es seitens der Bundesregierung für Wissenschaftseinrichtungen im Rahmen der Abwehr von Cyberangriffen?

35. Wie stellt die Bundesregierung sicher, dass Akteure in Wissenschaft und Forschung über die Unterstützungsleistungen seitens des Bundes bestmöglich informiert sind?

Die Fragen 34 und 35 werden gemeinsam beantwortet.

Auf die Antworten zu den Fragen 28 und 33 wird verwiesen.

36. Plant die Bundesregierung, nach Vorbild des Landes Nordrhein-Westfalen, die Einrichtung einer durchgehend erreichbaren Kontaktstelle „Cybercrime“, an die sich betroffene Wissenschaftseinrichtungen unkompliziert wenden können, wenn ja, zu wann, und wenn nein, warum nicht?

Das Bundeskriminalamt unterhält wie auch Nordrhein-Westfalen und die anderen Länder eine ZAC (Zentrale Ansprechstelle Cybercrime) und ist Vorsitzender des sogenannten ZAC-Verbunds.

37. Plant die Bundesregierung weiterführende Maßnahmen zur Unterstützung von Wissenschaftseinrichtungen mit Blick auf den Schutz militär- und sicherheitsrelevanter Forschung, wenn ja, welche, und zu wann sollen diese in Kraft treten, und wenn nein, warum nicht?

Es wird auf das Positionspapier „Forschungssicherheit im Lichte der Zeitenwende“ des BMBF verwiesen (abrufbar unter: www.bmbf.de/bmbf/shareddocs/kurzmeldungen/de/2024/03/240311-positionspapier-forschungssicherheit.html).

38. Welche Maßnahmen plant die Bundesregierung ggf. zum verstärkten Schutz der Bundeswehruniversitäten in Hamburg und München vor Cyberangriffen?

Über die vorhandenen Schutzmaßnahmen dieser Dienststellen hinaus sind keine zusätzlichen Maßnahmen erforderlich.

39. Mit welchen Maßnahmen plant die Bundesregierung, die deutschen Wissenschaftseinrichtungen bei der Ertüchtigung ihrer IT-Infrastruktur zum Schutz vor Cyberangriffen zu unterstützen?

Die Bundesregierung beabsichtigt hinsichtlich der Ressortforschungseinrichtungen in ihrem Zuständigkeitsbereich eine Ertüchtigung der IT-Infrastruktur zum besseren Schutz vor Cyberangriffen im Rahmen des Programms IT-Konsolidierung Bund. So können etwa Ressortforschungseinrichtungen auf gehärtete Anwendungen und IT-Infrastrukturplattformen der IT-Konsolidierung Bund zurückgreifen.

Die Bundesregierung fördert seit November 2022 das Vorhaben „Reallabor für moderne Cybersicherheit in Forschungseinrichtungen“, das exemplarisch für zwei Wissenschaftseinrichtungen untersucht und aufzeigt, mit welchen Mitteln eine höhere Sicherheit vor Cyberangriffen an derartigen Einrichtungen geschaffen werden kann.

40. Gab es in Reaktion auf die Veröffentlichung des Berichts „Die Lage der IT-Sicherheit in Deutschland“ des Bundesamts für Sicherheit in der Informationstechnik (BSI) in den Jahren 2022 und 2023 innerhalb der Bundesregierung Gespräche zu Möglichkeiten der Verbesserung der Resilienz deutscher Wissenschaftseinrichtungen vor Cyberangriffen?

    a) Wenn ja, was war der Erkenntnisgewinn aus diesen Gesprächen?

    b) Wenn nein, warum nicht?

Die Fragen 40 bis 40b werden gemeinsam beantwortet.

Auf die Antworten zu den Fragen 33, 37 und 39 wird verwiesen.

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.bundesanzeiger-verlag.de
ISSN 0722-8333